

INTELBRAS Intelligent Management Center Network Traffic Analyzer Administrator Guide

Preface

The *INTELBRAS INC Network Traffic Analyzer Administrator Guide* includes 15 chapters, which describe how to configure NTA to process data and present reports, generic configuration procedures, and important parameters.

This preface includes the following topics about the documentation:

- [Audience.](#)
- [Conventions.](#)
- [About the INTELBRAS INC documentation set.](#)
- [Obtaining documentation.](#)
- [Technical support.](#)

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the INTELBRAS INC.

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in the documentation are for illustration only and might be unavailable on your device.

Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	An alert that provides helpful information.

About the INTELBRAS INC documentation set

The INTELBRAS INC documentation set includes the following categories of documents:

Category	Documents	Purposes
Hardware specifications and installation	INTELBRAS INC Getting Started Guide	Quickly guides you through the INC main features and troubleshooting common problems.
	INTELBRAS INC Centralized Deployment Guide with Embedded Database	Provides a complete guide to INC platform and components installation and centralized deployment using embedded database.
	INTELBRAS INC Centralized Deployment Guide with Local Database	Provides a complete guide to INC platform and components installation and centralized deployment using local database.
	INTELBRAS INC Centralized Deployment Guide with Remote Database	Provides a complete guide to INC platform and components installation and centralized deployment using remote database.
	INTELBRAS INC Distributed Deployment Guide with Local Database	Provides a complete guide to INC platform and components installation and distributed deployment using local database.
	INTELBRAS INC Distributed Deployment Guide with Remote Database	Provides a complete guide to INC platform and components installation and distributed deployment using remote database.
	INTELBRAS INC Probe Installation Guide	Provides a complete guide to INC Probe installation and deployment.
	SQL Server 2008 Installation and Configuration Guide	Guides you through installing SQL Server 2008 for INC.
	SQL Server 2008 R2 Installation and Configuration Guide	Guides you through installing SQL Server 2008 R2 for INC.
	SQL Server 2012 Installation and Configuration Guide	Guides you through installing SQL Server 2012 for INC.
	SQL Server 2014 Installation and Configuration Guide	Guides you through installing SQL Server 2014 for INC.
	Oracle 11g Installation and Configuration	Guides you through installing Oracle 11g on Linux for INC.

Category	Documents	Purposes
	Guide(for Linux)	
	Oracle 11g R2 Installation and Configuration Guide(for Linux)	Guides you through installing Oracle 11g R2 on Linux for INC.
	Oracle 12c Installation and Configuration Guide(for Linux)	Guides you through installing Oracle 12c on Linux for INC.
	Red Hat Enterprise Linux 6.4 Installation Guide	Guides you through installing Red Hat Enterprise Linux 6.4 for INC.
	Red Hat Enterprise Linux 7.0 Installation Guide	Guides you through installing Red Hat Enterprise Linux 7.0 for INC.
Software configuration	INTELBRAS INC Enterprise and Standard Platform Administrator Guide	Describes operation procedures on the INC platform.
	INTELBRAS INC Quality of Service Manager Administrator Guide	Describes operation procedures on the INC Quality of Service Manager.
	INTELBRAS INC Resource Automation Manager Administrator Guide	Describes operation procedures on the Resource Automation Manager.
	INTELBRAS INC Service Health Manager Administrator Guide	Describes operation procedures on the Service Health Manager.
	INTELBRAS INC VAN Connection Manager Administrator Guide	Describes operation procedures on the INC VAN Connection Manager.
	INTELBRAS INC VAN Software Defined Network Manager Administrator Guide	Describes operation procedures on the INC VAN Software Defined Network Manager.
	INTELBRAS INC VAN Fabric Manager Administrator Guide	Describes operation procedures on the INC VAN Fabric Manager.
	INTELBRAS INC Application Manager Administrator Guide	Describes operation procedures on the INC Application Manager.
	INTELBRAS INC Branch Intelligent Management System Administrator Guide	Describes operation procedures on the INC Branch Intelligent Management System.
	INTELBRAS INC Business Service Manager Administrator Guide	Describes operation procedures on the INC Business Service Manager.
	INTELBRAS INC IPsec VPN Manager Administrator Guide	Describes operation procedures on the INC IPsec VPN Manager.
	INTELBRAS INC MPLS VPN Manager Administrator Guide	Describes operation procedures on the INC MPLS VPN Manager.
	INTELBRAS INC Network	Describes operation procedures on the INC

	Traffic	

Category	Documents	Purposes
	Analyzer Administrator Guide	Network Traffic Analyzer.
	INTELBRAS INC Service Operation Manager Administrator Guide	Describes operation procedures on the INC Service Operation Manager.
	INTELBRAS INC User Behavior Auditor Administrator Guide	Describes operation procedures on the INC User Behavior Auditor.
	INTELBRAS INC UC Health Manager Admin Guide	Describes operation procedures on the INC UC Health Manager.
	INTELBRAS INC Wireless Service Manager Administrator Guide	Describes operation procedures on the INC Wireless Service Manager.
	INTELBRAS INC User Access Manager Administrator Guide	Describes operation procedures on the INC User Access Manager.
	INTELBRAS INC TACACS+ Authentication Manager Administrator Guide	Describes operation procedures on the INC TACACS+ Authentication Manager.
	INTELBRAS INC EAD Security Policy Administrator Guide	Describes operation procedures on the INC EAD Security Policy Manager.
	Online Help	Helps you properly use INC.
Operations and maintenance	Release Notes	Provides most recent INC release information.

Obtaining documentation

To access the most up-to-date INTELBRAS product documentation, go to the INTELBRAS website at <http://www.intelbras.com.br>

Technical support

service@intelbras.com

<http://www.intelbras.com.br>

Contents

Introduction to Network Traffic Analyzer	1
NTA data source overview	1
NTA and network flow record collection overview	3
NTA and network flow record processing overview	4
NTA server configuration	4
Traffic analysis task management	5
Application, protocol, and application category management	6
Filtering strategies	6
NTA parameter settings	7
Network behavior anomaly detection	7
NTA widgets	9
NTA views	9
Entering the default perspective	9
Entering the desktop view	9
Entering the quick service process	10
Lower-level INC	10
Viewing a lower-level NTA server	10
Viewing traffic analysis task reports on a lower-level NTA server	10
Analyzing the network traffic between virtual machines	11
Configuring NTA for traffic analysis and auditing	12
Managing NTA data sources	12
Device management	13
Probe management	19
Managing NTA servers	22
Viewing the NTA server list	22
Viewing the NTA server details page	23
Modifying an NTA server configuration	24
Redeploying the NTA server configuration	25
Capturing an NTA server flux log	26
Managing applications in NTA	26
Managing applications	27
Managing protocols	34
Managing application categories	37
Configuring NTA traffic analysis parameters	42
Basic and advanced settings	42
Collaborating with the platform topology	44
Using NTA filtering strategies	47
Viewing the filter strategy list	48
Viewing the filter condition list	48
Adding a filter strategy	49
Modifying a filter strategy	51
Deleting a filter strategy	53
Database space management	53
Viewing current disk space usage statistics	53
Viewing database usage trend statistics	54
Data export	54
Viewing the data export config list	55
Querying the data export logs	55
Modifying the data export configuration	56
Auditing the exported data	56
Anomaly detection management	56
Viewing the anomaly detection list	57
Modifying an anomaly template that uses the common parameters	58
Modifying an anomaly template that uses anomaly type-specific parameters	58

Host session monitoring	60
Host session monitoring overview	60
Host session monitoring reporting	60
Host session monitoring configuration considerations	60
Managing host session monitoring	60
Setting threshold alarm parameters for host sessions	60
Viewing host session monitor reports	61
Navigating to the host session monitor reports	62
Summary reports for host sessions	62
Detailed reports for host sessions	63
Interface monitoring	68
Interface traffic analysis overview	68
Interface traffic analysis reporting overview	68
Interface traffic analysis configuration considerations	69
Managing interface traffic analysis tasks	70
Viewing a traffic analysis task	70
Viewing interface traffic analysis task details	71
Adding an interface traffic analysis task	72
Modifying an interface traffic analysis task	76
Deleting an interface traffic analysis task	80
Adding an interface traffic analysis task by using the detection function	80
Viewing interface traffic analysis reports	81
Navigating to the interface traffic analysis reports	81
Summary reports for all interface tasks	81
Detailed reports for an interface traffic analysis task	84
VLAN/VXLAN monitoring	117
VLAN/VXLAN traffic analysis overview	117
VLAN/VXLAN traffic analysis reporting overview	117
VLAN/VXLAN traffic analysis configuration considerations	118
Managing VLAN/VXLAN traffic analysis tasks	119
Viewing VLAN/VXLAN traffic analysis tasks	119
Viewing VLAN/VXLAN traffic analysis task details	120
Adding a VLAN/VXLAN traffic analysis task	121
Modifying a VLAN/VXLAN traffic analysis task	122
Deleting a VLAN/VXLAN traffic analysis task	123
Viewing VLAN/VXLAN traffic analysis reports	123
Navigating to VLAN/VXLAN traffic analysis reports	124
Summary reports for all VLAN/VXLAN traffic analysis tasks	124
Detailed reports for a VLAN/VXLAN traffic analysis task	126
Probe monitoring	156
Probe traffic monitoring overview	156
Probe traffic analysis reporting overview	156
Probe traffic analysis configuration considerations	157
Managing probe traffic analysis tasks	157
Viewing a traffic analysis task	157
Viewing probe traffic analysis task details	158
Adding a probe traffic analysis task	159
Modifying a probe traffic analysis task	161
Deleting a probe traffic analysis task	162
Viewing probe traffic analysis reports	162
Navigating to the probe traffic analysis reports	163
Summary reports for all probe tasks	163
Detailed reports for a probe traffic analysis task	164
Application monitoring	193
Application traffic analysis overview	193
Application traffic analysis reporting overview	193
Application traffic analysis configuration considerations	194

Managing application traffic analysis tasks	194
Viewing a traffic analysis task	195
Viewing application traffic analysis task details	195
Adding an application traffic analysis task	197
Modifying an application traffic analysis task	201
Deleting an application traffic analysis task	205
Viewing application traffic analysis reports	205
Navigating to the application traffic analysis reports	205
Summary reports for all application tasks	205
Detailed reports for an application traffic analysis task	207
Host monitoring	221
Host traffic analysis overview	221
Host traffic analysis reporting overview	221
Host traffic analysis configuration considerations	223
Managing host traffic analysis tasks	223
Viewing a traffic analysis task	223
Viewing host traffic analysis task details	224
Adding a host traffic analysis task	225
Modifying a host traffic analysis task	230
Deleting a host traffic analysis task	235
Viewing host traffic analysis reports	235
Navigating to the host traffic analysis reports	235
Summary reports for all host tasks	236
Detailed reports for a host traffic analysis task	237
VPN monitoring	269
VPN traffic analysis overview	269
VPN traffic analysis reporting overview	269
VPN traffic analysis configuration considerations	270
Managing VPN traffic analysis tasks	271
Viewing a traffic analysis task	271
Viewing VPN traffic analysis task details	271
Adding a VPN traffic analysis task	272
Modifying a VPN traffic analysis task	274
Deleting a VPN traffic analysis task	275
Viewing VPN traffic analysis reports	275
Navigating to the VPN traffic analysis reports	275
Summary reports for all VPN tasks	276
Granular reports for a VPN traffic analysis task	278
Interbusiness monitoring	305
Interbusiness traffic analysis overview	305
Interbusiness traffic analysis reporting overview	305
Interbusiness traffic analysis configuration issues	306
Managing interbusiness traffic analysis tasks	306
Viewing a traffic analysis task	306
Viewing traffic analysis task details	307
Adding an interbusiness traffic analysis task	307
Modifying a traffic analysis task	311
Deleting a traffic analysis task	314
Viewing interbusiness traffic analysis reports	314
Navigating to the interbusiness traffic analysis reports	314
Summary reports for all interbusiness traffic analysis tasks	314
Granular reports for an interbusiness traffic analysis task	315
BGP AS monitoring	324
BGP AS traffic analysis overview	324
BGP AS traffic analysis reporting overview	324
BGP AS traffic analysis configuration considerations	325
Managing BGP AS traffic analysis tasks	326
Viewing BGP AS traffic analysis tasks	326

Viewing BGP AS traffic analysis task details	326
Adding a BGP AS traffic analysis task	328
Modifying a BGP AS traffic analysis task	330
Deleting a BGP AS traffic analysis task	332
Viewing BGP AS traffic analysis reports	332
Navigating to the BGP AS traffic analysis reports	332
Summary reports for all BGP AS traffic analysis tasks	333
Detailed reports for a BGP AS traffic analysis task	334
Performing traffic log audits in NTA	360
Configuring NTA for traffic log auditing	360
Adding data sources to NTA	360
Selecting the device or probe	361
Configuring the aggregation policy	362
Creating an interface, probe, or VPN traffic analysis task	362
Performing a traffic log audit	363
Viewing traffic log audit reports	364
Source host reports	364
Destination host reports	366
Session reports	368
NTA reports	371
NTA widgets	373
Dashboard widgets	373
Configuring the dashboard display	374
Configuring dashboard widget parameters	374
Viewing the display effect	375
Home page widgets	376
Configuring home page widget parameters	376
Viewing the display effect	377
Analyzing traffic between virtual machines	379
Deploying a probe on a virtual machine	380
Setting the network configuration for a virtual machine network adapter	381

Introduction to Network Traffic Analyzer

The NTA service module integrates Layer 4 through Layer 7 network monitoring into the INC network management platform. NTA uses the instrumentation in network devices such as routers and switches to provide realtime and historical reporting on network application usage. Administrators tailor NTA data collection and reporting capabilities to meet specific reporting needs. Administrators and operators view NTA reports directly from the INC integrated platform.

