

HP Network Node Manager iSPI Performance for Traffic Software

For the Windows[®] and Linux operating systems

Software Version: 10.00

Reports Online Help

Document Release Date: July 2014

Software Release Date: July 2014



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Red Hat® Enterprise Linux® is a registered trademark of Red Hat, Inc. in the United States and other countries.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

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

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

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

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

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

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

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

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

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Contents	3
Chapter 1: Interface Traffic Reports	7
Calendar Report	8
Chart Detail Report	9
Heat Chart Report	9
Managed Inventory Report	10
Most Changed Report	12
Peak Period Report	12
Top N Report	13
Top N Chart Report	13
Top N Table Report	14
Chapter 2: Interface Traffic 1 Minute Reports	15
Interface Traffic 1 Minute Headline Report	16
Interface Traffic 1 Min Top N Analysis Report	18
Interface Traffic_1_min Top Applications for ToS Report	22
Interface Traffic_1_min Top Conversations for Application Report	25
Interface Traffic_1_min Top Conversations for ToS Report	26
Interface Traffic_1_min Top Destinations for Applications Report	28
Interface Traffic_1_min Top Sources for Applications Report	29
Interface Traffic_1_min Top Sources for ToS Report	30
Interface Traffic_1_min Top Applications Report	33
Interface Traffic_1_min Top Conversations Report	34
Interface Traffic_1_min Top Destinations Report	35
Interface Traffic_1_min Top Interfaces Report	36
Interface Traffic_1_min Top Sources Report	37
Interface Traffic_1_min Top TypeOfService Report	37
Interface Traffic_1_min Top Destination Ports Report	38
Interface Traffic_1_min Top Sources for Destination Port Report	39
Interface Traffic_1_min Top Destinations for Destination Port Report	43

Interface Traffic_1_min Top Conversations for Destination Port Report	47
Interface Traffic 1 Min Top N Chart Analysis Report	50
Interface Traffic_1_min Top Applications for ToS Report	54
Interface Traffic_1_min Top Conversations for Application Report	57
Interface Traffic_1_min Top Conversations for ToS Report	58
Interface Traffic_1_min Top Destinations for Applications Report	60
Interface Traffic_1_min Top Sources for Applications Report	61
Interface Traffic_1_min Top Sources for ToS Report	62
Interface Traffic_1_min Top Applications Report	64
Interface Traffic_1_min Top Conversations Report	65
Interface Traffic_1_min Top Destinations Report	66
Interface Traffic_1_min Top Interfaces Report	67
Interface Traffic_1_min Top Sources Report	67
Interface Traffic_1_min Top TypeOfService Report	68
Interface Traffic_1_min Top Destination Ports Report	69
Interface Traffic_1_min Top Sources for Destination Port Report	69
Interface Traffic_1_min Top Destinations for Destination Port Report	73
Interface Traffic_1_min Top Conversations for Destination Port Report	76
Interface Traffic 1 Min Top N Table Analysis Report	80
Interface Traffic_1_min Top Applications for ToS Report	84
Interface Traffic_1_min Top Conversations for ToS Report	85
Interface Traffic_1_min Top Conversations for Application Report	85
Interface Traffic_1_min Top Destinations for Applications Report	86
Interface Traffic_1_min Top Sources for Applications Report	87
Interface Traffic_1_min Top Sources for ToS Report	88
Interface Traffic_1_min Top Applications Report	88
Interface Traffic_1_min Top Conversations Report	89
Interface Traffic_1_min Top Destinations Report	90
Interface Traffic_1_min Top Interfaces Report	91
Interface Traffic_1_min Top Sources Report	91
Interface Traffic_1_min Top TypeOfService Report	92

Interface Traffic_1_min Top Destination Ports Report	92
Interface Traffic_1_min Top Sources for Destination Port Report	93
Interface Traffic_1_min Top Destinations for Destination Port Report	97
Interface Traffic_1_min Top Conversations for Destination Port Report	100
Chapter 3: Interface Traffic Aggregated Reports	105
Interface Traffic Aggregated Headline Report	106
Interface Traffic Aggregated Top N Analysis Report	108
Interface Traffic Aggregated Top Applications by ToS Report	112
Interface Traffic Aggregated Top Conversations for Application Report	115
Interface Traffic Aggregated Top Conversations by ToS Report	116
Interface Traffic Aggregated Top Destinations by Application Report	119
Interface Traffic Aggregated Top Sources by Application Report	119
Interface Traffic Aggregated Top Sources by ToS Report	120
Interface Traffic Aggregated Top Applications Report	123
Interface Traffic Aggregated Top Conversations Report	124
Interface Traffic Aggregated Top Destinations Report	125
Interface Traffic Aggregated Top Interfaces Report	126
Interface Traffic Aggregated Top Sources Report	127
Interface Traffic Aggregated Top TypeOfService Report	127
Interface Traffic Aggregated Top Destination Ports Report	128
Interface Traffic Aggregated Top Sources for Destination Port Report	129
Interface Traffic Aggregated Top Destinations for Destination Port Report	133
Interface Traffic Aggregated Top Conversations for Destination Port Report	137
Interface Traffic Aggregated Top N Chart Analysis Report	140
Interface Traffic Aggregated Top Applications by ToS Report	144
Interface Traffic Aggregated Top Conversations for Application Report	147
Interface Traffic Aggregated Top Conversations by ToS Report	148
Interface Traffic Aggregated Top Destinations by Application Report	151
Interface Traffic Aggregated Top Sources by Application Report	151
Interface Traffic Aggregated Top Sources by ToS Report	152
Interface Traffic Aggregated Top Applications Report	155

Interface Traffic Aggregated Top Conversations Report	156
Interface Traffic Aggregated Top Destinations Report	156
Interface Traffic Aggregated Top Interfaces Report	157
Interface Traffic Aggregated Top Sources Report	158
Interface Traffic Aggregated Top TypeOfService Report	158
Interface Traffic Aggregated Top Destination Ports Report	159
Interface Traffic Aggregated Top Sources for Destination Port Report	160
Interface Traffic Aggregated Top Destinations for Destination Port Report	163
Interface Traffic Aggregated Top Conversations for Destination Port Report	167
Interface Traffic Aggregated Top N Table Analysis Report	170
Interface Traffic Aggregated Top Applications by ToS Report	175
Interface Traffic Aggregated Top Conversations by ToS Report	177
Interface Traffic Aggregated Top Conversations for Application Report	180
Interface Traffic Aggregated Top Destinations by Application Report	181
Interface Traffic Aggregated Top Sources by Application Report	181
Interface Traffic Aggregated Top Sources by ToS Report	182
Interface Traffic Aggregated Top Applications Report	185
Interface Traffic Aggregated Top Conversations Report	186
Interface Traffic Aggregated Top Destinations Report	186
Interface Traffic Aggregated Top Interfaces Report	187
Interface Traffic Aggregated Top Sources Report	187
Interface Traffic Aggregated Top TypeOfService Report	188
Interface Traffic Aggregated Top Destination Ports Report	189
Interface Traffic Aggregated Top Sources for Destination Port Reports	189
Interface Traffic Aggregated Top Destinations for Destination Port Report	193
Interface Traffic Aggregated Top Conversations for Destination Port Report	197
We appreciate your feedback!	201

Chapter 1: Interface Traffic Reports

The HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) provides you with the Interface traffic reports to view and analyze the network performance data in the NNM iSPI Performance for Traffic environment. You can use the `Interface Traffic` extension pack to generate reports for raw traffic data available in the NPS database. These reports operate on all the traffic data samples that are collected by the Leaf Collectors. This data is preserved in the NPS database in the following forms:

- Data aggregated at every hour: The data is stored for seven days
- Data aggregated at every minute: The data is stored for three days

Use these reports only to perform a detailed analysis of traffic data for a short time interval and a limited set of days.

You can view the following types of Interface Traffic reports:

- Calendar
- Chart Detail
- Heat Chart
- Managed Inventory
- Most Changed
- Peak Period
- Top N
- Top N Chart
- Top N Table

Prerequisites for viewing the Interface Traffic reports

The following prerequisites must be met to view the Interface Traffic reports:

- Install the NNM iSPI Performance for Metrics in your environment before installing the NNM iSPI Performance for Traffic.
- Make sure that the `Interface_Traffic` extension pack is installed successfully. To check for a successful installation, run the following command on the NPS system:
On Windows

```
%NPSInstallDir%\NNMPerformanceSPI\bin\statusALL.ovpl
```

On Linux

```
\opt\OV\NNMPerformanceSPI\bin\statusALL.ovpl
```

If the command displays the status of the extension pack as OK, it indicates that the installation is successful.

Accessing the Interface Traffic Reports

To access the Interface Traffic reports from the NNMi console, follow these steps:

1. Log on to the NNMi console.
2. Click **Actions > NNM iSPI Performance > Reporting-Report Menu** from the menu bar. This launches the Network Performance Server page.
3. Click **iSPI Traffic > Interface_Traffic > Interface TrafficMetrics** under the Reports tab in the navigation panel to see the list of reports that you can launch using Interface Traffic extension pack.

Calendar Report

The Calendar report uses a traditional, calendar-style layout to show hourly statistics for two metrics in a single, extended graph spanning over multiple days. This report cannot operate with a time range less than 24 hours. By default, this report displays the data for the current month.