NTA combines the features of a network flow collector with a data analysis and processing engine and database, and a reporting facility for presenting network flow data in INC. Like most network monitoring systems, NTA enables administrators to define the data received by NTA, the data that is analyzed and how, and the data that is presented.

NTA enables you to view the network flow data provided by the devices in your network. Out-of-the-box configuration of NTA provides network flow data collection, analysis, and reporting. NTA users must have an understanding of network flow records and the devices in the environment that generate network flow records. Users must also know how to configure NTA to process the data and present reports.

NTA data source overview

NTA uses network flow data to generate network resource statistics. An IP flow, commonly called a flow, is defined as a set of IP packets passing an observation point in the network during a specified time interval. All packets that belong to a flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the observation point (see RFC 5101, RFC 3917, and RFC 3954).

An IP network flow contains a stream of IP packets that share, at a minimum, the following parameters during a specified time period:

- Source and destination IP addresses
- Source and destination ports
- Layer 4 protocol (TCP, UDP, or ICMP)

This general definition does not include technologies, such as TCP, which identify flows for bidirectional protocols. Vendors can add parameters to further identify network flows in the implementations of network flow technologies.

Network device vendors implement network flow technologies in devices such as routers and switches that forward packets from source to destination. Devices that generate network flow records are called flow generators. Flow generators summarize the packets they observe as part of a flow into a flow record.

The structure and contents of a network flow record may vary, depending on the standard to which the implementation adheres. Also, proprietary implementations may have their own definitions for the structure and content of a network flow record. As a general rule, a network flow record shares several of the following parameters:

- Version number
- Sequence number
- Indexes of input and output interfaces (ifIndex)
- Timestamps for flow start and finish
- Number of bytes
- Number of packets
- Layer 3 and Layer 4 header information, including source and destination IP addresses and port numbers, IP protocol, and Type of Service (ToS) value

- TCP flag summary information
- Layer 3 routing information

The data available in network flow records and the data available in protocol analysis and other diagnostic tools differ. Network flow records provide a summary of the information contained in layers 4 through 7 of a network flow rather than the contents of the IP packets that constitute a flow. Information found in layers 1 through 3 is usually discarded in network flow implementations. As a result, systems such as NTA that use network flow records provide summarized data based on the contents of layers 4 through 7 in IP packets.

Network flow data is an efficient and cost-effective way to provide administrators and network operators with visibility into network resource usage, which helps them identify many issues and usage trends. It is not, however, a packet inspection or deep diagnostic tool such as a protocol analyzer, which is more commonly used for diagnosing and pinpointing problems at all seven layers of an IP network.

Network flow generators forward or push network flow records to an external device called a flow collector that aggregates and processes network flow information. NTA is a network flow collector for IP traffic information. NTA supports most standard IP network flow monitoring protocols including NetStream v5/v9, NetFlow v5/v9, and sFlow v5.

NetStream is an HPE network traffic collection technique that includes three versions: v5, v8, and v9. The most frequently used versions are v5 and v9. NTA can receive and analyze NetStream packets in v5 or v9 format. NetStream v5 defines a flow by the 7-tuple elements of IP packets, and it does not support aggregation data export. NetStream v9 defines a flow by the 7-tuple elements of IP packets, and it supports aggregation data export and MPLS packet statistics.

NetStream supports two traffic statistics collection modes:

- **Accurate statistics collection mode**—The router or switch collects statistics for each IP packet passing through. The collected statistics are accurate. This mode requires high device performance.
- **Sampled statistics collection mode**—The router or switch samples the IP packets passing through. The collected statistics are not accurate. This mode requires low device performance.

With NetFlow technologies, the routers and switches track all inbound conversations on each interface on which NetFlow is enabled. A NetFlow-enabled router or switch examines each packet based on the following key fields:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- ToS
- Input/Output interface

If packets share identical contents in each of the seven fields, the router or switch assumes these packets are part of the same flow. The NetFlow router or switch then summarizes the conversation, generates a NetFlow record, and forwards it to the NetFlow collector. One NetFlow packet can contain summarized details for as many as 24 to 30 conversations. When a NetFlow-enabled router or switch is configured properly and the router or switch is not overloaded, NetFlow data can achieve 100% accuracy.

Like NetFlow, sFlow also summarizes traffic into a network flow record that it pushes to a collector. It is also a technology that is implemented in devices, such as routers and switches, which forward traffic from source to destination.

Unlike NetFlow, however, sFlow is implemented in hardware with a dedicated chip that performs the flow analysis and processing. For this reason, sFlow technologies introduce much less load onto the router or switch on which sFlow is enabled.

Another key difference between NetFlow and sFlow is that sFlow does not analyze every packet in a flow but rather statistically samples every n th packet. As a result, sFlow data is often considered to be less accurate than NetFlow data.

When you use routers or switches to collect network traffic statistics, they must support NetFlow, NetStream, or sFlow. If a device does not support any of these protocols, configure port mirroring on it to mirror the network traffic to be analyzed to a probe server. The server is deployed a probe application program to collect statistics of the received mirrored traffic and generate probe traffic logs. The probe server then uploads the probe traffic logs to the NTA server. NTA analyzes the network traffic based on the received probe traffic logs.

The HPE probe servers include Linux servers with probe application programs installed and vMON virtual machines. A probe application program must be installed on a physical or virtual Linux server. It collects statistics of the received traffic of a physical or virtual network. A vMON is an OVF template with an embedded probe application program and can be deployed on a VMware virtual server. It collects statistics of the received traffic of a virtual network.

NTA and network flow record collection overview

To configure NTA and devices to collect a record of network flow data:

1. Identify the areas of interest for which you want to capture network flow data.

This may include business services, applications, or systems and the underlying technologies that deliver these services, and network devices or interfaces, servers, storage, or other network resources.

When you identify where you want to capture network flow data, develop a plan to enable network flow data. Segments of the network that are often valuable from a network flow collection perspective include network ingress and egress points, aggregation points, and server farms.

2. Identify all the devices in the network that are capable of generating network flow records.

The network flow data protocols that NTA supports and for which it can process flow records are NetStream v5/v9, NetFlow v5/v9, and sFlow v5. You must determine whether the devices that are network flow capable are compatible with the versions supported by NTA. Routers and switches are the most likely candidates for network flow capable devices.

3. Perform a gap analysis of the areas in your network that are network flow data capable and those that are not.

Do this by mapping the areas from step 1 to the device inventory you created in step 2. This enables you to identify the areas for which you can collect network flow data and those areas that you cannot.

This analysis provides the following important planning aids:

- A list of the devices and their interfaces for which you enable network flow data.
- A list of the devices and areas in your network that have no instrumentation.

Identifying the areas that have no network flow instrumentation helps determine if you can use alternatives, such as a probe server.

4. Configure devices that have network flow capabilities to forward network flow data for the interfaces.

In this step, enable network flow data collection. You can also configure on which interfaces network flow collection should be enabled.

You need to configure these devices to forward network traffic flow data to the NTA server that functions as a network flow collector. Therefore, in addition to enabling network flow data on each of these devices, you configure the NTA server as the flow collector on these devices.

See the vendor documentation for the NTA server configuration to forward network flow records. The NTA server may be an INC platform server that has the NTA service module deployed on

it. Otherwise, it may be a server that is configured as a dedicated NTA server that communicates with an INC platform server in a distributed INC deployment.

5. As an option, you can configure port mirroring on the routers or switches that do not support any of the NetStream v5/v9, NetFlow v5/v9, or sFlow v5 protocols. Then, the traffic can be mirrored to the port connecting to the probe server. You can manage the probes in NTA and configure the probes to send the traffic logs to the NTA server.
6. After you complete the configuration of all network flow data devices, configure the NTA server to receive and process the network flow records from every device you have configured.

For routers, switches, network flow probes and other devices that support NetStream v5/v9, NetFlow v5/v9, or sFlow v5, use the **Device Management** feature under the **Settings** area of NTA.

For more information on using **Device Management** to configure NTA to receive network flow data records for, see "[Device management](#)."

7. Configure the NTA server to receive and process the network flow records from every probe server you have installed. Use the **Probe Management** feature under the **Settings** area to add probes to NTA.

For more information on using **Probe Management** to configure NTA to receive network flow data records from probe servers, see "[Probe management](#)."

NTA provides administrators with access to modify the configuration of an NTA server. From the server configuration page, modify the following NTA server settings:

- o Server description
- o Port used by NTA to receive flow records
- o FTP access information
- o Traffic analysis log aggregation policy
- o Filter policy
- o Disk space usage threshold
- o Action to take when the disk space usage threshold is reached

You can also enable and disable NTA processing of flow records from devices and probes on this page. For more information on configuring these features, see "[Managing NTA servers](#)."

After you complete these steps, NTA is configured to receive network flow records. However, NTA does not begin processing or analyzing flow records for any source until you create a traffic analysis task.

NTA and network flow record processing overview

You must select the probes and devices for which you want to process data, and you must configure traffic analysis tasks; otherwise, NTA ignores all forwarded network flow records. The administrators can use the NTA features to configure if, what, and how network flow records are processed. These features include NTA server management, traffic analysis task management, application and category management, NTA filter strategies, and parameter settings. This section provides an overview of each of these features and describes how you use them to configure NTA to process network flow records.

NTA server configuration

Using the features described in "[Device management](#)" and "[Probe management](#)," you can configure devices and probes to establish communication paths between NTA and the devices in your infrastructure that you have enabled for network flow record generation. After you add a device or probe, select the probes and devices for which you want to process data, as described in "[Modifying an NTA server configuration](#)." Until you do this, devices and probes are not available as configuration

options in certain traffic analysis tasks such as interface and VPN traffic analysis tasks, and the data from devices and probes are not included in any traffic analysis tasks.

Traffic analysis task management

Traffic analysis task management ties network flow records to data analysis, reporting, and report navigation. Out of the box, NTA does not generate reports using the network flow records that are directed to it through configurations on the devices and through the device and probe management configurations in NTA. Administrators must create traffic analysis tasks that define how NTA reports all network flow record data.

Traffic analysis tasks define how resources in a network are grouped for analysis and reporting purposes. This has a direct impact on the utility and accessibility of the data presented in NTA reports. Traffic analysis tasks also define how NTA presents report navigation and how you access reports. NTA creates reports and makes them available on the left navigation tree under the **Traffic Analysis and Audit** area based on task configuration.

NTA traffic analysis tasks govern whether network flow records are presented as reports in NTA. The next step is to create traffic analysis tasks because traffic analysis tasks direct NTA to process and report on the network flow records it receives. Traffic analysis tasks enable you to configure from which devices, interfaces, and probes you process network flow records, as well as, which NTA network flow collector server processes the records. NTA supports the following types of network flow analysis tasks:

- Interface
- VLAN/VXLAN
- Probe
- Application
- Host
- VPN
- Interbusiness traffic analysis
- BGP AS

For interface, VLAN/VXLAN, probe, and VPN traffic analysis tasks, define from which interface, VLAN/VXLAN, probe, or VPNs the task processes network flow records and reports. NTA processes all received network flow records for host, application, and interbusiness tasks as these types of tasks are not tied to specific network flow record sources.

Traffic analysis tasks also allow you to organize how network resources are grouped in NTA for analysis and reporting purposes. This is a powerful configuration option that requires consideration, as NTA summarizes data found in network flow records based on the way you have grouped resources. For example, if you create an application task that groups six disparate applications, NTA provides summarized reporting for all six applications, not for individual applications in the group.

In general, you should group network resources by the seven types of network flow analysis task options provided by NTA. However, NTA allows you to group resources of the same type. For example, create an interface traffic analysis task that contains one or more interfaces from one or more devices. This enables you to provide summarized reporting for interfaces based on the group criteria you define. These are some of the options:

- Location
- Function
- Interface type
- Organization structure

Interbusiness traffic analysis tasks provide additional grouping capabilities because this task type combines host and application grouping into tasks that are business-service oriented. NTA analyzes

and summarizes network flow records based on your method of grouping like resources. That is probably the most important benefit.

The final aspect of traffic analysis tasks to consider is that the way you group tasks and the traffic analysis tasks that you create define how you access them. Traffic analysis tasks generate links on the left navigation tree under the **Traffic Analysis and Audit** area that you use to access the reports generated by them. Creating tasks that organize your resources effectively and contain only the resources on which you want to report results in an efficient navigation tree and easy report access.

For environments that have multiple devices that generate network flow data and multiple interfaces for which administrators want to collect data, careful planning of NTA traffic analysis task management is essential. This document contains a chapter for each monitoring type in NTA. These chapters summarize reporting capabilities and describe configuration considerations. They also include instructions for creating tasks and accessing the reports generated by tasks. Review the chapter for the monitoring and reporting type you want to enable in NTA to ensure that you get the most out of NTA and the network flow data available in your network.

Application, protocol, and application category management

The following features enable administrators to configure how NTA handles applications in the processing and reporting of network flow records:

- **Application**—The association of a port number to an application name. NTA comes with many predefined applications. NTA also enables administrators to create user-defined applications. After applications are created, administrators can select one or more applications for network flow record processing when they create application, host, or interbusiness traffic analysis tasks.
- **Protocol**—The association of a protocol number to a protocol name. NTA installs with predefined protocols. NTA also enables administrators to create user-defined protocols. Enable or disable any of the protocols to include or exclude the selected protocol from analysis and reporting.
- **Application category**—A grouping of applications. NTA installs with predefined application categories that group applications by application type. Create your own application categories to organize applications into categories. You can also add user-defined applications to application categories.

For more information on managing applications, protocols, and application categories in NTA, see "[Managing applications](#)," "[Managing protocols](#)," and "[Managing application categories](#)."

Filtering strategies

Filter strategies in NTA enable you to define whether the network flow records that NTA receives are processed or discarded by NTA. With filter strategies, you are able to do the following:

- Choose to process and analyze or discard packets based on their source or destination IP address or by source or destination Layer 4 port number.
- Process or discard TCP, UDP, or ICMP traffic.
- Analyze or discard traffic based on one or more combinations of source and destination IP addresses, port number, and protocol.

Filter strategies contain a name, description, default filter policy, and one or more filter conditions. Two types of filter policies are available. The **Discard** filter discards any packet that matches the filter conditions. The **Receive** filter processes and reports on any packet that matches the filter conditions.

The **Default Policy** defines how log packets are treated by default when the conditions of the packet do not match any of the filter conditions in the filter strategy.

A filter condition is a rule that defines the conditions under which log packets either are processed or discarded. A filter strategy can have many filter conditions, but every filter strategy must have at least

one filter condition. At least one of the filter conditions must contain a filter policy that does not match the default filter policy.

NTA supports a broad set of filter options for filtering by IP address, port, and protocol. You can create multiple filter conditions for every filter strategy. Every NTA server supports an unlimited number of filter strategies.

NTA enables you to specify which NetFlow, NetStream, and sFlow packets are processed and which are discarded. For example, create filter strategies for every device or every VPN on every device that forwards NetFlow, NetStream, or sFlow traffic to NTA. You can create filter strategies by port number or traffic type across all devices that forward flow traffic to NTA. For example, create a simple filter that discards all ICMP traffic from NTA analysis and reporting. For more detailed information on filtering strategies in NTA, see "[Using NTA filtering strategies](#)."

NTA parameter settings

The NTA Parameter Settings feature enables you to configure key analysis and reporting options. You can configure how many entries NTA displays for TopN reporting, how many days NTA maintains the flow data collected by devices, the maximum number of displayed entries for audits, and the direction of VLAN/VXLAN traffic analysis tasks.

You can enable or disable the following:

- ToS/MPLS Exp traffic analysis
- Unknown application traffic analysis
- Host session monitoring
- Baseline analysis
- Threshold alarming
- VPN traffic analysis
- Peak traffic analysis
- Realtime traffic
- Conversation aggregation TopN
- DNS setting

For detailed information on managing parameter settings in NTA, see "[Configuring NTA traffic analysis parameters](#)."

Network behavior anomaly detection

NTA collects statistics on traffic flow records and compares the statistics with a set of thresholds to discover anomalies. The thresholds that NTA uses are saved in predefined anomaly detection templates. When NTA discovers an anomaly, it sends the anomaly information (including the source and destination IP addresses of the packet, the IP address of the device, and the type and number of the interface) to INC so INC notifies administrators of the anomaly through its alarm module.

NTA provides the following predefined anomaly detection templates:

- **TCP Null Scan**—Determines whether a port is closed on the target host. The attacker sends to the target host port a TCP packet with no flags in the packet header. If the port is closed, the host returns a TCP RST packet. Otherwise, the packet is discarded.
- **TCP Fin Scan**—Determines port status and the operating system version (UNIX or Windows) on the target host. The attacker sends to the target host port a TCP packet with the FIN bit set in the packet header. If the port is closed, the host returns a TCP RST packet. Otherwise, the packet is discarded.

- **TCP Syn Fin Scan**—Indicates that a network attack has occurred. TCP SYN is used to initiate a TCP connection, and cannot be set with the FIN and RST bits. Other similar combinations include SYN/FIN, SYN/FIN/PSH, SYN/FIN/RST, and SYN/FIN/RST/PSH.
- **TCP Xmas Scan**—Determines if ports are closed on the target host. The attacker sends to the target host port a TCP packet with the FIN, URG, and PSH bits set in the packet header. If the port is closed, the host returns a TCP RST packet. Otherwise, the packet is discarded.
- **UDP Bomb Attack**—Detects an attack on an old version operating system. The attacker fills the UDP header with some invalid values, such as length values. Some old version operating systems crash when flooded with such packets.
- **Snork Attack**—Detects a DoS attack against Windows NT RPC service. This attack is accomplished by sending UDP packets with source port 7, 19, or 135, and destination port 135.
- **UDP Flood Attack**—Detects a UDP-based DoS attack. This attack significantly consumes the network bandwidth and degrades the network performance.
- **DNS Rogue Hack**—Detects an attack that exploits the DNS protocol to transmit illegal data. The attacker disguises the data as DNS traffic to send through the UDP port 53. Administrators must specify a list of valid DNS servers to distinguish between legitimate and disguised DNS traffic.
- **Invalid ToS**—Detects packets that contain invalid ToS values, such as 0, 2, 4, 8, and 16.
- **Land Attack**—Detects an attack on a host operating system. This attack is accomplished by sending spoofed packets with source address the same as the destination address, causing the operating system flooded with these packets to crash or hang.
- **Invalid IP Protocol**—Detects spoofed IP packets with protocol numbers equal to or greater than 134. These protocol numbers are unassigned or reserved, and should not be used in normal networks.
- **Corrupt IP Option**—Detects an attack on Windows operating system hosts. The attacker crashes the target Windows system or bypasses security checks by sending packets to the system with carefully crafted IP options.
- **Time Stamp IP Option**—Detects an attack on NetBSD hosts. The attacker launches a remote DOS attack against the target NetBSD system by flooding the system with TCP packets that contain unmatched IP timestamp options, causing the NetBSD system to crash.
- **Source Route IP Option**—Detects an attacker that uses IP source options to hide its true address and accesses restricted areas of a network by specifying a different path.
- **Record Route IP Option**—Detects an attacker that uses IP route record options to gain information about the architecture and topology information of the network through which the IP packets passed.
- **Security IP Option**—Detects forged IP packets with security options in the packet header. The IP security option is obsolete and therefore its presence in the IP header is suspect.
- **Stream ID IP Option**—Detects forged IP packets with stream ID options in the packet header. The stream ID option is obsolete and therefore its presence in the IP header is suspect.
- **Ping of Death Attack**—Detects an attack on hosts or network devices. The attacker sends large ICMP packets greater than 65507 bytes in size, causing the hosts or network devices that receive these packets to crash, freeze, or reboot.
- **Large ICMP Packet**—Detects large ICMP packet attack detection. Typically, ICMP packets contain short messages. The presence of large ICMP packets might indicate that something is wrong in the network.
- **Fragmented ICMP Packet**—Provides ICMP fragment detection. Because ICMP packets contain short messages, there is no legitimate reason for ICMP packets to be fragmented.
- **ICMP Redirects**—Detects when an attacker sends spoofed ICMP redirect packets to the target host to alter its routing table.
- **ICMP Destination Unreachable**—Detects when the attacker uses spoofed ICMP unreachable packets to mislead the target host to cut the connection to a specified network. This may

happen when operating systems drop the connection to a specified network upon receiving an ICMP unreachable packet, indicating that the network is unreachable.

- **ICMP Request Excess**—Detects an attack on a host operating system. The attacker floods the target host with ICMP echo requests, or Ping messages, which significantly consumes the resources and bandwidth of the host.
- **ICMP Reply Excess**—Detects when an attacker uses the ICMP reply messages to probe a host for its operating system information.
- **ICMP Source Quench**—Detects when an attacker uses spoofed ICMP source quench packets to limit the bandwidth available to other users. ICMP source quench packets can reduce the data transmission rate, which is recovered after the sending of such packets is stopped.
- **ICMP Parameter Problem**—Detects ICMP packets that contain invalid parameters.
- **ICMP Time Exceeded**—Detects when an attacker sends spoofed ICMP time exceeded messages to either or both of the communication parties to cut their connection.
- **DHCP Offer Packet**—Detects when an attacker sends a spoofed DHCP Offer packet with a random IP address to the host requesting the DHCP service, causing network anomalies.

You must configure these templates. For more information, see "[Anomaly detection management](#)."

NTA widgets

To facilitate monitoring of the network performance operating status, NTA provides various widgets. With these widgets, the administrator can monitor the network performance from different aspects at the same time. For example, with home page and dashboard widgets provided by NTA, the administrator can use the home page function of INC to customize and view these widgets. For more information about NTA widgets, see "[NTA widgets](#)."

NTA views

For better user experience, INC provides diversified views for different services and solutions to display NTA functions.

Entering the default perspective

1. Log in to INC.
2. Click the **Service** tab on the top navigation bar.
3. From the navigation tree, select **Traffic Analysis and Audit**.

This document describes NTA functions in default perspective.

Entering the desktop view

1. Log in to INC.
2. Perform one of the following tasks on the INC home page:
 - Click the **Desktop** icon  **Desktop** in the top right corner.
 - Select **Desktop View** from the **View** list in the top right corner.
3. In the desktop view, click the **Add application** icon .

You can customize applications as needed. For more information about the desktop view,

4. To switch to the default perspective, use one of the following methods:
 - o Click the **Start** icon  at the left of the desktop.
 - o Right-click the desktop, and then select **Classic** from the shortcut menu.

Entering the quick service process

1. Log in to INC.
2. On the INC home page, select **Quick Service Process** from the **View** list in the top right corner.
3. In the **Select Template Category** area, select **NTA&UBA Configuration Management**.
For information about the quick service process,
4. To switch to the default perspective, click **Default Perspective** in the top right corner.

Lower-level INC

NTA supports the lower-level INC feature. The current NTA server acts as an upper-level server to manage a bunch of lower-level NTA servers and can access the lower-level servers for traffic analysis task reports on them.

For information about adding a lower-level NTA server,

Viewing a lower-level NTA server

1. Click the **Service** tab.
2. From the navigation tree, select **Traffic Analysis and Audit**.
3. Click the **Shortcut Menu** icon  next to **Sub Traffic Analysis Server**.
All lower-level NTA servers are displayed in the menu that opens.
4. Click the IP address of a lower-level NTA server.
The window of the selected lower-level NTA server opens.

Viewing traffic analysis task reports on a lower-level NTA server

1. Click the **Service** tab.
2. From the navigation tree, select **Traffic Analysis and Audit**.
3. Click the **Shortcut Menu** icon  next to **Sub Traffic Analysis Server**.
All lower-level NTA servers are displayed in the menu that opens.
4. Click the **Expand** icon  next to the IP address of a lower-level NTA server.
The task types of the selected lower-level NTA server are displayed.
5. Click the **Expand** icon  next to a task type.
Traffic analysis tasks of the selected task type are displayed.
6. Click a task name to view the traffic analysis task report.

Analyzing the network traffic between virtual machines

More and more enterprises are using virtualization technology. By running multiple virtual machines on one VMware server, you can improve the physical server usage, reduce the hardware investments, and reduce the power consumption of the data center.

Virtual machines running on the same VMware server can provide more types of services for network users at the same time. Each virtual machine has its own IP/MAC address. Therefore, all traffic passing through the devices can be captured by the device supporting NetStream v5/v9, NetFlow v5/v9, or sFlow v5, and sent to NTA for processing and analysis. However, because the traffic between virtual machines is internally forwarded by the vSwitches of the VMware server without passing through the devices, such traffic cannot be captured and forwarded to NTA for processing and analysis.