Use this report to:

- View gradual trends over time
- View isolated spikes
- View abnormal conditions
- View hour of day patterns
- Compare two metrics

The Calendar report defaults to the following values:

- Interfaces (interfaces that are configured to report flow packets) = All
- Dates/Times = Last 1 hour
- Metric(s) Shown on Y1 Axis (Primary Metric) = Volume - In Bytes (sum)
- Metric(s) Shown on Y2 Axis (Secondary Metric) = Volume - Out Bytes (sum)

The default view shows the data for the current month. Depending on how long the NNM iSPI Performance for Traffic has been collecting data from flow collectors, you may have the option of looking at data for the previous two months as well as the last 31 days.

Chart Detail Report

The Chart Detail report enables you to perform a trend analysis for the network health and performance. This report displays a comparative analysis of the selected metrics for each time unit.

Use this report to:

- Analyze the trend of network health and performance for multiple contributors to network traffic based on one unit of time.
- Detect any persistent problem in the network health and performance.

The Chart Detail report defaults to the following values:

- Flow collectors = All
- Metric(s) Shown on Y1 Axis (Primary Metric) = Volume - In Bytes (sum)
- Metric(s) Shown on Y2 Axis (Secondary Metric) = Volume - Out Bytes (sum)

The graph on this report tracks up to six metrics over the selected time period.

The Chart Detail report enables you to view the data in the tabular format as well. To view the table, click **Options**, and then select **Table**. The Table appears instead of the chart. To view both the chart and the table, click **Options**, and then select **Chart and Table**.

Heat Chart Report

The Heat Chart report provides the hourly or daily performance of a single metric in a color-coded format. This report cannot operate with a time range less than 24 hours.

The legend at the top of the report maps a range of normalized performance values to a particular color. Beneath the legend, a table represents the normalized values of a performance metric (rows of the table represent hours of the day; columns of the table represent days). Each cell inside the table is color-coded and each cell inside the table indicates a specific value of the metric.

You can move the mouse pointer on the cell to see the raw data for each hour.

The Heat Chart report defaults to the following values:

- Interfaces (interfaces that are configured to report flow packets) = All
- Dates/Times = Last 1 hour
- Metric(s) Shown on Y1 Axis (Primary Metric) = Volume - In Bytes (sum)

The default topology filters for the Heat Chart report are as follows:

- Interfaces = All
- Time Period = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metric = Volume – In Byte (sum)

Time range options are any period that is not less than 24 hours.

Managed Inventory Report

The Managed Inventory report displays the number of unique instances of the available topology attributes that you can use for network traffic analysis.

You can use the available attributes to filter the data of your interest and create a report that represents only the area of your interest. The report presents the list of attributes in the form of a table. The Count column of the table indicates the number of entries for each attribute.

You can use the following topology attributes with the Interface Health reports:

- Interface ID
- Interface Name
- Qualified Interface Name
- Node Name
- Interface ODBID
- Node ODBID
- Interface UUID
- Interface Alias
- Interface Physical Address
- Interface Type
- SecGroup Name
- SecGroup UUID
- Interface SecGroup Name
- Interface SecGroup UUID

- Node UUID
- Tenant Name
- Tenant UUID
- Flow Version
- IP Protocol
- Class of Service
- Application Name
- Source Port
- Destination Port
- Source Host IP Address
- Destination Host IP Address
- Source Host Name
- Destination Host Name
- Source Vlan ID
- Destination Vlan ID
- Source Vlan
- Destination Vlan
- Collector Name
- Source Site Name
- Destination Site Name
- Type of Service
- Source AS
- Destination AS
- Source Subnet Address
- Destination Subnet Address
- Type of Service - IP Precedence

- Type of Service - DSCP

Most Changed Report

The Most Changed report compares performance of the components for two different (consecutive) time periods and ranks network elements by the amount of change. The sort order is most-changed to least-changed. You can obtain Most changed report with user-specified metric, applied on the topology filter for the selected time interval.

This report contains one table and provides data for one metric only.



The table columns are:

- Component
- Performance for the previous time period
- Performance for the selected time period
- Growth, expressed as a percentage increase
- Change

The Most Changed report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Rank Metric = Volume - In Bytes (sum)
- Top N Option = Top 10

Using the Most Changed report, you can identify the network elements that are affected by the change in traffic flow. You can also perform a root cause analysis of the network congestion.

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

Peak Period Report

The Peak Period report ranks the metrics that indicate the network traffic during the busiest time of the selected time range. The graph on this report tracks up to six primary metrics and six secondary

over the selected time period.



Top N Report

The Top N report ranks top contributors to the network traffic by the metric you select.

You can choose a rank number of 5, 10, 25, 50, or 100. The report enables you to see Top N or Bottom N report of the selected metrics.

The Top N report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

This report ranks network elements by the metrics you select. This report shows data in the form of bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.



Top N Chart Report

The Top N Chart report ranks network traffic metrics by the top N 'Grouping By' metrics and shows the data in the form of line graphs over time (N different line graphs).

You can choose a rank number of 5, 10, 25, 50, or 100. The report enables you to see Top N or Bottom N report of the selected metrics.

The Top N report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (**Add New Grouping**) button. Use the  (**Remove Grouping**) button to remove a grouping attribute.

Top N Table Report



The Top N Table report ranks network traffic metrics by the top N 'Grouping By' metrics.

You can choose a rank number of 5, 10, 25, 50, or 100. The report enables you to see Top N or Bottom N report of the selected metrics.

This report ranks network elements by the metrics you select. Unlike the Top N report, this report does not show any bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

The Top N Table report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (**Add New Grouping**) button. Use the  (**Remove Grouping**) button to remove a grouping attribute.

Chapter 2: Interface Traffic 1 Minute Reports

The HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) provides you with the Interface traffic reports to view and analyze the network performance data in the NNM iSPI Performance for Traffic environment. You can use the `Interface Traffic_1_min` extension pack to generate reports for traffic data aggregated at every 1 minute. This data is stored in the NPS database for up to 31 days. Therefore, you can use this report group to build reports with historical data and view reports on performance metrics for the last one year.

Note: The `Interface Traffic_1_min` reports are disabled by default. For information on how to enable these reports, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every 1 minute and the data is preserved. Data about the less significant contributors to network traffic are aggregated and displayed as `Anonymous` or `-1` on these reports. The above processing is done on every flow-enabled interface. The strings, such as `hostname`, are displayed as `Anonymous` and the integers, such as `port number` are displayed as `-1`.

This category of reports enables you to perform the following tasks:

- Display top contributors reports: The top contributors reports are reports that enable you to directly inspect top contributors for applications, type of service, sources, destinations, and conversations.
- Perform contextual analysis for a contributor: The top contributors reports enable you to further analyze the data by generating reports by using the contextual navigation feature of the NPS. You can select one of the displayed contributors and launch a report that provides drill-down analysis for the selected contributor.

You can view the following types of Interface Traffic 1 minute reports:

- `Headline Report`
- `Top N Analysis Report`
- `Top N Chart Analysis Report`
- `Top N Table Analysis Report`

Prerequisites for viewing the Interface Traffic reports

The following prerequisites must be met to view the Interface Traffic 1 minute reports:

- Install the NNM iSPI Performance for Metrics in your environment before installing the NNM iSPI Performance for Traffic.

- Make sure that the `Interface_Traffic_1_min` extension pack is installed successfully. To check for a successful installation, run the following command on the NPS system:
On Windows

```
%NPSInstallDir%\NNMPerformanceSPI\bin\statusALL.ovpl
```

On Linux

```
\opt\OV\NNMPerformanceSPI\bin\statusALL.ovpl
```

If the command displays the status of the extension pack as OK, it indicates that the installation is successful.

- Enable the `Interface_Traffic_1_min` reports. For information on how to enable these reports, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

Accessing the Interface Traffic 1 minute Reports

To access the Interface Traffic 1 minute reports from the NNMi console, follow these steps:

1. Log on to the NNMi console.
2. Click **Actions > NNM iSPI Performance > Reporting-Report Menu** from the menu bar. This launches the Network Performance Server page.
3. Click **iSPI Traffic > Interface_Traffic_1_min** under the Reports tab in the navigation panel to see the list of reports that you can launch using Interface Traffic_1_min extension pack.

Interface Traffic 1 Minute Headline Report

The Headline Report provides a broad view of traffic performance for the past one hour, using the following graphs:

Graph	Description
Top N Conversations Incoming	Displays the top N incoming conversations between the selected source and destination hosts.
Top N Conversations Outgoing	Displays the top N outgoing conversations between the selected source and destination hosts.
Top N Destinations Incoming	Displays the top N destination hosts that receive the maximum volume of data. Displays the volume of ingress data.
Top N Destinations Outgoing	Displays the top N destination hosts that send the maximum volume of data. Displays the volume of egress data.

Graph	Description
Top N Sources Incoming	Displays the top N source hosts that receive the maximum volume of data. Displays the volume of ingress data.
Top N Sources Outgoing	Displays the top N source hosts that send the maximum volume of data. Displays the volume of egress data.
Top N Applications Incoming	Displays the top N applications receiving the maximum volume of data.
Top N Applications Outgoing	Displays the top N applications sending the maximum volume of data.
Top N ToS Incoming	Displays the top N types of services receiving the maximum volume of data.
Top N ToS Outgoing	Displays the top N types of services sending the maximum volume of data.

This report enables you to:

- View every aspect of traffic performance at once.
- View trends and verify that the traffic performance is meeting expectations.
- Identify isolated aberration in the graphs and detect any unexpected utilization or performance trend.