Hewlett Packard Enterprise provides the probe server for analyzing the traffic between virtual machines.

The HPE probe servers include Linux servers with probe application programs installed and vMON virtual machines.

- When you use Linux servers with probe application programs installed, you must create a virtual Linux server on the VMware server and deploy a probe application program on the virtual Linux server. After the deployment, the operators must set the vSwitch. For information about using the probe to analyze the traffic between virtual machines, see "[Analyzing traffic between virtual machines](#)."
- When the vMON virtual machines are used, the operators must import vMON on the VMware server, and set the vSwitch after importing the vMON. For more information about the vMON usage, see *HPE Intelligent Management Center v7.3 Virtual Monitor Administrator Guide*.

Configuring NTA for traffic analysis and auditing

NTA enables you to manage the reception, analysis, and presentation of network flow records. You must configure devices to forward network flow data to NTA, add devices and probes to NTA, select each device and probe in the NTA server configuration page, and then create a task for each type of reporting you want. NTA produces reports using data generated by devices and probes and you can configure the NTA parameters to tune specifically how NTA analyzes and presents data.

This chapter describes how to add devices and probes to NTA. It describes the configuration options for NTA server management, and the process of managing applications, protocols, and application categories in NTA. It reviews the parameters for tuning, describes the NTA filtering strategies, and it reviews the process for managing database space.

Managing NTA data sources

NTA supports two types of devices as network flow data sources. The first type of devices are devices such as routers and switches that support NetStream v5/v9, NetFlow v5/v9, or sFlow v5 monitoring. You can add devices to NTA using the Device Management feature. When network flow data from one or more of these devices is necessary, you can modify the NTA server configuration, and deploy the new configuration. This makes it easy to adjust your network flow analysis configuration as your needs change.

The second device type for which NTA processes network flow data is a probe. A probe in NTA is a server that has the probe application program installed. A probe creates network flow records from devices that do not support network flow record generation. Using the probe, you can mirror traffic from a router or switch port or through an inline tap to a probe server that collects and analyzes the traffic before forwarding to an NTA server. As with Device Management, the Probe Management feature of NTA allows you to add probes without enabling network flow record processing for them until the need arises.

The NTA **Device List** contains devices such as routers, switches, and other devices that have been added to NTA as a potential source of network flow records. Adding a device or probe to NTA establishes a communication path between NTA as the network flow collector and the devices or probes that generate network flow records. It does not enable data collection or processing in NTA, nor does it add the device or probe to traffic analysis tasks for reporting purposes. To do so, you must select every device and probe for which you want to process data using the feature described in "[Modifying an NTA server configuration](#)." After you do this, the device or probe becomes available for use in all traffic analysis tasks, and the device data then becomes generally available to traffic analysis tasks. To include device data in specific interface and VPN tasks, create a traffic analysis task, and select the devices you want to include in the reporting. Adding devices to NTA does not enable NetStream, NetFlow, or sFlow on the device itself. You must also enable NetStream, NetFlow, or sFlow on the devices that you add to this list.

After you add a probe to NTA, you must select it using the feature described in "[Managing NTA servers](#)." The probe data then becomes generally available to traffic analysis tasks. To include probe data in a specific probe traffic analysis task, you must add the probe to a probe traffic analysis tasks. For more information on configuring a probe traffic analysis task, see "[Managing probe traffic analysis tasks](#)."

This section describes the process of adding routers, switches, and probes as data source devices in NTA.

Device management

NTA functions as a NetStream v5/v9, NetFlow v5/v9, and sFlow v5 collector for network flow statistical analysis and reporting. The Device Management feature of NTA enables you to view, add, modify, or remove devices that are network flow data sources in NTA. Routers and switches that support NetStream v5/v9, NetFlow v5/v9, and sFlow v5 data are devices that are data flow sources in NTA. You can add them to NTA using the Device Management feature. You can also add a router or switch as a network flow source to NTA. You can view, modify, and delete routers and switches that have been added to NTA network flow sources.

Every device that NTA processes network flow records for consumes a license. NTA provides the ability to add routers and switches as potential network flow data sources. When network flow data from one or more of these devices in the **Device List** is needed, you can modify the NTA server configuration to deploy the new configuration, enabling you to adjust your network flow analysis configuration as needs change.

This section describes the process of viewing, adding, modifying, and removing routers, switches and other devices as network flow data sources in NTA. "[Managing NTA servers](#)" describes the process of configuring an NTA server as a NetStream v5/v9, NetFlow v5/v9, or sFlow v5 collector and to enable or disable specific devices and probes for collection and analysis. This guide does not provide instructions for enabling NetStream, NetFlow, or sFlow on routers, switches, or other devices. For more information on how to enable NetStream, NetFlow, or sFlow on a particular device, see the vendor documentation.

Viewing the NTA Device List

The NTA **Device List** contains all devices such as routers, switches, and other devices that have been added to NTA as a potential source of network flow records. Adding a device to NTA establishes communication between NTA as the network flow collector and the devices that generate network flow records. Adding devices to NTA does not enable NetStream, NetFlow, or sFlow on the device. You must also configure NetStream, NetFlow, or sFlow on the devices that you add to this list.

To view the NTA **Device List**:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Device Management** link.

NTA displays all devices that are data sources for the NTA service module in the **Device List** in the main pane of the **Device Management** page.

Device List contents

- **Name**—Contains the name of the device that provides network flow data. The contents of this field link to the NTA **Device Details** page for more detailed information on the associated device. For more information on this feature, see "[Viewing the NTA Device Details page](#)."
 - **Device IP**—Contains the IP address of the device that provides the network flow data.
 - **Description**—Contains a description for the device that provides the network flow data.
 - **Device Resource Info**—This field contains an icon  for navigating to the device resource information page for the associated device. This icon is displayed only for devices that are added as data source devices by selecting devices from the INC platform.
 - **Modify**—Contains an icon  for modifying the associated device.
 - **Delete**—Contains an icon  for deleting the associated device.
3. To query NTA for the most recent **Device List**, click **Refresh** in the upper left corner of the **Device List**.

You can sort the **Device List** by the **Name**, **Device IP**, and **Description** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing the NTA Device Details page

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Device Management** link.
NTA displays all devices that are data sources in the **Device List** in the main pane of the **Device Management** page.
3. In the **Name** field of the device for which you want to view details, click the contents.
The NTA **Device Details** page for the selected device opens.

Device Details

- **Device IP**—Contains the IP address of the associated device that provides the network flow data.
 - **Name**—Contains the name of the device that provides the network flow data. By default, NTA autopopulates this field with the device name when you select a device using the **Add** option under **Device Management**. However, you can override the **Device Label** by assigning a new name to the device.
 - **Description**—Contains a description for the device that provides the network flow data.
 - **SNMP Community**—Contains the SNMP Read community string for the associated device. It does not contain the SNMP Read community string configured on the device. However, for NTA to function properly, the SNMP Read community string in NTA must match the SNMP Read community string that is configured on the device.
 - **SNMP Port**—Contains the SNMP port number used by NTA to communicate with and receive data from the device forwarding network flow data.
 - **Log Source IP**—Contains the IP address of the device that sends logs.
 - **NetStream Statistics Identifier**—Indicates whether NetStream Statistics Identifier is valid for the selected device.
 - **NetStream New Feature**—Indicates whether the NetStream flow sampling feature is enabled for the selected device. Only Comware-based devices support NetStream New Feature.
 - **NetStream Sampling Rate**—Indicates NetStream sampling rate configured by the device. For example, 1 indicates a sampling rate of 1:1, and 100 indicates a sampling rate of 1:100. For devices that support NetStream New Feature, NTA can obtain the sampling rate automatically. For devices that do not support NetStream New Feature, the NetStream sampling rate must be set manually. The sampling rate must be the same as that of the device. Otherwise, traffic statistics errors occur.
 - **sFlow Settings**—Indicates whether sFlow is enabled for devices. You can enable the sFlow feature for devices by using NTA.
 - **Dynamic sFlow Sampling Rate Adjustment**—Whether dynamic adjustment is enabled or disabled for the sFlow sampling rate.
 - **Sample Rate**—Rate at which sFlow samples packets. For example, 1000 indicates a sampling rate of 1:1000.
 - **VPN Name**—Name of the VPN instance deployed by sFlow.
 - **sFlow Interface List**—List of interfaces with sFlow enabled.
4. Click **Back** to return to the **Device List**.

Adding an NTA data source device

Use the **Add** feature on the **Device Management** page to add devices as data sources for NTA. However, you must be an administrator to add, modify, or delete devices that are used as data sources in NTA.

To add an NTA data source device:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Device Management** link.

NTA displays all devices that are data sources for the NTA service module in the **Device List** in the main pane of the **Device Management** page.

3. Click **Add**.

The **Add Device** page opens. You can add data source devices by adding devices manually or by selecting devices from the INC platform.

- If you add data source devices manually, the devices do not consume licenses of the INC platform. However, you cannot manage these devices, including monitoring performance, configuring backups, and receiving syslog or trap packets from parsing devices.
- If you add data source devices by selecting devices from the INC platform, you can manage the devices by using the basic network management function of the INC platform. However, these devices consume licenses of the INC platform. For more information about adding devices to the INC platform,

After you have added a device to NTA as a network flow data source, for it to become available for analysis task configurations and reporting, you must also select it by using the NTA Server Management feature. For more information about selecting a device by using the NTA Server Management feature, see "[Managing NTA servers](#)," specifically "[Modifying an NTA server configuration](#)."

You must also configure the device to forward NetStream, NetFlow, or sFlow traffic to the NTA server. For more information about configuring a router or switch to forward NetStream, NetFlow, or sFlow data to a collector, see the vendor documentation. For more information about configuring the NTA server as a collector, see "[Managing NTA servers](#)."

Adding data source devices manually

1. In the **Device IP** field, enter the IP address of the device.

Make sure the IP address communicates with the NTA server correctly. You cannot modify this field after you add the device.

2. In the **Name** field, enter the name of the device.

You cannot modify this field after you add the device.

3. In the **Description** field, enter the description for the device.

4. In the **SNMP Community** field, enter the SNMP Read community string of the device.

NTA reads the interface information of the device by using the SNMP Read community string. You can only configure SNMP Read community strings of SNMPv2 or v2c for devices that are added manually. For devices that use SNMP Read community strings of SNMPv3, add them by selecting them from the INC platform.

5. In the **SNMP Port** field, enter the SNMP listening port number for the device. The default value is UDP port 161.

6. In the **Log Source IP** field, enter the IP address of the log source for this device. If NTA cannot access a device through SNMP, you must specify the IP address. Otherwise, leave this field blank. You must specify a unique log source IP address for each device added as a log source.



IMPORTANT:

If the device you are adding has multiple IP addresses, add only one IP address for the data source device. To prevent incorrect traffic analysis results, do not create multiple instances of the same data source device using different IP addresses.

7. Select **Valid** from the **NetStream Statistics Identifier** list if the device supports NetStream Statistics Identifier. Select **Invalid** if the device does not support NetStream Statistics Identifier.

8. Select **Enable** from the **NetStream New Feature** list if the device supports NetStream Sampling Feature, and go to step 10. Select **Disable** if the device does not support NetStream Sampling Feature.

- For a device that supports NetStream Sampling Feature, it adds the sampling rate to the packets it sends to the NTA server. NTA reverts the data flow according to the sampling rate.

- For a device that does not support NetStream Sampling Feature, it does not add the sampling rate to the packets it sends to the NTA server.

NOTE:

- Only Comware-based devices support NetStream New Feature.
 - For Cisco devices, select **Invalid** from the **NetStream Statistics Identifier** list, and select **Disable** from the **NetStream New Feature** list.
-

- For devices that do not support NetStream New Feature, you must enter the NetStream sampling rate.
The sampling rate you enter must be the same as that you have configured on the device. Otherwise, traffic statistics errors occur. If you have not configured a sampling rate on the device, enter 1 to specify the sampling rate as 1:1.
- Click **OK** to add the device as a data source.
The **sFlow Settings** field cannot be configured when you manually add a device.

Adding data source devices by selecting devices from the INC platform

- Click **Select** next to the **Device IP** field.
The **Select Devices** dialog box opens.
- To select devices by a view or subview, do the following:
 - In the **Query Conditions** area, click the **By View** tab.
 - Click the **Expand** icon  next to the **IP View**, **Device View**, or **Custom View**, and then select a subview. The **Devices Found** area displays all devices in the subview.
 - **IP View**—Displays all devices that belong to a network segment.
 - **Device View**—Displays all devices that belong to a device category.
 - **Custom View**—Displays all devices that belong to a custom view or **Devices Not In Views**. All devices that do not belong to any view are added automatically to **Devices Not In Views**.
- To select devices by an advanced search, do the following:
 - In the **Query Conditions** area, click the **Advanced** tab.
 - Specify one or more of the following query criteria:
 - **Device IP**—Enter the IP address you want to query.
 - **Exact Query**—Select the option if you want NTA to search for the exact IP address you have entered in the **Device IP** field. Clear the **Exact Query** option if you want NTA to match only a certain portion of the IP address.
 - **Device IP List**—Configure multiple device IP addresses for the search. Click the **Device IP List Configuration** icon  to open the **Device IP List Configuration** window.
Enter one or multiple device IP addresses in the **Input Device IP** field (to enter multiple IP addresses, enter one IP address on each line), and then click **Add** to add the IP addresses to the **Device IP List** field below.
To delete an IP address in the **Device IP List** field, select the IP address, and then click **Delete**.
Click **OK** to close the **Device IP List Configuration** window.
To clear the **Device IP List** field, click the **Clear** icon .
 - **Device Label**—Enter a partial or complete name for the devices you want to add.
 - **Device Status**—Select device status from the **Device Status** list.
 - **Device Category**—Select a device type from the **Device Category** list.
 - **Device Series**—Select a device series from the **Device Series** list.

- **Contact**—Enter a partial or complete contact name.
 - **Location**—Enter a partial or complete location.
 - **Device Reachability**—Select the device reachability status from the **Device Reachability** list. Click **Query**. The **Devices Found** area displays all matching devices.
4. Highlight the device you want to select from the **Devices Found** list, and then click the **Add selected** icon  to add it to the **Selected Devices** list.

To remove a device, highlight the device and click the **Remove selected** icon .
 5. Confirm that the device you have selected has been added by reviewing the **Selected Devices** list.
 6. Click **OK**.
NTA autopopulates the **Device IP**, **Name**, and **SNMP Community** fields.
 7. In the **Description** field, enter the description for the device.
 8. In the **SNMP Port** field, enter the SNMP listening port number for the device. The default value is UDP port 161.
 9. In the **Log Source IP** field, enter the IP address of the log source for this device. If NTA cannot access a device through SNMP, you must specify the IP address. Otherwise, leave this field blank. You must specify a unique log source IP address for each device added as a log source.

IMPORTANT:

If the device you are adding has multiple IP addresses, add only one IP address for the data source device. To prevent incorrect traffic analysis results, do not create multiple instances of the same data source device using different IP addresses.

10. Select **Valid** from the **NetStream Statistics Identifier** list if the device supports NetStream Statistics Identifier. Select **Invalid** if the device does not support NetStream Statistics Identifier.
11. Select **Enable** from the **NetStream New Feature** list if the device supports NetStream Sampling Feature, and go to step 12. Select **Disable** if the device does not support NetStream Sampling Feature.
 - For a device that supports NetStream Sampling Feature, it adds the sampling rate to the packets it sends to the NTA server. NTA reverts the data flow according to the sampling rate.
 - For a device that does not support NetStream Sampling Feature, it does not add the sampling rate to the packets it sends to the NTA server.

NOTE:

- Only Comware-based devices support NetStream New Feature.
- For Cisco devices, select **Invalid** from the **NetStream Statistics Identifier** list, and select **Disable** from the **NetStream New Feature** list.

12. For devices that do not support NetStream New Feature, you must enter the NetStream sampling rate.
The sampling rate you enter must be the same as that you have configured on the device. Otherwise, traffic statistics errors occur. If you have not configured a sampling rate on the device, enter 1 to specify the sampling rate as 1:1.
13. Specify whether to enable sFlow for the device. Enable sFlow only for devices added to NTA by selecting IP addresses. After enabling sFlow, you must set the sFlow sampling rate and interfaces with sFlow enabled.
 - **Dynamic sFlow Sampling Rate Adjustment**—Select **Yes** to enable dynamic adjustment for the sFlow sampling rate. Select **No** to disable dynamic adjustment for the sFlow sampling rate. If sFlow cannot process packets based on the configured sampling rate, packet loss might occur, and the traffic collected by NTA might be significantly smaller than the actual traffic. In this case, enable this parameter.

- **Sample Rate**—Enter the rate at which sFlow samples packets. For example, 1000 indicates that the sampling rate is 1: 1000.
 - **VPN Name**—Enter the name of the VPN instance to be deployed.
 - **sFlow Interface List**—Click **Select**. The dialog box for selecting interfaces opens. Select the interfaces for which you want to enable sFlow, and click **OK**.
14. Click **OK** to add the device as a data source. NTA will deploy the sFlow-related configuration to devices with sFlow enabled through SNMP.

NOTE:

To deploy a VPN instance by using sFlow, you must configure Telnet parameters in the INC platform.

Modifying an NTA data source device

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Device Management** link.
NTA displays all devices that are data sources for the NTA service module in the **Device List** in the main pane of the **Device Management** page.
3. Click the **Modify** icon  for the NTA data source device entry you want to modify.
The **Modify Device** page opens.

 IMPORTANT:

After you create an NTA data source device, you cannot modify its IP address or name.

4. In the **Description** field, enter a description for this device.
5. In the **SNMP Community** field, modify the SNMP read community string.
This field must match the SNMP read community string that is configured on the device that is being added. The configuration takes effect only on devices with SNMPv1 or SNMPv2c enabled. For a device with SNMPv3 enabled, you must configure the device IP by selecting a device IP and correctly configure the SNMPv3 parameters of the device in the INC platform.
6. In the **SNMP Port** field, modify the UDP port number that is being used for SNMP polling on the device.
The value you enter in this field must match the port number that is configured on the device that is being added. The default value for this field and for SNMP polling is 161.
7. In the **Log Source IP** field, add or modify the IP address of the Log Source for this device.
If NTA cannot access a device through SNMP, you must specify the IP address. Otherwise, leave this field blank. You must specify a unique IP address for each device added as a log source.

 IMPORTANT:

If the device you are adding has multiple IP addresses, add only one IP address for the data source device. To prevent incorrect traffic analysis results, do not create multiple instances of the same data source device using different IP addresses.

8. Select **Valid** from the **NetStream Statistics Identifier** list if the device supports NetStream Statistics Identifier. Select **Invalid** if the device does not support NetStream statistics identifier.
9. Select **Enable** from the **NetStream New Feature** list if the device supports NetStream Sampling Feature, and go to step 11. Select **Disable** if the device does not support NetStream Sampling Feature.
 - For a device that supports NetStream Sampling Feature, it adds the sampling rate to the packets it sends to the NTA server. NTA reverts the data flow according to the sampling rate.

- For a device that does not support NetStream Sampling Feature, it does not add the sampling rate to the packets it sends to the NTA server.

! IMPORTANT:

- Only Comware-based devices support NetStream New Feature.
 - For Cisco devices, select **Invalid** from the **NetStream Statistics Identifier** list, and select **Disable** from the **NetStream New Feature** list.
-

10. Modify the NetStream sampling rate.

The configuration takes effect on only devices that do not support NetStream New Feature. For example, 1 indicates a sampling rate of 1:1, and 100 indicates a sampling rate of 1:100. The sampling rate configuration must be the same as that of the device. Otherwise, traffic statistics errors occur.

11. Select whether to enable sFlow for the device.

You can enable sFlow only for devices added to NTA through selecting IP addresses. After enabling sFlow, you must set the sFlow sampling rate and interfaces with sFlow enabled.

- **Dynamic sFlow Sampling Rate Adjustment**—Select **Yes** to enable dynamic adjustment for the sFlow sampling rate. Select **No** to disable dynamic adjustment for the sFlow sampling rate. If sFlow cannot process packets based on the configured sampling rate, packet loss might occur, and the traffic collected by NTA might be significantly smaller than the actual traffic. In this case, enable this parameter.
- **Sample Rate**—Enter the rate at which sFlow samples packets. For example, 1000 indicates that a sampling rate of 1:1000.
- **VPN Name**—Enter the name of the VPN instance to be deployed.
- **sFlow Interface List**—Click **Select**. The dialog box for selecting interfaces opens. Select the interfaces for which you want to enable sFlow, and click **OK**.

12. Click **OK** to confirm the modifications.

NTA deploys the sFlow-related configuration to devices with sFlow enabled through SNMP.

Deleting an NTA data source device

Deleting a device from NTA does not delete the data received from the device prior to the deletion. The database retains the data for all deleted devices according to the NTA server configuration.

! IMPORTANT:

Deleting an NTA data source device terminates all associated traffic analysis tasks.

To delete an NTA data source device:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Device Management** link.

NTA displays all devices that are data sources for the NTA service module in the **Device List** in the main pane of the **Device Management** page.

3. Click the **Delete** icon  for the NTA data source device entry you want to delete.
4. Click **OK** to confirm the deletion of the selected NTA data source device.

The **Device List** reflects the deletion of the selected device.

Probe management

NTA provides a solution for collecting and analyzing traffic from devices that do not support NetStream v5/v9, NetFlow v5/v9, or sFlow v5. Using the probe, you can mirror traffic from a router or switch port to a probe server that collects and analyzes the traffic before forwarding as network flow

records to an NTA server. In NTA, the communication between the NTA server and the probe is configured using the Probe Management features of NTA. You must also select the probe in the **Server Management** page for the probe to become available in traffic analysis task configurations and reports.

For more information on selecting a probe in the NTA server configuration, see "[Managing NTA servers](#)," specifically "[Modifying an NTA server configuration](#)." You must be an administrator to add, modify, or delete probes in NTA. This section describes these features and the process for integrating traffic data from a probe into NTA.

Viewing the probe list

View all probes configured in NTA in the probe list. From this list, you can view the details of a probe configuration, add new probes, and modify or delete existing probes.

To view the probe list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Probe Management** link.

NTA displays all probes in the **Probe List** in the main pane of the **Probe Management** page.

Probe List contents

- **Name**—Contains the name of the probe. The contents of this field link to the **Probe Details** page for the associated probe.
 - **IP**—Contains the IP address of the probe.
 - **Description**—Contains the description for the associated probe.
 - **Enable Layer 7 Application Identification**—Identifies whether Layer 7 application identification has been enabled for traffic from this probe.
 - **Modify**—Contains an icon  for modifying the associated probe.
 - **Delete**—Contains an icon  for deleting the associated probe.
3. To query NTA for the most recent **Probe List**, click **Refresh** located in the upper left corner of the **Probe List**.

You can sort the **Probe List** by the **Name**, **IP**, **Description**, and **Enable Layer 7 Application Identification** fields. Click the column label to sort the list by the selected field. The column label is a toggle switch that allows you to toggle between the various sort options specific to each field.

Viewing the NTA probe details page

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Probe Management** link.
NTA displays all probes in the **Probe List** in the main pane of the **Probe Management** page.
3. Click the contents of the **Name** field to navigate to the **Probe Details** page for the associated probe.

Probe Details

- **Name**—Contains the probe name assigned to it by the administrator.
 - **IP**—Contains the IP address of the associated probe.
 - **Description**—Contains a description for the associated probe.
 - **Enable Layer 7 Application Identification**—Identifies whether Layer 7 application identification has been enabled for the selected probe.
4. Click **Back** to return to the **Probe List**.

Adding a probe

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. Click the **Probe Management** link.

- NTA displays all probes in the **Probe List** in the main pane of the **Probe Management** page.
3. Click **Add**.
The **Add Probe** page opens.
 4. In the **Name** field, enter a name for the probe.
The name for each probe must be unique.
 5. In the **IP** field, enter the IP address of the probe.
The IP address of the server cannot be the same IP address as the device from which traffic is being mirrored.
 6. In the **Description** field, enter a brief description for this probe.
 7. Do one of the following:
 - If you want NTA to include Layer 7 application information in the analysis of traffic received by the probe, select **Yes** from the **Enable Layer 7 Application Identification** list.
 - To disable the identification of Layer 7 application identification from probe data analysis, select **No**.
 8. Enter the password for the probe in the **Probe Password** field.
The password must be the same as the password set when you installed the probe. If you have not set a password during the probe installation, leave the **Probe Password** field empty. To set a password for a probe, see *HPE Intelligent Management Center Probe Installation Guide*.
 9. Click **OK** to add the probe.
After you have added a probe to NTA as a network flow data source, you must also select it using the NTA Server Management feature. Then, the probe becomes available for traffic analysis task configurations and reports. For more information about selecting a probe using the NTA Server Management feature, see "[Managing NTA servers](#)," specifically "[Modifying an NTA server configuration](#)."
You must also install the probe application program on a dedicated server and configure it to receive traffic mirrored from the ports whose statistics you want to view.
You must also configure the router or switch to mirror traffic from one or more ports to the port to which the probe server or NTA is connected. If you are using a tap kit, you must also install the tap kit inline into the link being monitored. See the vendor documentation for configuring a router or switch to enable NetStream, NetFlow, or sFlow data to a collector or for information on installing tap kits. For more information about configuring the NTA server to receive network flows from a probe, see "[Managing NTA servers](#)."