[To launch this report:](#)

1. In the NPS console, go to the Reports workspace.
2. Select **iSPI Traffic > Interface Traffic_1_min > Headline**.

The Headline report defaults to the following values:

- Time Range = Last 1 hour
- Grain = 5 minutes
- Topology group tracking method = SCD Type 1

Tip: HP recommends that you schedule the generation and delivery of the Headline report. Without scheduling, the NNM iSPI Performance for Traffic may take considerable amount of time to generate the Headline report.

Interface Traffic 1 Min Top N Analysis Report

The NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods. The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available 1 Minute Top N Reports

Report	Description
Interface Traffic_1_min Top Applications for ToS	Displays the top applications across the network for the selected ToS value.
Interface Traffic_1_min Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.
Interface Traffic_1_min Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic_1_min Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.
Interface Traffic_1_min Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic_1_min Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.
Interface Traffic_1_min Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic_1_min Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.
Interface Traffic_1_min Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic_1_min Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic_1_min Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic_1_min Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.

Report	Description
Interface Traffic_1_min Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic_1_min Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic_1_min Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.
Interface Traffic_1_min Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports in the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N reports may prove to be a time consuming and repetitive process. To overcome this problem, the NNM iSPI Performance for Traffic enables you to select the Top N Analysis report, that works as the launching point for all the 1-minute Top N reports.

This report ranks network elements by the metrics you select. This report shows data in the form of bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

To launch the Top N reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic > Interface_Traffic_1_min**.
3. Select **Top N Analysis** .
4. In the Select Report Type panel, select the type of the report you want to launch, and then click **Confirm Selection**. The default selection is Top Interfaces that launches Interface Traffic_1_min Top Interfaces Report. The NNM iSPI Performance for Traffic launches the following reports for each option:
 - Top Sources: Launches the Interface Traffic_1_min Top Sources Report.
 - Top Destinations: Launches the Interface Traffic_1_min Top Destinations Report.
 - Top Conversations: Launches the Interface Traffic_1_min Top Conversations Report.
 - Top Types of Services: Launches the Interface Traffic_1_min Top TypeOfService Report.
 - Top Destination Ports: Launches the Interface Traffic_1_min_Top - DestinationPorts Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**

- a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Traffic_1_min Top Sources for Application Report
 - Destinations for Application: Launches the Interface Traffic_1_min Top Destinations for Application Report
 - Conversations for Application: Launches the Interface Traffic_1_min Top Conversations for Application Report
- c. Click **Confirm Selection**.

- **Top Type of Service**

- a. Select **Type of Service**.

Note: The NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:
 - Application for ToS: Launches the Interface Traffic_1_min Top Applications for ToS Report
 - Sources for ToS: Launches the Interface Traffic_1_min Top Sources for ToS Report
 - Conversations for ToS: Launches the Interface Traffic_1_min Top Conversations for ToS Report
- c. Click **Confirm Selection**.

- **Top Destination Ports**

a. Select **Destination Port**.

Note: The NNM iSPI Performance for Traffic sorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
- Sources for Destination Port: Launches the Interface Traffic_1_min Top Sources for Destination Port report
 - Destinations for Destination Port: Launches the Interface Traffic_1_min Top Destinations for Destination Port report
 - Conversations for Destination Port: Launches the Interface Traffic_1_min Top Conversations for Destination Port report
- c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time you launch the Top N Analysis menu. If you select the topology filter as either Application Name or Type of Service (either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when you launch the 'Top N Analysis' report again.

You can set the topology filters using Run Prompts link on the Top N Analysis report. Once selected, you can remove the filters using the Reset feature only. However, the specific filters that you can select for a report depends on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.


To check which are the applicable fields to filter on a particular report, launch the Topology Selector in the context of that report. That is, first launch that report and then launch the Topology Selector using the Run Prompts link.

To list the 1 Minute Top N Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.

3. Click  **My Area Options > My Preferences.**
4. Select the option **Show hidden entries.**
5. Click **OK.**

Interface Traffic_1_min Top Applications for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps: [click here.](#)

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Applications for ToS report is a Top N report. This report shows top applications across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Applications for ToS report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Conversations for Application Report

The Interface Traffic_1_min Top Conversations for Application report is a Top N report. This report shows top talkers (source-destination pairs) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. By default, this report shows data grouped by only Destination Host Name. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Conversations for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps: [click here](#).

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Conversations for ToS report is a Top N report. This report shows top talkers (source-destination pairs) across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. By default, this report shows data grouped by only destination hosts. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for ToS report defaults the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Destinations for Applications Report

The Interface Traffic_1_min Top Destinations for Application report is a Top N report. This report shows top hosts (which receive data packets from different hosts) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows top destination hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Applications report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Sources for Applications Report

The Interface Traffic_1_min Top Sources for Application report is a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets that are mapped to a specific application; the report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows top source hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Applications report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Sources for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:[click here](#).

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true
6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Sources for ToS report is a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for ToS report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Applications Report

The Interface Traffic_1_min Top Applications report is a Top N report. This report shows top N applications across the network that contribute to the network traffic.

The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (min)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (avg)

- Bandwidth - Out Mbps (min)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (avg)
- Bandwidth Utilization (min)
- Bandwidth Utilization (max)
- Bandwidth Utilization (avg)

The Interface Traffic_1_min Top Applications report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use NNM iSPI Performance for Traffic Top Conversations reports to monitor the top talkers in the environment.

The Interface Traffic_1_min Top Conversations report, by default, shows top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of traffic performance indicators for every source-destination pair, or in other words, for every conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Destinations Report

The Interface Traffic_1_min Top Destinations report is a Top N report. This report shows top N hosts across the network that receive data packets.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.



Interface Traffic_1_min Top Interfaces Report

The Interface Traffic_1_min Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic_1_min Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (**Add New Grouping**) button. Use the  (**Remove Grouping**) button to remove a grouping attribute.

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is

provided as an option.

Interface Traffic_1_min Top Sources Report

The Interface Traffic_1_min Top Sources report is a Top N report. This report shows top N hosts across the network that send data packets to different destinations.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top TypeOfService Report

The Interface Traffic_1_min Top TypeOfService report is a Top N report. This report shows top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic_1_min Top Destination Ports Report

The Interface Traffic_1_min Top Destination Ports report is a Top N report. These reports show top N [destination ports](#)¹ across the network that receive data packets.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destination Ports report defaults to the following values:

¹Recipients of data packets

- Grouping by Elements = Destination Port
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option is available only for the Top N report. It shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph.

Note: The Display Time Series Chart option runs a time-consuming query; therefore, it is provided as an option.

Interface Traffic_1_min Top Sources for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:
- On Windows*

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows


```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Sources for Destination Port report presents a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option is available only for the Top N report. It shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph.

Note: The Display Time Series Chart option runs a time-consuming query; therefore, it is provided as an option.

Interface Traffic_1_min Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Destinations for Destination Port report presents a Top N report. This report shows top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the Destination port 160 shows top destinations that receive data packets on the network traffic on Destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option is available only for the Top N report. It shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph.

Note: The Display Time Series Chart option runs a time-consuming query; therefore, it is provided as an option.

Interface Traffic_1_min Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, `%TrafficDataDir%` is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.


```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic_1_min Top Conversations for Destination Port report presents a Top N report. This report shows top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only. However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option is available only for the Top N report. It shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph.

Note: The Display Time Series Chart option runs a time-consuming query; therefore, it is provided as an option.

Interface Traffic 1 Min Top N Chart Analysis Report

The NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods. The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available 1 Minute Top N Chart Reports

Report	Description
Interface Traffic_1_min Top Applications for ToS	Displays the top applications across the network for the selected ToS value.
Interface Traffic_1_min Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.
Interface Traffic_1_min Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic_1_min Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.

Report	Description
Interface Traffic_1_min Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic_1_min Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.
Interface Traffic_1_min Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic_1_min Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.
Interface Traffic_1_min Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic_1_min Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic_1_min Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic_1_min Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.
Interface Traffic_1_min Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic_1_min Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic_1_min Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.
Interface Traffic_1_min Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports in the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N Chart reports may prove to be a time consuming and repetitive process. To overcome this problem, NNM iSPI Performance for Traffic enables you to select the Top N Chart Analysis report, that works as the launching point for all the 1 minute Top N Chart reports.

To launch the Top N Chart reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic > Interface_Traffic_1_min**.
3. Select **Top N Chart Analysis** .
4. In the Select Report Type panel, select the type of the report you want to launch, and then click **Confirm Selection**. The default selection is Top Interfaces. The NNM iSPI Performance for Traffic launches the following reports for each option:
 - Top Sources: Launches the Interface Traffic 1 min - Top_Sources - Top N Chart Report.
 - Top Destinations: Launches the Interface Traffic 1 min - Top_Destinations - Top N Chart Report.
 - Top Conversations: Launches the Interface Traffic 1 min - Top_Conversations - Top N Chart Report.
 - Top Types of Services: Launches the Interface Traffic 1 min - Top_TypeOfService - Top N Chart Report.
 - Destination Ports: Launches the Interface Traffic 1 min - Top_DestinationPorts - Top N Chart Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**
 - a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Traffic 1 min - Sources_for_Application - Top N Chart Report.
 - Destinations for Application: Launches the Interface Traffic 1 min - Destinations_for_Applications - Top N Chart Report
 - Conversations for Application: Launches the Interface Traffic 1 min - Conversations_for_Application - Top N Chart Report
- c. Click **Confirm Selection**.

- **Top Type of Service**

- a. Select **Type of Service**.