Modifying a probe

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Probe Management** link.
NTA displays all probes in the **Probe List** in the main pane of the **Probe Management** page.
3. Click the **Modify** icon  for the probe you want to modify.
The **Modify Probe** page opens.
4. Modify the name of the probe in the **Name** field.
The name of each probe must be unique.

IMPORTANT:

After you create a probe, you cannot modify its IP address.

5. Modify the description for the probe in the **Description** field.
6. Do one of the following:
 - If you want NTA to include Layer 7 application information in the analysis of traffic received by the probe, select **Yes** from the **Enable Layer 7 Application Identification** list.

- To disable the identification of Layer 7 application identification from probe data analysis, select **No**.
- 7. Click **OK** to accept your modifications to the existing probe entry.

Deleting a probe

Delete a probe you have added to NTA. Deleting a probe from NTA does not delete the data received from the probe prior to deletion. The data for all deleted probes is retained in the database in accordance with the NTA server configuration.

To delete a probe:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Probe Management** link.
NTA displays all probes in the **Probe List** in the main pane of the **Probe Management** page.
3. Click the **Delete** icon  for the probe you want to delete.
4. Click **OK** to confirm the deletion of the selected probe.
The **Device List** reflects the deletion of the selected device.



IMPORTANT:

Deleting a probe terminates all associated traffic analysis tasks.

Managing NTA servers

Deploy the NTA service module on the INC master server or a subordinate server in distributed deployment. The NTA Server Management feature allows you to manage the configuration of all NTA servers, whether NTA is deployed on the master server. Each NTA server is added to the service list when the NTA service module is deployed.

When NTA is deployed on the master server, the server name is the loopback address or 127.0.0.1 by default. When NTA is deployed on a subordinate server, the server name is the server IP address by default. When the NTA service module is uninstalled, the installation program removes the NTA instance from the server list.

Deploy a maximum of 10 NTA servers for one NTA module. Multiple servers can share load to improve the NTA server performance. For no more than ten NTA servers, purchase a license for one NTA module and ensure that the total number of managed device nodes is within the license limit. For more than ten NTA servers, you must purchase more than one set of the INC platform and NTA module.

Viewing the NTA server list

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.
NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.

Server list contents

- **Server Name**—Contains the name of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server. The contents of this field are a link for viewing more detailed information for the associated server.
- **Server IP**—Contains the IP address of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server.
- **Description**—Contains the description for the associated NTA server.

- **Capture Flux Log**—Contains an icon  for initiating the capture of the traffic log for the associated NTA server for one hour. This option provides the traffic log data for the traffic log auditing feature of NTA.
 - **Deploy Configuration**—Contains an icon  for deploying the configuration for the associated NTA server.
 - **Modify**—Contains an icon  for modifying the associated NTA server.
3. To query NTA for the most recent **Server List**, click **Refresh** in the upper left corner of the **Server List**.
- You can sort the **Server List** by the **Server Name**, **Server IP**, and **Description** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing the NTA server details page

1. Select **Service > Traffic Analysis and Audit > Settings**.
 2. Click the **Server Management** link.
- NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.
3. Click the contents of the **Server Name** field to navigate to the server details page for the associated server.

Server base information

- **Server Name**—Contains the name of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server.
- **Server Description**—Contains a description for the associated server.
- **Processor IP**—Contains the IP address for the associated server.
- **Listening Port**—Identifies the ports that the associated server uses to listen for network flow records.
- **FTP Main Directory**—Identifies the root directory for the FTP service running on the associated server.
- **FTP Username**—Identifies the username of the FTP account used by probes to upload data to the NTA server.
- **Traffic Analysis Log Aggregation Policy**—Identifies whether the standard or rough aggregation policy is in use on the associated server.
- **Filter Policy**—Identifies whether a filtering policy has been applied to network flow records directed to the associated server.
- **Usage Threshold of the Database Disk (1-95%)**—Identifies the threshold for the percent of database disk utilization defined for the associated server.
- **When Database Disk Usage Reaches Threshold**—Identifies the action that is taken if the disk that the database resides on reaches the threshold specified in the **Usage Threshold of the Database Disk** field.

Traffic Analysis—Device information

- **Device Name**—Contains the name of the device that provides network flow data for the associated server.
- **Device IP**—Contains the IP address of the device that provides the network flow data for the associated server.
- **Device Description**—Contains a description for the device that provides the network flow data for the associated server.

Traffic Analysis—Probe information

- **Probe Name**—Contains the name of the probe that provides the network flow data for the associated server.
 - **Probe IP**—Contains the IP address of the probe that provides the network flow data for the associated server.
 - **Enable Layer 7 Application Identification**—Identifies whether Layer 7 application identification has been enabled for traffic from this probe that provides the network flow data for the associated server.
4. Click **Back** to return to the **Server List**.

Modifying an NTA server configuration

1. From the top navigation bar, select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.
NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.
3. In the **Modify** field, click the **Modify** icon  for the NTA server you want to modify.
4. In the **Server Name** field, modify the NTA server name.
5. In the **Server Description** field, modify the description for the NTA server.
You cannot modify the IP address of an NTA server.
6. In the **Listening Port** field, modify the UDP ports that NTA uses to communicate with the devices and probes that send traffic data.



IMPORTANT:

If you change the port assignments in this field, you must also change them on the devices and probes transmitting the traffic data to the NTA server.

7. In the **FTP Main Directory** field, enter or modify the path to the FTP main directory.
8. In the **FTP Username** field, enter or modify the FTP username.
9. In the **FTP Password** field, enter or modify the FTP password.
10. From the **Traffic Analysis Log Aggregation Policy** list, select the aggregation policy you want to apply to all log files processed by this NTA server. Options are:
 - **No Aggregation (Best Report Timeliness)**—This option does not aggregate data, and is suitable for environments that have high requirements on report timeliness. This mode requires much disk space because a huge number of logs are generated.
 - **Aggregation (Standard)**—This option aggregates data at 5-minute intervals and is suitable for environments that have a medium number of logs generated and requires less disk space than the **No Aggregation** mode and more disk space than the **Aggregation (Rough Granularity)** mode.
 - **Aggregation (Rough Granularity)**—This option aggregates data at 20-minute intervals and is suitable for environments that have a small number of logs generated and requires the least disk space.
11. From the **Filter Policy** list, select the filter policy to discard any data you do not want to process and report on. Options are the user-defined filters created using the NTA Filter Strategy feature and **Not Filter**.
Select the **Not Filter** option if you do not want to exclude any data using filters.
You must create a filter strategy before you can select it. To create a filter strategy, see "[Using NTA filtering strategies](#)."
12. Enter the percent of disk space on the disk or volume assigned to the database that can be used by NTA before NTA either stops receiving logs or deletes logs to release disk space.

13. From the **When Database Disk Usage Reaches Threshold** list, select the action you want NTA to take when the NTA database disk or volume consumption exceeds the threshold you set previously.
Options are:
 - o **Stop Receiving Logs**—When the specified threshold or percent of disk space is reached, NTA no longer processes or stores traffic analysis data until additional disk space is released or added to the database volume.
 - o **Delete Logs to Release Space**—When the specified threshold or percent of disk space is reached, NTA deletes existing logs from the oldest, until the disk space usage drops below the threshold or percent.
14. After you add a device to NTA as described in "[Device management](#)," select it on the **Server Configuration** page to make it available for processing and reporting when you create a task.
 - a. To enable the processing of network flow data from a device (router or switch) in NTA, select the check box next to the device name in the **Traffic Analysis—Device Information** area.
 - b. To disable the processing of network flow data from a device in NTA, select the check box next to the device name. If you want to add a device that is not displayed on the **Device Information** list, see "[Managing NTA data sources](#)," specifically "[Device management](#)."
15. After you add a probe to NTA as described in "[Probe management](#)," you must select it on the **Server Configuration** page to make it available for processing and reporting when you create a task.
 - a. To enable the processing of network flow data from a probe in NTA, select the check box next to the probe name in the **Traffic Analysis—Probe Information** area.
 - b. To disable the processing of network flow data from a probe in NTA, select the check box next to the probe name. To add a probe that is not displayed on the **Probe Information** list, see "[Managing NTA data sources](#)," specifically "[Probe management](#)."

! IMPORTANT:

Every device and probe selected in the **Server Configuration** page consumes a license. If you do not have enough licenses to add a device or probe, then you must clear a device or probe before adding a new one. If the device or probe you clear is configured for an interface or probe task, you must remove it from the task before you can select a new device or probe in the **Server Configuration** page. For more information on modifying a traffic analysis task, see "Modifying traffic analysis task" for the task type you want to modify. For example, to modify an interface task, see "[Modifying an interface traffic analysis task](#)."

16. Click **Deploy** to accept and deploy your NTA server configuration changes.
17. After NTA completes the deployment of the NTA configuration changes, the **Configuration Deployment Result** page opens. Review the results in the **Deployment Details** fields for **Processor**, **Receiver**, and **Probe Deployment Result** to verify that the changes you made were deployed successfully.
18. Click **Back** to return to the **Server Management** page.

Redeploying the NTA server configuration

NTA enables you to restore or redeploy the existing NTA server configuration with or without modifications to it.

To redeploy the NTA server configuration:

1. From the top navigation bar, select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.

NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.

3. In the **Deploy Configuration** field for the NTA server for which you want to redeploy the configuration, click the icon .
After NTA has completed the redeployment of the NTA configuration, the **Configuration Deployment Result** page opens.
4. Review the results in the **Deployment Details** fields for **Processor**, **Receiver**, and **Probe Deployment Result** to verify that the configuration was redeployed successfully.
5. Click **Back** to return to the **Server Management** page.

Capturing an NTA server flux log

This option initiates the capture of traffic log data for use with the traffic log auditing feature of NTA. This feature captures the traffic log for the selected NTA server for one hour. For more information about using the traffic log auditing feature, see "[Performing traffic log audits in NTA.](#)"

To capture an NTA server flux log:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.
NTA displays all NTA servers in the **Server List** in the main pane of the **Server Management** page.
3. In the **Capture Flux Log** field for the NTA server for which you want to capture a flux log, click the **Capture** icon .
4. Click **OK** to capture the flux log. The **Capture Flux Log** column displays the time when the capturing started. The column does not display the time after the capturing is completed.

The **Server Management** page displays the results of the capture flux log request at the top of the page. Review the results of this request to ensure that NTA is configured to successfully capture the flux log. After you capture the flux log, use the traffic log auditing feature to view captured data. For more information about the traffic log auditing feature, see "[Performing traffic log audits in NTA.](#)"

Managing applications in NTA

NTA enables you to manage the applications for which NTA analyzes and reports. Using the NTA Application Management features, you can create applications, protocols, and application categories, and define which of the protocols NTA analyzes. This enables you to refine and customize NTA to meet your specific traffic monitoring and reporting needs.

Applications enable you to configure NTA to analyze and report on predefined applications or applications in use in your environment that NTA does not include in the predefined application list.

Two types of applications are available: Layer 4 and Layer 7. With Layer 4 applications, you specify the application name and the Layer 4 protocol in use, TCP, UDP, or both. Specify the Layer 4 port number that the application uses. When a match is found, NTA attributes the traffic in NTA reports to the application name you provided.

With Layer 7 applications, you specify the application name and a regular expression string that NTA uses to compare against the contents of the Layer 7 portion of every IP packet. When a match is found, NTA attributes the traffic in NTA reports to the application name you provided.

NTA uses a protocols list for analyzing network traffic. You can create user-defined protocols and modify predefined protocol names. You can enable or disable the protocols on this list to tune NTA to meet your reporting needs.

Application categories enable you to group applications for summarized analysis and reporting. You can create application categories that are organized by application or by protocol. When you create an application category based on application, you select from the list of existing applications comprised of the predefined and user-defined applications. When you create an application category

based on protocol, you select protocols from the NTA predefined and user-defined protocols list. Either way, NTA provides summarized analysis and reporting for all applications in the group.

The first step in customizing NTA to meet your needs is to review the NTA list of predefined applications to identify the applications it does and does not contain. Compare the results of your review against the list of applications used in your environment for which you expect to use NTA traffic analysis reporting. Then, create applications in NTA for all applications that are not on the list. For more information about creating and managing applications, see "[Managing applications](#)."

Then, review the protocols list in NTA and identify any protocols in use in your environment and verify that they are enabled in the **Protocol List**. For more information about managing protocols, see "[Managing protocols](#)."

After you add the applications and enable or disable the protocols, create application categories to group applications and protocols to meet your analysis and reporting needs. For more information about creating application categories, see "[Managing application categories](#)."

This section describes the process for managing applications, protocols, and application categories in NTA.

Managing applications

NTA analyzes traffic from an application perspective based on the list of applications within NTA. NTA enables you to add custom applications to the list that NTA uses to process and analyze and present network flow data. This feature enables you to identify and analyze applications used by your organization that are not included in NTA as system or predefined applications.

Two types of applications are available: Layer 4 and Layer 7. With Layer 4 applications, you specify the application name, and the Layer 4 protocol in use, TCP, UDP, or both. Specify the Layer 4 port number that the application uses and the IP addresses of hosts that use the application. Therefore, Layer 4 applications can be identified by host. When a match is found, NTA attributes the traffic in NTA reports to the application name you provided.

With Layer 7 applications, content that can be found in the header of an IP packet is used to identify the application. This feature is particularly useful for applications that use dynamic port assignments such as P2P, BT, and eDonkey. To create a Layer 7 application, you specify a regular expression string that NTA uses to compare the contents of the IP header of every packet. When a match is found, NTA attributes the traffic in NTA reports to the application name you provided. Applications using inconsistent ports are common in most networks and processing them in NTA can consume considerable NTA system resources. Therefore, Layer 7 applications include the option to enable or disable them. This enables you to create the applications, and then use them on an as-needed basis.

This section describes the process for viewing, adding, modifying, and removing applications from NTA.

Viewing the application list

All the applications that NTA uses to analyze and present network flow data from an application perspective can be found in the **Application List**.

To view the application list:

1. From the top navigation bar, select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.

NTA displays all applications in the **Application List** in the main pane of the **Application Management** page.

Application list contents

- **Application**—Contains the name of the application. This field is a link to the **Application Details** page for more detailed information on the associated application.
- **Protocol**—Identifies the Layer 4 IP protocol, TCP or UDP, for the associated application.

- **Port**—Contains the TCP or UDP port number for the associated Layer 4 application. A Layer 7 application does not need specific port number. The port number could be a port number or a port number range.
- **Application Type**—Identifies which layer of the seven-layer OSI reference model at which this application operates.
- **Description**—This field provides a description of the application.
- **Enable**—Identifies whether the application is enabled.
- **Pre-defined**—Identifies whether the associated application is predefined or user-defined. A value of **Yes** in this field indicates that the associated application is system or predefined. A value of **No** in this field indicates that the associated application is user-defined.
- **Modify**—Contains an icon  for modifying the associated application.
- **Delete**—Contains an icon  for deleting the associated application.

To navigate the **Application List**:

- Click the **Next Page** icon  to page forward in the **Application List**.
- Click the **Last Page** icon  to page forward to the end of the **Application List**.
- Click the **Previous Page** icon  to page backward in the **Application List**.
- Click the **First Page** icon  to page backward to the front of the **Application List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Application List** to configure how many items per page you want to display.
- For an **Application List** that has more than one page, click a number at the lower right of the main pane to go to that page.
- To query NTA for the most recent **Application List**, click **Refresh** in the upper left corner of the **Application List**.

You can sort the **Application List** by the **Application**, **Protocol**, **Port**, **Application Type**, **Description**, **Enable**, and **Pre-defined** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Querying the application list

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab. NTA displays all applications known to NTA in the **Application List** in the main pane of the **Application Management** page.
4. In the upper right corner of the **Application List** page, enter a partial or complete name of the application to be queried in the query field, and click the **Query** icon  to filter out the unmatched applications.
5. To filter applications by using more query criteria, click the **Advanced** icon  next to the query field to expand the query criteria panel above the application list. Specify one or more of the following query criteria:
 - **Application**—Enter a partial or complete name for each application you want to locate.
 - **Protocol**—Select the Layer 4 IP protocol you want to filter the associated application for from the **Protocol** list. Options are **TCP**, **UDP**, and **TCP/UDP**.

- **Port**—Enter the TCP or UDP port number for the associated applications you want to locate. Otherwise, enter a range of port numbers for the associated applications you want to locate.
 - **Application Type**—Select the application type, **Layer 4**, **Layer 7**, or **All**, from the **Application Type** list.
 - **Pre-defined**—Filter applications. To filter for predefined applications, select **Yes** from the list. To filter for applications that are user-defined, select **No** from the list. To include both predefined and user-defined applications, select **Not limited**.
6. Click **Query**.
The query results are displayed on the **Application List**.
 7. Click **Reset** to restore the full contents of the **Application List**.

Adding an application

Two types of applications are available: Layer 4 and Layer 7. With Layer 4 applications, you specify the application name and the Layer 4 protocol in use, TCP, UDP, or both. Specify the Layer 4 port number that the application uses and the IP addresses of hosts that use the application. Therefore, Layer 4 applications can be identified by host. When a match is found, NTA attributes the traffic in NTA reports to the application name provided.

Applications using dynamic or inconsistent port assignments are common in most networks and processing them can consume considerable system resources. With Layer 7 applications, NTA enables you to identify content that can be found in the header of an IP packet to be used to identify an application. This feature is particularly useful for applications that use dynamic port assignments such as P2P, BT, and eDonkey.

To create a Layer 7 application, specify a regular expression string that NTA uses to compare the contents of the IP header of every packet. When a match is found, NTA attributes the traffic to the application name you provided in reports. Therefore, Layer 7 applications include the option to enable or disable them. This enables you to create an application and use it on an as-needed basis.

To add a user-defined application to NTA:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.
NTA displays all applications known to NTA in the **Application List** in the main pane of the **Application Management** page.
4. Click **Add**.
The **Add Application** page opens.
5. In the **Application** field, enter the name for the application.
6. In the **Description** field, enter a brief description for the application.
7. From the **Protocol** list, select the Layer 4 IP protocol.
Options are **TCP**, **UDP**, and **TCP/UDP**. If you select **TCP/UDP**, you add two applications to the application list, one using TCP and the other using UDP.
8. From the **Application Type** list, select the application type, **Layer 4** or **Layer 7**. If you selected **Layer 4**, go to step 10. If you selected **Layer 7**, go to step 9.
9. Perform the following tasks when **Layer 7** is selected:
 - a. Enter a string in the **Regular Expression** field. NTA uses the regular expression to identify the application in the Layer 7 portion of each IP packet examined. For more information on the use of regular expressions in NTA, see "[Regular expressions in NTA](#)."

IMPORTANT:

After you create an application, you cannot modify the **Protocol**, **Application Type**, or **Port** number. You can only create a new application with the revised **Protocol**, **Application Type**, and **Port** number.

- b. Select **Yes** from the **Enable** list to enable regular expression matching for the application.
Select **No** if you do not want to enable regular expression matching for the application.
 10. Perform the following tasks when **Layer 4** is selected:
 - o Enter the TCP or UDP port number that the application uses in the **Port** field. Otherwise, enter a range of port numbers that the application uses.
 - o Enter the IP address that the application uses in the **Host IP** field. This step is optional.
You can configure a Layer 4 application to include one or more host IP addresses. You can enter a range of IP addresses, or a combination of IP host addresses and IP address ranges. However, no two addresses or address ranges entered in the **Host IP** field can overlap.
To enter the IP address for a single host, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/64
 11. Click **Add** next to the **Host IP** field.
The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.
 12. Click **OK** to create the application.
- After you create an application, NTA uses it to analyze and report on traffic data.

Modifying an application

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.
NTA displays all applications known to NTA in the **Application List** in the main pane of the **Application Management** page.
4. In the **Modify** field for the application you want to modify, click the **Modify** icon .
The **Modify Application** page opens.
5. In the **Application** field, modify the name for the application.
6. In the **Description** field, modify the description for the application.
7. In the **Port** field, modify the port number or port number range for the user-defined application.
You can enter a range of port numbers for the application.
You cannot modify the **Protocol** or **Application Type** after you create a user-defined application, or the **Protocol**, **Application Type**, or **Port** for a predefined application. Create a new application with the revised **Protocol** and **Application Type**.
8. Perform the following tasks when **Layer 7** is selected:
 - a. Modify the regular expression string in the **Regular Expression** field. NTA uses the regular expression string to identify the application in the Layer 7 portion of each IP packet examined.

For more information on the use of regular expressions in NTA, see "[Regular expressions in NTA.](#)"

- b.** Select **Yes** from the **Enable** list if you want to enable regular expression matching for the application. Select **No** if you do not want to enable regular expression matching for the application.
- Perform the following tasks when **Layer 4** is selected:
- a.** Enter the IP address that the application uses in the **Host IP** field. This step is optional.
- You can configure a Layer 4 application to include one or more host IP addresses. Otherwise, enter a range of IP addresses, or a combination of IP host addresses and IP address ranges. However, no two addresses or address ranges entered in the **Host IP** field can overlap.
- To enter the IP address for a single host, enter the IP address using dotted decimal notation.
- Example of a valid IP address:
- 10.153.89.10
- Example of a valid network/subnet mask in dotted decimal notation:
- 10.153.89.0/255.255.255.0
- Example of a valid network/subnet mask using CIDR notation:
- 10.153.89.0/24
- Example of a valid IPv6 address:
- a001:410:0:1::1
- Example of a valid IPv6 address and subnet mask using CIDR notation:
- a001:410:0:1::1/64
- b.** Click **Add** next to the **Host IP** field.
- The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.
- c.** Click **Delete** next to the **Host IP** field.
- The addresses and masks you select are deleted from the **Host IP List** field.
- Click **OK** to accept your modifications to the application.

Batch importing applications

You can import user-defined applications from a .csv file in batches. Each line of the file defines one application, including the application name, protocol, port number, and application description.

To import user-defined applications to NTA in batches:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.
NTA displays all applications in the **Application List** in the main pane of the **Application Management** page.
4. Click **Import**.
The **Import Application** page opens.
5. Click **Browse**.
The **Choose file** dialog box opens.
6. Locate the application definition file to be imported, and click **Open**.
NTA automatically populates the **Application Definition File** field with the file path and name.
7. Click **Upload File**.
NTA starts to resolve the file contents. The **Import Application** page displays the resolution result on the **Application List**.

Imported application list

- **Line NO.**—Number of the line that holds the application.
 - **Application**—Name of the application, which is defined by the first column of the file.
 - **Protocol**—Protocol used by the application, which is defined by the second column of the file.
 - **Port**—Port number used by the application, which is defined by the third column of the file.
 - **Description**—Description on the application, which is defined by the fourth column of the file.
 - **Status**—Status of the application. After NTA completes the resolution, the correct status of an application is **To be imported**. If prompted that the format is wrong, check the file format.
Select **8, 15, 50, 100, or 200** from the list at the lower right of the **Application List** to configure how many items per page you want to display.
8. Click **Import** to import applications in batches.
If the import succeeds, the **Status** field on the **Application List** displays **Successful**. If the import is failed, the **Status** field shows the reason for the failure.
9. Click **Back** to return to the **Application Management** page.

Deleting applications

You can delete user-defined applications. Deleting an application from NTA does not delete the data for the associated application. The data for all deleted applications are retained in the database in accordance with the NTA server configuration.

Deleting a single application

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.
NTA displays all applications in the **Application List** in the main pane of the **Application Management** page.
4. Click the **Delete** icon  for the application you want to delete.

IMPORTANT:

You can delete user-defined applications only. You cannot delete system or predefined applications.

5. Click **OK** to confirm the deletion of the selected application.
The **Application List** reflects the deletion of the selected application.

Deleting applications in batches

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application** tab.
NTA displays all applications in the **Application List** in the main pane of the **Application Management** page.
4. Select one or more applications.
5. Click **Batch Delete**.
6. Click **OK** to confirm the deletion of the selected applications.

Regular expressions in NTA

If you selected **Layer 7** from the **Application Type** list to add an application, you must enter a regular expression string in the **Regular Expression** field that NTA uses to identify the application in the Layer 7 portion of each IP packet examined.

A regular expression contains 1 to 255 characters in hexadecimal notation or in text string. The hexadecimal notation contains \x01 through \xff. The text string can contain letters, digits, and symbols (also known as metacharacters).

Metacharacters in regular expressions

- **Brackets ([])**—Matches a single character contained within the brackets. For example, **[abc]** matches **a**, **b**, or **c**.
- **Vertical bar (|)**—Matches either the expression before or the expression after the operator. For example, **ab|cd** matches **ab** or **cd**.
- **Parentheses ()**—Defines a subexpression. For example, **a(b|c)d** matches **abd** or **acd**, but not **ab**, **cd**, or **abcd**.
- **Dot (.)**—Matches any single character. For example, **a.b** matches **avb**, but not **ab** or **avwb**. Contained within a bracket expression, this character matches a literal dot.
- **Asterisk (*)**—Matches the preceding element zero or more times. For example, **a*bc** matches **bc**, **abc**, **aabc**, and so on. Contained within a bracket expression, this character matches a literal asterisk.
- **Plus sign (+)**—Matches the preceding element one or more times. For example, **a+bc** matches **abc**, **aabc**, **aaabc**, and so on. Contained within a bracket expression, this character matches a literal plus sign.
- **Question mark (?)**—Matches the preceding element zero or one time. For example, **a?bc** only matches **bc** or **abc**. Contained within a bracket expression, this character matches a literal question mark.
- **Caret (^)**—Matches the beginning of a string. For example, **^the** matches the string **the man is tall**, but not **is the man tall**. A bracket expression containing this character (**[^]**) matches a single character that is not contained within the brackets. For example, **[^abc]** matches **abcd** or **ef**, but not **ac** or **bc**.
- **Dollar sign (\$)**—Matches the end of a string. For example, **man\$** matches the string **abnormal man**, but not **the man is tall**.
- **Minus sign (-)**—Represents a range if it is not the first or last character within the brackets. For example, **[a-c]** matches any lower-case character from **a** to **c** (that is, **a**, **b**, or **c**). Being the first or last character in a bracket expression, this character matches a literal minus sign.