Note: The NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:
 - Application for ToS: Launches the Interface Traffic 1 min - Applications_for_ToS - Top N Chart Report.
 - Sources for ToS: Launches the Interface Traffic 1 min - Sources_for_ToS - Top N Chart Report.
 - Conversations for ToS: Launches the Interface Traffic 1 min - Conversations_for_ToS - Top N Chart Report.
- c. Click **Confirm Selection**.

- **Top Destination Ports**

- a. Select **Destination Port**.

Note: The NNM iSPI Performance for Traffic sorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
 - Sources for Destination Port: Launches the Interface Traffic_1_min Top Sources for Destination Port Chart report.
 - Destinations for Destination Port: Launches the Interface Traffic_1_min Top Destinations for Destination Port Chart report.
 - Conversations for Destination Port: Launches the Interface Traffic_1_min Top Conversations for Destination Port Chart report.
- c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Chart Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time you launch the Top N Chart Analysis Report. If you select the topology filter as either Application Name or Type of Service

(either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when you launch the 'Top N Chart Analysis' report again.


You can set the topology filters using Run Prompts link on the Top N Chart Analysis report. Once selected, you can remove the filters using the Reset feature only. However, the specific filters that you can select for a report depends on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.

To check which are the applicable fields to filter on a particular report, launch the Topology Selector in the context of that report. That is, first launch that report and then launch the Topology Selector using the Run Prompts link.

To list the 1 Minute Top N Chart Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.
3. Click  **My Area Options > My Preferences**.
4. Select the option **Show hidden entries**.
5. Click **OK**.

Interface Traffic_1_min Top Applications for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps: [click here](#).

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Applications for ToS report is a Top N Chart report. This report shows line graphs for top applications across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Applications for ToS report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for Application Report

The Interface Traffic_1_min Top Conversations for Application report is a Top N Chart report. This report shows line graphs for top talkers (source-destination pairs) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. By default, this report shows data grouped by only destination hosts. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps: [click here](#).

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Conversations for ToS report is a Top N Chart report. This report shows top talkers (source-destination pairs) across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. By default, this report shows data grouped by only destination hosts. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for ToS report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations for Applications Report

The Interface Traffic_1_min Top Destinations for Application report is a Top N Chart report. This report shows line graphs for top hosts (which receive data packets from different hosts) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows top destination hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Applications report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for Applications Report

The Interface Traffic_1_min Top Sources for Application report is a Top N Chart report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets that are mapped to a specific application. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows line graphs for top source hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Applications report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps: [click here](#).

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic_1_min Top Applications for ToS report
- The Interface Traffic_1_min Top Sources for ToS report
- The Interface Traffic_1_min Top Conversations for ToS report

The Interface Traffic_1_min Top Sources for ToS report is a Top N Chart report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows line graphs for top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for ToS report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Applications Report

The Interface Traffic_1_min Top Applications report is a Top N Chart report. This report shows top N applications across the network that contribute to the network traffic in the form of line graphs.

The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (min)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (avg)
- Bandwidth - Out Mbps (min)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (avg)
- Bandwidth Utilization (min)
- Bandwidth Utilization (max)
- Bandwidth Utilization (avg)

The Interface Traffic_1_min Top Applications report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use NNM iSPI Performance for Traffic Top Conversations reports to monitor the top talkers in the environment.

By default, the Interface Traffic_1_min Top Conversations report shows top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the

Top N values of traffic performance indicators for every source-destination pair, or in other words, for every conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations Report

The Interface Traffic_1_min Top Destinations report is a Top N Chart report. This report shows top N hosts across the network that receive data packets in the form of line graphs.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10



Interface Traffic_1_min Top Interfaces Report

The Interface Traffic_1_min Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic_1_min Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

Interface Traffic_1_min Top Sources Report

The Interface Traffic_1_min Top Sources report is a Top N Chart report. This report shows top N hosts (in the form of line graphs) across the network that send data packets to different destinations.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top TypeOfService Report

The Interface Traffic_1_min Top TypeOfService report is a Top N report. This report shows top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking on a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destination Ports Report

The Interface Traffic_1_min Top Destination Ports report presents a Top N Chart report. These reports show top N [destination ports](#)¹ across the network that receive data packets in the form of line graphs.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destination Ports report defaults to the following values:

- Grouping by Elements = Destination Port
- Time Range = Last 1 day
- Grain = 1 hour
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

¹Recipients of data packets

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:
On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Sources for Destination Port report presents a Top N chart report. This report shows line graphs for top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/0V/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Destinations for Destination Port report presents a Top N chart report. This report shows line graphs for top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top destinations that receive data packets on the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data

collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic_1_min Top Conversations for Destination Port report presents a Top N chart report. This report shows line graphs for top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only. However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic 1 Min Top N Table Analysis Report

NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods.

This report ranks network elements by the metrics you select. Unlike the Top N report, this report does not show any bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available 1 Minute Top N Table Reports

Report	Description
Interface Traffic_1_min Top Applications for ToS	Displays the top applications across the network for the selected ToS value.
Interface Traffic_1_min Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.
Interface Traffic_1_min Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic_1_min Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.
Interface Traffic_1_min Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic_1_min Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.

Report	Description
Interface Traffic_1_min Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic_1_min Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.
Interface Traffic_1_min Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic_1_min Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic_1_min Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic_1_min Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.
Interface Traffic_1_min Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic_1_min Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic_1_min Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.
Interface Traffic_1_min Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports on the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N Table reports may prove to be a time consuming and repetitive process. To overcome this problem, NNM iSPI Performance for Traffic enables you to select the Top N Table Analysis report, that works as the launching point for all the 1 minute Top N Table reports.

To launch the Top N Table reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic > Interface_Traffic_1_min**.
3. Select **Top N Table Analysis** .
4. In the Select Report Type panel, select the type of the report you want to launch. and then click **Confirm Selection**. The default selection is Top Interfaces. NNM iSPI Performance for Traffic

launches the following reports for each option:

- Top Sources: Launches the Interface Traffic 1 min - Top_Sources - Top N Table Report.
- Top Destinations: Launches the Interface Traffic 1 min - Top_Destinations - Top N Table Report.
- Top Conversations: Launches the Interface Traffic 1 min - Top_Conversations - Top N Table Report.
- Top Types of Services: Launches the Interface Traffic 1 min - Top_TypeOfService - Top N Table Report.
- Destination Ports: Launches the Interface Traffic 1 min - Top_DestinationPorts - Top N Table Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**

- a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Traffic 1 min - Sources_for_Application - Top N Table Report.
 - Destinations for Application: Launches the Interface Traffic 1 min - Destinations_for_Applications - Top N Table Report
 - Conversations for Application: Launches the Interface Traffic 1 min - Conversations_for_Application - Top N Table Report
- c. Click **Confirm Selection**.

- **Top Type of Service**

- a. Select **Type of Service**.

Note: The NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:
 - Application for ToS: Launches the Interface Traffic 1 min - Applications_for_ToS - Top N Table Report.
 - Sources for ToS: Launches the Interface Traffic 1 min - Sources_for_ToS - Top N Table Report.
 - Conversations for ToS: Launches the Interface Traffic 1 min - Conversations_for_ToS - Top N Table Report.
- c. Click **Confirm Selection**.

- **Top Destination Ports**

- a. Select **Destination Port**.

Note: The NNM iSPI Performance for Trafficsorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
 - Sources for Destination Port: Launches the Interface Traffic_1_min Top Sources for Destination Port Table report.
 - Destinations for Destination Port: Launches the Interface Traffic_1_min Top Destinations for Destination Port Table report.
 - Conversations for Destination Port: Launches the Interface Traffic_1_min Top Conversations for Destination Port Table report.
- c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Table Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time you launch the Top N Table Analysis Report. If you select the topology filter as either Application Name or Type of Service (either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when you launch the 'Top N Table Analysis' report again.


You can set the topology filters using Run Prompts link on the Top N Table Analysis report. Once selected, you can remove the filters using the Reset feature only. However, the specific filters that you can select for a report depends on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.

To check which are the applicable fields to filter on a particular report, launch the Topology Selector in the context of that report. That is, first launch that report and then launch the Topology Selector using the Run Prompts link.

To list the 1 Minute Top N Table Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.
3. Click  **My Area Options > My Preferences**.
4. Select the option **Show hidden entries**.
5. Click **OK**.

Interface Traffic_1_min Top Applications for ToS Report

The Interface Traffic_1_min Top Applications for ToS report shows line graphs for top applications across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Applications for ToS report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for ToS Report

The Interface Traffic_1_min Top Conversations for ToS report shows top talkers (source-destination pairs) across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. By default, this report shows data grouped by only destination hosts. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for ToS report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for Application Report

The Interface Traffic_1_min Top Conversations for Application report shows line graphs for top talkers (source-destination pairs) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. By default, this report shows data grouped by only destination hosts. However, if you add Source Host

Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations for Applications Report

The Interface Traffic_1_min Top Destinations for Applications report shows line graphs for top hosts (which receive data packets from different hosts) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows top destination hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Applications report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for Applications Report

The Interface Traffic_1_min Top Sources for Applications report shows top source hosts (hosts that send out data packets) across the network that generate flow packets that are mapped to a specific application. The report is generated by using the contextual navigation feature of the NPS.

Therefore, HP recommends that you launch the Traffic_1_min Top Applications report first, select an application, and then launch this report. The report shows line graphs for top source hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Applications report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for ToS Report

The Interface Traffic_1_min Top Sources for ToS report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Traffic_1_min Top TypeOfService report first, select a ToS value, and then launch this report. The report shows line graphs for top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for ToS report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Applications Report

The Interface Traffic_1_min Top Applications report shows top N applications across the network that contribute to the network traffic in the form of line graphs.

The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (min)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (avg)
- Bandwidth - Out Mbps (min)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (avg)
- Bandwidth Utilization (min)
- Bandwidth Utilization (max)
- Bandwidth Utilization (avg)

The Interface Traffic_1_min Top Applications report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use NNM iSPI Performance for Traffic Top Conversations reports to monitor the top talkers in the environment.

By default, the Interface Traffic_1_min Top Conversations report shows top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of traffic performance indicators for every source-destination pair, or in other words, for every conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as *Anonymous* on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations Report

The Interface Traffic_1_min Top Destinations Report is a Top N Table report. This report shows top N hosts across the network that receive data packets in the form of line graphs.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as *Anonymous* on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10



Interface Traffic_1_min Top Interfaces Report

The Interface Traffic_1_min Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic_1_min Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

Interface Traffic_1_min Top Sources Report

The Interface Traffic_1_min Top Sources report shows top N hosts (in the form of line graphs) across the network that send data packets to different destinations.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top TypeOfService Report

The Interface Traffic_1_min Top TypeOfService report shows top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking on a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destination Ports Report

The Interface Traffic_1_min Top Destination Ports report shows top N [destination ports](#)¹ across the network that receive data packets in the form of line graphs.

¹Recipients of data packets

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destination Ports report defaults to the following values:

- Grouping by Elements = Destination Port
- Time Range = Last 1 day
- Grain = 1 hour
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Sources for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Sources for Destination Port report presents a Top N table report. This report shows tabular data for top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic_1_min Top Destinations for Destination Port report is a Top N table report. This report shows tabular data for top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the Destination port 160 shows top destinations that receive data packets on the network traffic on Destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic_1_min Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic_1_min Top Conversations for Destination Port report is a Top N table report. This report shows tabular data for top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only. However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every one minute and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic_1_min Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Chapter 3: Interface Traffic Aggregated Reports

The HP Network Node Manager iSPI Performance for Traffic Software (NNM iSPI Performance for Traffic) provides you with the Interface Traffic Aggregated reports to view and analyze the network performance data in the NNM iSPI Performance for Traffic environment. You can use the `Interface_Traffic_Aggregated` extension pack to generate reports for traffic data aggregated at every 5 minutes. This data is stored in the NPS database for up to 400 days. Therefore, you can use this report group to build reports with historical data and view reports on performance metrics for the last one year.

Note: You can modify the default aggregation interval and provide value (in minutes) in the range of 5 through 15. For more information, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every 5 minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as `Anonymous` or `-1` on these reports. The above processing is done on every flow-enabled interface. The strings, such as `hostname`, are displayed as `Anonymous` and the integers, such as `port number` are displayed as `-1`.

This category of reports enables you to perform the following tasks:

- Display top contributors reports: The top contributors reports are reports that enable you to directly inspect top contributors for applications, type of service, sources, destinations, and conversations.
- Perform contextual analysis for a contributor: The top contributors reports enable you to further analyze the data by generating reports by using the contextual navigation feature of the NPS. You can select one of the displayed contributors and launch a report that provides drill-down analysis for the selected contributor.

You can view the following types of Interface Traffic Aggregated reports:

- `Headline Report`
- `Top N Analysis Report`
- `Top N Chart Analysis Report`
- `Top N Table Analysis Report`

Quicklaunch ReportViews

The NNM iSPI Performance for Traffic also provides **Quicklaunch ReportViews**. The Quicklaunch ReportViews includes shortcuts to the most commonly used reports. These views provide reports based on data aggregated every 5 minutes. The NNM iSPI Performance for Traffic provides the following report views:

- Site to Site Application Traffic
- Top Application Bandwidth Utilization
- Top Destination Ports and Applications
- Top Destinations
- Top Interfaces

You can also create your own customized reports and add shortcuts to the Quicklaunch ReportViews. For more information, see the *Using Report Views* in the *HP Network Node Manager iSPI Performance for Metrics Software Online Help*.

Prerequisites for viewing the Interface Traffic Aggregated reports

The following prerequisites must be met to view the Interface Traffic Aggregated reports:

- Install the NNM iSPI Performance for Metrics in your environment before installing the NNM iSPI Performance for Traffic.
- Make sure that the `Interface_Traffic_Aggregated` extension pack is installed successfully. To check for a successful installation, run the following command on the NPS system:
On Windows

```
%NPSInstallDir%\NNMPerformanceSPI\bin\statusALL.ovpl
```

On Linux

```
\opt\OV\NNMPerformanceSPI\bin\statusALL.ovpl
```

If the command displays the status of the extension pack as OK, it indicates that the installation is successful.

Accessing the Interface Traffic Aggregated Reports

To access the Interface Traffic Aggregated reports from the NNMi console, follow these steps:

1. Log on to the NNMi console.
2. Click **Actions > NNM iSPI Performance > Reporting-Report Menu** from the menu bar. This launches the Network Performance Server page.
3. Click **iSPI Traffic > Interface_Traffic_Aggregated** under the Reports tab in the navigation panel to see the list of reports that you can launch using `Interface_Traffic_Aggregated` extension pack.

Interface Traffic Aggregated Headline Report

The Headline Report provides a broad view of traffic performance for the past one hour, using the following graphs:

Graph	Description
Top N Conversations Incoming	Displays the top N incoming conversations between the selected source and destination hosts.
Top N Conversations Outgoing	Displays the top N outgoing conversations between the selected source and destination hosts.
Top N Destinations Incoming	Displays the top N destination hosts that receive the maximum volume of data. Displays the volume of ingress data.
Top N Destinations Outgoing	Displays the top N destination hosts that send the maximum volume of data. Displays the volume of egress data.
Top N Sources Incoming	Displays the top N source hosts that receive the maximum volume of data. Displays the volume of ingress data.
Top N Sources Outgoing	Displays the top N source hosts that send the maximum volume of data. Displays the volume of egress data.
Top N Applications Incoming	Displays the top N applications receiving the maximum volume of data.
Top N Applications Outgoing	Displays the top N applications sending the maximum volume of data.
Top N ToS Incoming	Displays the top N types of services receiving the maximum volume of data.
Top N ToS Outgoing	Displays the top N types of services sending the maximum volume of data.

This report enables you to:

- View every aspect of traffic performance at once.
- View trends and verify that the traffic performance is meeting expectations.
- Identify isolated aberration in the graphs and detect any unexpected utilization or performance trend.

To launch this report:

1. In the NPS console, go to the Reports workspace.
2. Select **iSPI Traffic > Interface_Traffic_Aggregated > Headline**.

The Headline report defaults to the following values:

- Time Range = Last 1 hour
- Grain = 5 minutes
- Topology group tracking method = SCD Type 1

Tip: HP recommends that you schedule the generation and delivery of the Headline report. Without scheduling, the NNM iSPI Performance for Traffic may take considerable amount of time to generate the Headline report.

Interface Traffic Aggregated Top N Analysis Report

The NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods. The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available Interface Traffic Aggregated Top N Reports

Report	Description
Interface Traffic Aggregated Top Applications for ToS	Displays the top applications across the network for the selected ToS value.
Interface Traffic Aggregated Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.
Interface Traffic Aggregated Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic Aggregated Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.
Interface Traffic Aggregated Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic Aggregated Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.
Interface Traffic Aggregated Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic Aggregated Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.

Report	Description
Interface Traffic Aggregated Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic Aggregated Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic Aggregated Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic Aggregated Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.
Interface Traffic Aggregated Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic Aggregated Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic Aggregated Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.
Interface Traffic Aggregated Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports in the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N reports may prove to be a time consuming and repetitive process. To overcome this problem, the NNM iSPI Performance for Traffic enables you to select the Top N Analysis report that works as the launching point for all the Interface Traffic Aggregated Top N reports.

This report ranks network elements by the metrics you select. This report shows data in the form of bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

To launch the Top N reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic_Aggregated**.
3. Select **Top N Analysis** .
4. In the Select Report Type panel, select the type of the report you want to launch and then click **Confirm Selection**. The default selection is Top Interfaces. The NNM iSPI Performance for Traffic launches the following reports for each option:

- Top Interfaces: Launches the Interface Traffic Aggregated Top Interfaces Report.
- Top Sources: Launches the Interface Traffic Aggregated Top Sources Report
- Top Destinations: Launches the Interface Traffic Aggregated Top Destinations Report.
- Top Conversations: Launches the Interface Traffic Aggregated Top Conversations Report.
- Top Type of Service: Launches the Interface Traffic Aggregated Top TypeOfService Report.
- Top Destination Ports: Launches the Interface Traffic Aggregated Top DestinationPorts Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**

- a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Traffic Aggregated Top Sources for Application Report.
 - Destinations for Application: Launches the Interface Traffic Aggregated Top Destinations for Application Report
 - Conversations for Application: Launches the Interface Traffic Aggregated Top Conversations for Application Report
- c. Click **Confirm Selection**.

- **Top Type of Service**

- a. Select **Type of Service**.

Note: The NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:

- Application for ToS: Launches the Interface Traffic Aggregated Top Applications for ToS Report.
 - Sources for ToS: Launches the Interface Traffic Aggregated Top Sources for ToS Report.
 - Conversations for ToS: Launches the Interface Traffic Aggregated Top Conversations for ToS Report.
- c. Click **Confirm Selection**.
- **Top Destination Ports**
 - a. Select **Destination Port**.

Note: The NNM iSPI Performance for Traffic sorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
 - Sources for Destination Port: Launches the Interface Traffic Aggregated Top Sources for Destination Port report.
 - Destinations for Destination Port: Launches the Interface Traffic Aggregated Top Destinations for Destination Port report.
 - Conversations for Destination Port: Launches the Interface Traffic Aggregated Top Conversations for Destination Port report.
- c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time the Top N Analysis Report is launched. If you select the topology filter as either Application Name or Type of Service (either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when 'Top N Analysis' report is launched next.


You can set the topology filters using Run Prompts link on the Top N Analysis report. Once selected, the topology filters can only be removed by the Reset feature. However, the specific filters that you can select for a report depend on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.

To check fields that are applicable to filter on a particular report first launch the report and then launch the Topology Selector using the Run Prompts link.

To list the Interface Traffic Aggregated Top N Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.
3. Click  **My Area Options > My Preferences**.
4. Select the option **Show hidden entries**.
5. Click **OK**.

Interface Traffic Aggregated Top Applications by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:
enable.topn.subtypes.tos=true
6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Applications by ToS report is a Top N report. This report shows top applications across the network for a specific ToS value and is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Applications by ToS report defaults to the following values:

- Grouping by = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Conversations for Application Report

The Interface Traffic Aggregated Top Conversations for Application report is a Top N report. This report shows top talkers (source-destination pairs) across the network for a specific application and is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report.

By default, this report shows data grouped by only destination hosts. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Application report defaults to the following values:

- Grouping by = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Conversations by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report

- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Conversations by ToS report is a Top N report. This report shows top talkers (source-destination pairs) across the network for a specific ToS value and is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report.

By default, this report shows data grouped by destination hosts only. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for each conversation. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations by ToS report defaults to the following values:

- Grouping by = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Destinations by Application Report

The Interface Traffic Aggregated Top Destinations by Application report is a Top N report. This report shows top hosts (that receive data packets from different hosts) across the network for a specific application and is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. The report shows top destination hosts for the selected application. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations by Application report defaults to the following values:

- Grouping by = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Sources by Application Report

The Interface Traffic Aggregated Top Sources by Application report is a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow

packets that are mapped to a specific application. This report is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. The report shows top source hosts for the selected application. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by Application report defaults to the following values:

- Grouping by = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Sources by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows


```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Sources by ToS report is a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by ToS report defaults to the following values:

- Grouping by = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Applications Report

The Interface Traffic Aggregated Top Applications report is a Top N report. This report shows top N applications across the network that contribute to the network traffic. The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (avg)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (min)
- Bandwidth - Out Mbps (avg)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (min)
- Bandwidth Utilization (avg)
- Bandwidth Utilization (max)
- Bandwidth Utilization (min)

The Interface Traffic Aggregated Top Applications report defaults to the following values:

- Grouping by = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top / Bottom 'N' = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use NNM iSPI Performance for Traffic Top Conversations report enables you to monitor the top talkers in the environment.

By default, the Interface Traffic Aggregated Top Conversations Report report shows top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of traffic performance indicators for each conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Destinations Report

The Interface Traffic Aggregated Top Destinations report is a Top N report. This report shows top N hosts across the network that receive data packets. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.



Interface Traffic Aggregated Top Interfaces Report

The Interface Traffic Aggregated Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic Aggregated Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (**Add New Grouping**) button. Use the  (**Remove Grouping**) button to remove a grouping attribute.

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Sources Report

The Interface Traffic Aggregated Top Sources report is a Top N report. This report shows top N hosts across the network that send data packets to different destinations. For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top TypeOfService Report

The Interface Traffic Aggregated Top TypeOfService report is a Top N report. This report shows top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking on a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Destination Ports Report

The Interface Traffic Aggregated Top Destination Ports Report presents a Top N report. These reports show top N [destination ports](#)¹ across the network that receive data packets.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated

¹Recipients of data packets

every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destination Ports report defaults to the following values:

- Grouping by Elements = Destination Port
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Sources for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Sources for Destination Port report is a Top N report. This report shows top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port. This report is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Destination Ports report first, select a destination port, and then launch this report.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 day
- Grain = 1 hour
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:
On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Destinations for Destination Port report is a Top N report. This report shows top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top destinations that receive data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic Aggregated Top Conversations for Destination Port report presents a Top N report. This report shows top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only. However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Display Time Series Chart

This option shows the variation of the metric for the different entries in the bar graph over the selected period as a stacked chart graph. The default value is No.

Note: The Display Time Series Chart option runs a time-consuming query. Therefore, it is provided as an option.

Interface Traffic Aggregated Top N Chart Analysis Report

The NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods. The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available Interface Traffic Aggregated Top N Chart Reports

Report	Description
Interface Traffic Aggregated Top Applications for ToS	Displays the top applications across the network for the selected ToS value.
Interface Traffic Aggregated Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.

Report	Description
Interface Traffic Aggregated Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic Aggregated Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.
Interface Traffic Aggregated Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic Aggregated Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.
Interface Traffic Aggregated Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic Aggregated Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.
Interface Traffic Aggregated Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic Aggregated Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic Aggregated Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic Aggregated Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.
Interface Traffic Aggregated Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic Aggregated Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic Aggregated Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.
Interface Traffic Aggregated Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports on the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N Chart reports may prove to be a time consuming and

repetitive process. To overcome this problem, the NNM iSPI Performance for Traffic enables you to select the Top N Chart Analysis report that works as the launching point for all the Interface Traffic Aggregated Top N Chart reports.

To launch the Top N Chart reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic > Interface_Traffic_Aggregated**.
3. Select **Top N Chart Analysis**.
4. In the Select Report Type panel, select the type of the report you want to launch and then click **Confirm Selection**. The default selection is Top Interfaces that launches Interface Interface Traffic Aggregated - Top_Interfaces - Top N Chart Report. The NNM iSPI Performance for Traffic launches the following reports for each option:
 - Top Sources: Launches the Interface Interface Traffic Aggregated - Top_Sources - Top N Chart Report.
 - Top Destinations: Launches the Interface Interface Traffic Aggregated - Destinations_for_Applications - Top N Chart Report.
 - Top Conversations: Launches the Interface Interface Traffic Aggregated - Top_Conversations - Top N Chart Report.
 - Top Type of Services: Launches the Interface Interface Traffic Aggregated - Top_TypeOfService - Top N Chart Report.
 - Top Destination Ports: Launches the Interface Traffic Aggregated_Top - DestinationPorts Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**
 - a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Interface Traffic Aggregated - Sources_for_Application - Top N Chart Report.
 - Destinations for Application: Launches the Interface Interface Traffic Aggregated - Destinations_for_Applications - Top N Chart Report

- Conversations for Application: Launches the Interface Interface Traffic Aggregated - Conversations_for_Application - Top N Chart Report
 - c. Click **Confirm Selection**.
- **Top Type of Service**
 - a. Select **Type of Service**.

Note: The NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:
 - Application for ToS: Launches the Interface Interface Traffic Aggregated - Applications_for_ToS - Top N Chart Report.
 - Sources for ToS: Launches the Interface Interface Traffic Aggregated - Sources_for_ToS - Top N Chart Report.
 - Conversations for ToS: Launches the Interface Interface Traffic Aggregated - Conversations_for_ToS - Top N Chart Report.
 - c. Click **Confirm Selection**.
 - **Top Destination Ports**
 - a. Select **Destination Port**.

Note: The NNM iSPI Performance for Traffic sorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
 - Sources for Destination Port: Launches the Interface Traffic Aggregated Top Sources for Destination Port Chart report.
 - Destinations for Destination Port: Launches the Interface Traffic Aggregated Top Destinations for Destination Port Chart report.
 - Conversations for Destination Port: Launches the Interface Traffic Aggregated Top Conversations for Destination Port Chart report.

c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Chart Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time you launch the Top N Chart Analysis report. If you select the topology filter as either Application Name or Type of Service (either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when you launch the 'Top N Chart Analysis' report next.


You can set the topology filters using Run Prompts link on the Top N Chart Analysis report. Once selected, they can only be removed by the Reset feature. However, the specific filters that you can select for a report depend on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.

To check which are the applicable fields to filter on a particular report, launch the Topology Selector in the context of that report. You must first launch that report and then launch the Topology Selector using the Run Prompts link.

To list the Interface Traffic Aggregated Top N Chart Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.
3. Click  **My Area Options > My Preferences**.
4. Select the option **Show hidden entries**.
5. Click **OK**.

Interface Traffic Aggregated Top Applications by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Applications by ToS report is a Top N Chart report. This report shows line graphs for top applications across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Applications by ToS report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations for Application Report

The Interface Traffic Aggregated Top Conversations for Application report is a Top N Chart report. This report shows line graphs for top talkers (source-destination pairs) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. By default, this report shows data grouped by destination hosts only. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Source Host Name), you can view the Top N values for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Application report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

- Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

- Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

- Open the `nms-traffic-leaf.address.properties` file with a text editor.
- Remove the following line:

enable.topn.subtypes.tos=true

- Save and close the `nms-traffic-leaf.address.properties` file.
- Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Conversations by ToS report is a Top N Chart report. This report shows line graphs for top talkers (source-destination pairs) across the network for a specific ToS value and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. By default, this report shows data grouped by destination hosts only. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations by ToS report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations by Application Report

The Interface Traffic Aggregated Top Destinations by Application report is a Top N Chart report. This report shows line graphs for top hosts (that receive data packets from different hosts) across the network for a specific application and is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. The report shows top destination hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations by Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Sources by Application Report

The Interface Traffic Aggregated Top Sources by Application report is a Top N Chart report. This report shows line graphs for top source hosts (hosts that send out data packets) across the network that generate flow packets that are mapped to a specific application. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. The report shows top source hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by Application report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Sources by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```


On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Sources by ToS report is a Top N Chart report. This report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by ToS report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Applications Report

The Interface Traffic Aggregated Top Applications report is a Top N Chart report. This report shows line graphs for top N applications across the network that contribute to the network traffic.

The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (min)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (avg)
- Bandwidth - Out Mbps (min)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (avg)
- Bandwidth Utilization (min)
- Bandwidth Utilization (max)
- Bandwidth Utilization (avg)

The Interface Traffic Aggregated Top Applications report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use the NNM iSPI Performance for Traffic Top Conversations reports to monitor the top talkers in the environment.

By default, the Interface Traffic Aggregated Top Conversations report shows line graphs for top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of traffic performance indicators for every source-destination pair, or in other words, for every conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations Report

The Interface Traffic Aggregated Top Destinations report is a Top N Chart report. This report shows line graphs for top N hosts across the network that receive data packets.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10



Interface Traffic Aggregated Top Interfaces Report

The Interface Traffic Aggregated Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic Aggregated Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

Interface Traffic Aggregated Top Sources Report

The Interface Traffic Aggregated Top Sources report is a Top N Chart report. This report shows line graphs for top N hosts across the network that send data packets to different destinations.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top TypeOfService Report

The Interface Traffic Aggregated Top TypeOfService report is a Top N Chart report. This report shows line graphs for top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking on a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network

traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destination Ports Report

The Interface Traffic Aggregated Top Destination Ports report presents a Top N Chart report. These reports show line graphs for top N [destination ports](#)¹ across the network that receive data packets.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destination Ports report defaults to the following values:

- Grouping by Elements = Destination Port
- Time Range = Last 1 day
- Grain = 1 hour
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

¹Recipients of data packets

Interface Traffic Aggregated Top Sources for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Add the following lines:


```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Sources for Destination Port report presents a Top N chart report. This report shows line graphs for top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Destinations for Destination Port report presents a Top N chart report. This report shows line graphs for top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the Destination port 160 shows top destinations that receive data packets to the Destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic Aggregated Top Conversations for Destination Port report presents a Top N chart report. This report shows line graphs for top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only.

However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top N Table Analysis Report

The NNM iSPI Performance for Traffic categorizes the traffic data stored in NPS to effectively serve queries and retain larger volume of data for longer time periods.

This report ranks network elements by the metrics you select. Unlike the Top N report, this report does not show any bar charts or time series graphs. In a large environment, NPS can generate the Top N Table report faster than it can generate the Top N report. If you want to view Top N elements in the least possible time, choose the Top N Table report instead of the Top N report.

The following reports enable you to analyze the categorized traffic data based on data retention period, traffic type (traffic mapped to application, ToS, conversations, etc), and the source or destination for the traffic flow:

Available Interface Traffic Aggregated Top N Table Reports

Report	Description
Interface Traffic Aggregated Top Applications for ToS	Displays the top applications across the network for the selected ToS value.

Report	Description
Interface Traffic Aggregated Top Conversations for Application	Displays the top talkers (source-destination pairs) across the network for the selected application.
Interface Traffic Aggregated Top Conversations for ToS	Displays the top talkers (source-destination pairs) across the network for the selected ToS value.
Interface Traffic Aggregated Top Destinations for Applications	Displays the top destination hosts receiving data packets from different hosts across the network for the selected application.
Interface Traffic Aggregated Top Sources for Application	Displays the top hosts (hosts that send out data packets) across the network generating flow packets mapped to the selected application.
Interface Traffic Aggregated Top Sources for ToS	Displays the top source hosts (hosts that send out data packets) across the network generating flow packets with the selected ToS value.
Interface Traffic Aggregated Top Applications	Displays the top N applications across the network that contribute to the network traffic.
Interface Traffic Aggregated Top Conversations	Displays the top talkers (source-destination pairs) across the network. You can use this report to monitor the flow of data between two hosts.
Interface Traffic Aggregated Top Destinations	Displays the top N hosts across the network receiving the largest volume of data packets.
Interface Traffic Aggregated Top Interfaces	Displays the top N interfaces across the network with largest incoming and outgoing traffic volume.
Interface Traffic Aggregated Top Sources	Displays the top N hosts across the network sending largest volume of data packets to different destinations.
Interface Traffic Aggregated Top TypeOfService	Displays the top contributors to traffic based on selected Type of Service (ToS) values.
Interface Traffic Aggregated Top Destination Ports	Displays the top N destination ports that are receiving largest volume of data packets across the network.
Interface Traffic Aggregated Top Sources for Destination Port	Displays the top source hosts sending data packets to the selected destination port.
Interface Traffic Aggregated Top Destinations for Destination Port	Displays the top destinations hosts receiving data packets on the selected destination port.

Report	Description
Interface Traffic Aggregated Top Conversation for Destination Port	Displays the top talkers across the network for the selected destination port.

Listing all the available reports on the NPS Home Page may cause considerable usability problem. Selecting between various types of Top N Table reports may prove to be a time consuming and repetitive process. To overcome this problem, NNM iSPI Performance for Traffic enables you to select the Top N Table Analysis report, that works as the launching point for all the Aggregated Top N Table reports.

To launch the Top N Table reports:

1. In the NPS console, go to the Reports workspace.
2. Click **iSPI Traffic > Interface_Traffic > Interface_Traffic_Aggregated**.
3. Select **Top N Table Analysis**.
4. In the Select Report Type panel, select the type of the report you want to launch, and then click **Confirm Selection**. The default selection is Top Interfaces that launches Interface Traffic Aggregated - Top_Interfaces - Top N Table Report. The NNM iSPI Performance for Traffic launches the following reports for each option:
 - Top Interfaces: Launches the Interface Traffic Aggregated - Top_Interfaces - Top N Table Report.
 - Top Applications: Launches the Interface Traffic Aggregated - Top_Applications - Top N Table Report.
 - Top Sources: Launches the Interface Traffic Aggregated - Top_Sources - Top N Table Report.
 - Top Destinations: Launches the Interface Traffic Aggregated - Destinations_for_Applications - Top N Table Report.
 - Top Conversations: Launches the Interface Traffic Aggregated - Top_Conversations - Top N Table Report.
 - Top Type of Services: Launches the Interface Traffic Aggregated - Top_TypeOfService - Top N Table Report.
 - Top Destination Ports: Launches the Interface Traffic Aggregated_Top - DestinationPorts Report.

Follow these steps **only** if you have selected any of the following options:

- **Top Applications**
 - a. Select **Application Name**.

Note: The NNM iSPI Performance for Traffic sorts the list of applications alphabetically.

The NNM iSPI Performance for Traffic sets the application name to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected application:
 - Sources for Application: Launches the Interface Traffic Aggregated - Sources_for_Application - Top N Table Report.
 - Destinations for Application: Launches the Interface Traffic Aggregated - Destinations_for_Applications - Top N Table Report
 - Conversations for Application: Launches the Interface Traffic Aggregated - Conversations_for_Application - Top N Table Report
- c. Click **Confirm Selection**.

- **Top Type of Service**
 - a. Select **Type of Service**.

Note: NNM iSPI Performance for Traffic sorts the list of type of services alphabetically.

The NNM iSPI Performance for Traffic sets the selected type of service to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected type of service:
 - Application for ToS: Launches the Interface Traffic Aggregated - Applications_for_ToS - Top N Table Report.
 - Sources for ToS: Launches the Interface Traffic Aggregated - Sources_for_ToS - Top N Table Report.
 - Conversations for ToS: Launches the Interface Traffic Aggregated - Conversations_for_ToS - Top N Table Report.
- c. Click **Confirm Selection**.

- **Top Destination Ports**
 - a. Select **Destination Port**.

Note: NNM iSPI Performance for Traffic sorts the list of destination ports alphabetically.

The NNM iSPI Performance for Traffic sets the selected destination port to analyze the report data.

- b. Select any of the following Topology Filters to filter the traffic mapped to the selected destination port:
 - Sources for Destination Port: Launches the Interface Traffic Aggregated Top Sources for Destination Port Table report.
 - Destinations for Destination Port: Launches the Interface Traffic Aggregated Top Destinations for Destination Port Table report.
 - Conversations for Destination Port: Launches the Interface Traffic Aggregated Top Conversations for Destination Port Table report.
- c. Click **Confirm Selection**.

Top Interfaces is the default option for the Top N Table Analysis report. The NNM iSPI Performance for Traffic selects this option automatically every time you launch the Top N Table Analysis Report. If you select the topology filter as either Application Name or Type of Service (either using the Topology Filter tab or using the drill-down option), then the NNM iSPI Performance for Traffic automatically selects the corresponding report-type (Top Application or Top ToS), when 'Top N Table Analysis' report is launched next.


You can set the topology filters using Run Prompts link on the Top N Table Analysis report. Once selected, they can only be removed by the Reset feature. However, the specific filters that you can select for a report depends on the type of data the report displays. For example, even if you have set the topology filter as Application Name, for the Top ToS report, the NNM iSPI Performance for Traffic does not use the filter you have set, as Application Name is not included in the Topology Selector of the Top ToS report.

To check which are the applicable fields to filter on a particular report launch the Topology Selector in the context of that report. Launch that report first and then launch the Topology Selector using the Run Prompts link.

To list the Interface Traffic Aggregated Top N Table Reports in the BI Portal:

The Interface Traffic Aggregated Top N reports are hidden in the BI Server Public Folders by default. If you select **BI Server** on the NPS Home Page, select **Public Folders > iSPI Traffic**, and then select **Interface_Traffic_Aggregated** folder, you cannot see these folders listed.

To view these reports in the Public Folders, follow these steps:

1. Click **BI Server** on the NPS Home Page.
2. Click **Portal** to launch HP NNM iSPI Performance BI Portal.
3. Click  **My Area Options > My Preferences**.

4. Select the option **Show hidden entries**.
5. Click **OK**.

Interface Traffic Aggregated Top Applications by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The report shows top applications for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top applications that contributed with the maximum amount of data to the network traffic characterized by the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Applications by ToS report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

```
enable.topn.subtypes.tos=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

By default, the Interface Traffic Aggregated Top Conversation by ToS report shows data grouped by destination hosts only. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top talkers contributing to network traffic with the ToS value 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations by ToS report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations for Application Report

By default, the Interface Traffic Aggregated Top Conversations for Application report shows data grouped by destination hosts only. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of for every source-destination pair, or in other words, for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top talkers that contribute to the SNMP network traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations by Application Report

The report shows top destination hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows the hosts that received the maximum amount of data (in bytes) for SNMP.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations by Application report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Sources by Application Report

The Interface Traffic Aggregated Top Sources by Application report shows line graphs for top source hosts (hosts that send out data packets) across the network that generate flow packets that are mapped to a specific application. The report is generated using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top Applications report first, select an application, and then launch this report. The report shows top source hosts for the selected application.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the application SNMP shows top hosts that sent the maximum amount of the SNMP traffic.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by Application report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Sources by ToS Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable the data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Remove the following line:

enable.topn.subtypes.tos=true

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Applications by ToS report
- The Interface Traffic Aggregated Top Sources by ToS report
- The Interface Traffic Aggregated Top Conversations by ToS report

The Interface Traffic Aggregated Top Sources by ToS report shows top source hosts (hosts that send out data packets) across the network that generate flow packets with a specific ToS value. The report is generated by using the contextual navigation feature of the NPS. Therefore, HP recommends that you launch the Interface Traffic Aggregated Top TypeOfService report first, select a ToS value, and then launch this report. The report shows top source hosts for the selected ToS value.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the ToS value 25 shows top hosts that sent the maximum amount of data (in bytes) for the flow packets with the ToS value of 25.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources by ToS report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Applications Report

The report shows line graphs for top N applications across the network that contribute to the network traffic.

The NNM iSPI Performance for Traffic provides you with predefined application definitions. You can use the NNM iSPI Performance for Traffic Configuration form to modify the existing application definitions or create new application definitions.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Top Applications report enables you to choose the following additional bandwidth metrics that are not available with other reports:

- Bandwidth - In Mbps (min)
- Bandwidth - In Mbps (max)
- Bandwidth - In Mbps (avg)
- Bandwidth - Out Mbps (min)
- Bandwidth - Out Mbps (max)
- Bandwidth - Out Mbps (avg)
- Bandwidth Utilization (min)
- Bandwidth Utilization (max)
- Bandwidth Utilization (avg)

The Interface Traffic Aggregated Top Applications report defaults to the following values:

- Grouping by Elements = Application Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations Report

A **conversation** means the flow of data between two hosts. You can use NNM iSPI Performance for Traffic Top Conversations reports to monitor the top talkers in the environment.

By default, the Interface Traffic Aggregated Top Conversations report shows line graphs for top N hosts across the network that receive data packets. However, if you add Source Host Name as the 'Grouping By' metric (while retaining the original 'Grouping By' metric Destination Host Name), you can view the Top N values of traffic performance indicators for every source-destination pair, or in other words, for every conversation.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations Report

The Interface Traffic Aggregated Top Destinations report shows line graphs for top N hosts across the network that receive data packets.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (recipients of data packets) that received the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10



Interface Traffic Aggregated Top Interfaces Report

The Interface Traffic Aggregated Top Interfaces report ranks flow-enabled interfaces or nodes by the metric you select. Use this report to spot the interface or node that performed at the extremes. You can use this report to analyze the historical data for elements that are exhibiting unusual utilization levels.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The Interface Traffic Aggregated Top Interfaces report defaults to the following values:

- Grouping by Elements = Qualified Interface Name
- Start Date/Time = Depends on default Time Range and data available in the database
- Time Range = Last 1 hour
- Hour of Day = All
- Day of Week = All
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

By default, the report groups data by Qualified Interface Name. You can select multiple grouping attributes by using the  (Add New Grouping) button. Use the  (Remove Grouping) button to remove a grouping attribute.

Interface Traffic Aggregated Top Sources Report

The Interface Traffic Aggregated Top Sources report shows line graphs for top N hosts across the network that send data packets to different destinations.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows hostnames of Top N hosts (senders of data packets) that sent maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top TypeOfService Report

The Interface Traffic Aggregated Top TypeOfService report shows line graphs for top contributors to traffic based on Type of Service (ToS) values across the network.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics shows ToS values of flow packets (ingress and egress) with the maximum amount of data (in bytes).

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

You can further set a filter by clicking on a top Type of Service value, and then analyze further.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top TypeOfService report defaults to the following values:

- Grouping by Elements = Type of Service
- Time Range = Last 1 hour
- Grain = 5 minutes

- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destination Ports Report

These reports show line graphs for top N [destination ports](#)¹ across the network that receive data packets.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as -1 on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destination Ports report defaults to the following values:

- Grouping by Elements = Destination Port
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Sources for Destination Port Reports

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

¹Recipients of data packets

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.

2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMi.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Sources for Destination Port report presents a Top N table report. This report shows tabular data for top source hosts (hosts that send out data packets) across the network that send flow packets to a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top sources that send data packets to the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as *Anonymous* on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Sources for Destination Port report defaults to the following values:

- Grouping by Elements = Source Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Destinations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:
On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.

5. Add the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:
On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.

5. Remove the following lines:

```
topn.subtypes.dstport=true
```

```
enable.srcordst.dstport=true
```

6. Save and close the nms-traffic-leaf.address.properties file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMi.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

If you enable or disable data collection by using the steps given above, it will apply to all the three reports listed below:

- The Interface Traffic Aggregated Top Sources for Destination Port report
- The Interface Traffic Aggregated Top Destinations for Destination Port report
- The Interface Traffic Aggregated Top Conversations for Destination Port report

The Interface Traffic Aggregated Top Destinations for Destination Port report presents a Top N table report. This report shows tabular data for top destination hosts (hosts that receive data packets) across the network that receive flow packets on a specific Destination port.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top destinations that receive data packets on the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as Anonymous on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Destinations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

Interface Traffic Aggregated Top Conversations for Destination Port Report

By default, data collection for this report is disabled. Enabling data collection for this report may have an impact on the performance of NNM iSPI Performance for Traffic. To enable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %TrafficDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the nms-traffic-leaf.address.properties file with a text editor.
5. Add the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.

7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

To disable data collection for this report, follow these steps:

1. Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
2. Stop the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%TrafficInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

In this instance, `%NNMInstallDir%` is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

3. Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

In this instance, `%TrafficDataDir%` is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMDataDir%\nmsas\traffic-leaf\conf
```

In this instance, %NNMDataDir% is the NNM iSPI Performance for Traffic data directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Remove the following line:

```
topn.subtypes.dstport=true
```

6. Save and close the `nms-traffic-leaf.address.properties` file.
7. Restart the Leaf Collector by running the following command:

On Windows

```
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %TrafficInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is not installed on the same system as NNMI.

```
%NNMInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

In this instance, %NNMInstallDir% is the NNM iSPI Performance for Traffic install directory when the Leaf Collector is installed on the same system as NNMI.

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

The Interface Traffic Aggregated Top Conversations for Destination Port report presents a Top N table report. This report shows tabular data for top talkers across the network for a specific Destination port. By default, this report shows data grouped by Destination Host Name only. However, if you add Source Host Name as the 'Grouping By' metric, you can view the Top N values for every conversation.

For example, the report drawn with the Volume - In Bytes (sum) and Volume - Out Bytes (sum) metrics for the destination port 160 shows top talkers that contribute to the network traffic on the destination port 160.

You can choose a rank number of 5, 10, 25, 50, and 100. The report enables you to see Top N or Bottom N report of the selected metrics. For the bottom N selection, the report shows the bottom N records from the top contributors data retained by the NNM iSPI Performance for Traffic.

The NNM iSPI Performance for Traffic calculates the top contributors, such as sources, destinations, and applications, to network traffic per interface. The top contributors are calculated

every five minutes and the data is preserved. Data about the less significant contributors to network traffic is aggregated and displayed as *Anonymous* on these reports. The above processing is done on every flow-enabled interface.

The Interface Traffic Aggregated Top Conversations for Destination Port report defaults to the following values:

- Grouping by Elements = Destination Host Name
- Time Range = Last 1 hour
- Grain = 5 minutes
- Metrics = Volume - In Bytes (sum), Volume - Out Bytes (sum)
- Top N Option = Top 10

We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Reports Online Help (Network Node Manager iSPI Performance for Traffic Software 10.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.