Regular expression examples

- **Example 1**
Regular expression **^\x13BitTorrent protocol** matches the content of a BitTorrent handshake packet, which starts with hexadecimal character **\x13** and is followed by the string **BitTorrent protocol**. The regular expression would match **\x13BitTorrent protocol 1.22v**, but not **BitTorrent protocol 1.22v**, which does not start with **\x13**.
- **Example 2**
Regular expression **^a[bc].*d\$** would match **abd**, **abd**, or **acd**, but not **aed** (in which **e** is not included in bracket expression **[bc]**), **the abd** (which does not start with **a**), or **acde** (which does not end with **d**).
- **Example 3**
Regular expression **a+b?** matches any string that contains one or more **a**s followed by zero or one **b**. It would match **ab**, **a**, **aa**, **aab**, or **cabd**, but not **bb**.
- **Example 4**
Regular expression **a(bc)+d** matches any string that contains **a** and **d** with the string **bc** appearing one or more times in between. It would match **abcd** or **abcbcbcd**, but not **abcabd**.

Managing protocols

Protocol management allows you to add protocols and define the network or protocols to enable NTA traffic analysis and reporting. For example, if you enable ICMP, NTA analyzes bandwidth usage trends and other statistics for ICMP. Disabling protocols removes them from statistical analysis and reporting. This section describes the process for viewing and querying the protocols that can be analyzed and reported on in NTA.

Viewing the protocol list

NTA displays all protocols for which it processes network flow records in the **Protocol List**.

To view the protocol list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.

NTA displays all protocols in NTA in the **Protocol List** in the main pane of the **Application Management** page.

Protocol list contents

- **Protocol Name**—Contains the name of the protocol. This field is a link to the **Protocol Details** page for information on the associated protocol.
- **Protocol Number**—Contains a sequential number assigned to the protocol for NTA purposes. This field does not contain the port number for the associated protocol.
- **Enable**—Identifies whether the associated protocol is enabled for statistical analysis and reporting.
- **Pre-defined**—Identifies whether the associated protocol is system or predefined or user-defined. A value of **Yes** in this field indicates that the associated protocol is system or predefined. A value of **No** in this field indicates that the associated protocol is user-defined.
- **Modify**—Contains an icon  for enabling and disabling the associated protocol.
- **Delete**—Contains an icon  for deleting the associated protocol.

If the **Protocol List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Protocol List**.
- Click the **Last Page** icon  to page forward to the end of the **Protocol List**.
- Click the **Previous Page** icon  to page backward in the **Protocol List**.
- Click the **First Page** icon  to page backward to the front of the **Protocol List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Protocol List** to configure how many items per page you want to display.
- For a **Protocol List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To query NTA for the most recent **Protocol List**, click **Refresh** in the upper left corner of the **Protocol List**.

You can sort the **Protocol List** by the **Protocol Name**, **Protocol Number**, **Enable**, and **Pre-defined** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Querying the protocol list

1. Select **Service > Traffic Analysis and Audit > Settings**.

2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols in NTA in the **Protocol List** in the main pane of the **Application Management** page.
4. In the upper right corner of the **Protocol List** page, enter a partial or complete name of the protocols to be queried in the query field, and click the **Query** icon  to filter out the unmatched protocols.

To filter protocols by using more query criteria, click the **Advanced** icon  next to the query field to expand the query criteria panel above the protocol list. Specify one or more of the following query criteria:

- **Protocol Name**—Enter a partial or complete name for the protocols for which you want to search.
 - **Protocol Number**—Enter the number NTA has assigned to the protocol (not the port number for the protocol).
 - **Enable**—Select **Yes** to filter the list for all protocols that are enabled for analysis and reporting. Select **No** to filter the list for all protocols that are disabled from analysis and reporting. Select **Not limited** if you do not want to filter the list by protocols that have been either enabled or disabled.
 - **Pre-defined**—Select **Yes** to filter for protocols that are predefined. To filter for protocols that are user-defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.
5. Click **Query**.
The query results are displayed on the **Protocol List**.
 6. Click **Reset** to restore the full contents of the **Protocol List**.

Adding a protocol

1. From the top navigation bar, select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols on the **Protocol List** in the main pane of the **Application Management** page.
4. Click **Add**.
The **Add Protocol** page opens.
5. In the **Protocol Name** field, enter the name for the protocol.
6. In the **Protocol Number** field, enter the number for the protocol.



IMPORTANT:

After you add a protocol, you cannot modify the **Protocol Number**. You can add a new protocol with the revised protocol number.

7. To enable statistical analysis and reporting for the selected protocol, select **Yes** from the **Enable** list.
To disable statistical analysis and reporting for the selected protocol, select **No** from the **Enable** list.
8. Click **OK** to add the protocol.
After a protocol is added, NTA uses it to analyze and report on traffic data.

Modifying a protocol

To enable or disable the analysis and reporting of a protocol in NTA:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols in the **Protocol List** in the main pane of the **Application Management** page.
4. In the **Modify** field for the protocol you want to modify, click the **Modify** icon .
The **Modify Protocol** page opens.
5. In the **Protocol Name** field, modify the name for the protocol.
6. From the **Enable** list, select **Yes** to enable the statistical analysis and reporting for the selected protocol.
7. From the **Enable** list, select **No** to disable the statistical analysis and reporting for the selected protocol.
8. Click **OK** to accept your changes.

NTA begins analysis and reporting for the protocol that has been enabled. Reports for newly enabled protocols become available after several data collection intervals.

Batch importing protocols

To import user-defined protocols to NTA in batches:

1. Select **Service > Traffic Analysis and Audit > Settings**.
 2. Click the **Application Management** link.
 3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols on the **Protocol List** in the main pane of the **Application Management** page.
 4. Click **Import**.
The **Import Protocol** page opens.
 5. Click **Browse**.
The **Choose file** dialog box opens.
 6. Choose the protocol definition file to be imported, and click **Open**.
INC autopopulates **Protocol File** field with the file path and name.
 7. Click **Upload File**.
NTA starts to resolve the file contents. The **Import Protocol** page is refreshed to display the resolution result on the **Protocol List**.
- Imported protocol list**
- **Line NO.**—Number of the line that holds the protocol.
 - **Protocol Name**—Name of the protocol, which is defined by the first column of the file.
 - **Protocol Number**—Protocol number used by the protocol, which is defined by the second column of the file.
 - **Enable**—Indicates whether to enable the statistical analysis and reporting for the selected protocol, which is defined by the fourth column of the file.
 - **Status**—Status of the protocol. After NTA completes the resolution, the correct status of a protocol is **To be imported**. If prompted that the format is wrong, check the file format.
8. Click **Import** to import protocols in batches.
If the import succeeds, the **Status** field on the **Protocol List** displays **Successful**. If the import fails, the **Status** field displays the reason for the failure.
 9. Click **Back** to return to the **Application Management** page.

Deleting protocols

You can delete only user-defined protocols. You cannot delete system or predefined protocols.

Deleting a single protocol

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols on the **Protocol List** in the main pane of the **Application Management** page.
4. Click the **Delete** icon  for the protocol you want to delete.
5. Click **OK** to confirm the deletion of the selected protocol.
The **Protocol List** reflects the deletion of the selected protocol.

Deleting protocols in batches

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Protocol** tab.
NTA displays all protocols on the **Protocol List** in the main pane of the **Application Management** page.
4. Select one or more protocols.
5. Click **Batch Delete**.
6. Click **OK** to confirm the deletion of the selected protocols.

Managing application categories

Application Category management allows you to group similar applications into groups called application categories. NTA then analyzes the network flow records it receives based on application categories.

NTA provides many predefined application categories. You can create custom application categories and modify or delete predefined application categories to meet your specific needs.

Viewing the application category list

NTA displays all application categories in the application category list.

To view the application category list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.

NTA displays all application categories in the **Application Category List** in the main pane of the **Application Management** page.

Application category list contents

- **Name**—Contains the name of the application category. This field is a link to the **Application Category Details** page for more detailed information on the associated application category including the list of applications contained in the category.
- **Description**—Contains a description for the associated application category.
- **Type**—Identifies the application category. Options are **Application** and **Protocol**.
- **Pre-defined**—Identifies whether the associated application category is system or predefined or user-defined. A value of **Yes** in this field indicates that the associated

application category is system or predefined. A value of **No** in this field indicates that the associated application category is user-defined.

- **Modify**—Contains an icon  for modifying the associated application category.
- **Delete**—Contains an icon  for deleting the associated application category.

If the **Application Category List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Application Category List**.
- Click the **Last Page** icon  to page forward to the end of the **Application Category List**.
- Click the **Previous Page** icon  to page backward in the **Application Category List**.
- Click the **First Page** icon  to page backward to the front of the **Application Category List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Application Category List** to configure how many items per page you want to display.
For an **Application Category List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To query NTA for the most recent **Application Category List**, click **Refresh** in the upper left corner of the **Application Category List**.

You can sort the **Application Category List** by the **Name**, **Description**, **Type**, and **Pre-defined** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the various sort options specific to each field.

Querying the application category list

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.
NTA displays all application categories in the **Application Category List** in the main pane of the **Application Management** page.
4. In the upper right corner of the **Application Category List** page, enter a partial or complete name of the application categories to be queried in the query field, and click the **Query** icon  to filter out the unmatched application categories.
5. To filter application categories by using more query criteria, click the **Advanced** icon  next to the query field to expand the query criteria panel above the application category list. Specify one or more of the following query criteria:
 - **Name**—Enter a partial or complete name for the application category you want to search for in the **Name** field.
 - **Pre-defined**—To filter for application categories that are predefined, select **Yes** from the **Pre-defined** list. To filter for application categories that are user-defined, select **No** from the list. To include system or predefined and user-defined application categories, select **Not limited**.
6. Click **Query**.
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
7. Click **Reset** to restore the full contents of the **Application Category List**.

Adding an application category

You can create custom or user-defined application categories. This allows you to group one or more applications or protocols into a single category. NTA then combines and provides summarized statistical analysis and reporting for all applications or protocols in the category.

To add an application category:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.

NTA displays all application categories on the **Application Category List** in the main pane of the **Application Management** page.

4. Click **Add**.
The **Add Application Category** page opens.
5. In the **Name** field, enter a name for the application category.
6. In the **Description** field, enter a brief description for the application category.
7. From the **Type** list, select the type of application category you want to create.

Options are:

- o **Application**—Select this option if you want to create an application category that includes any of the Layer 4 or Layer 7 system or user-defined applications.
 - o **Protocol**—Select this option if you want to create an application category that includes any of the network and other protocols in NTA.
8. If you selected **Application** from the **Type** list, go to step 10.
 9. If you selected **Protocol** from the **Type** list, go to step 11.
 10. To add one or more applications to the category, click **Add** next to the **Application List** field.

The **Query Applications** dialog box displays an empty **Application List** in the lower portion of the dialog box.

To select applications to add to your category, you must first query the **Application List** as follows:

- a. In the **Query Applications** area of the dialog box, specify one or more of the following query criteria:
 - **Application**—Enter a partial or complete name for the application or applications you want to search for in the **Application** field.
 - **Pre-defined**—To search for applications that are predefined, select **Yes** from the **Pre-defined** list. To filter for applications that are user-defined, select **No** from the list. To include system or predefined and user-defined applications, select **Not limited**.
 - b. To display the full **Application List**, click **Query** without entering any search criteria.
The results of this query are displayed in the **Application List** below the **Query Applications** area. If the application you want to add does not exist in the **Application List**, add it as a user-defined application. For more information about adding applications to NTA, see "[Managing applications](#)."
 - c. Click **Query**.
The query results are displayed in the **Application List** below the **Query Applications** area.
 - d. Select the check boxes next to the applications you want to add to the application category.
 - e. Click **OK** to add the applications to the application category you want to create.
11. To add one or more protocols to the application category, click **Add** next to the **Application List** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To populate this list to select protocols to add to your category, you must first query the **Protocol List** as follows:

- a. In the **Query Protocols** area of the dialog box, specify one or more of the following query criteria:
 - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
 - **Pre-defined**—To search for protocols that are predefined, select **Yes** from the **Pre-defined** list. To filter for protocols that are user-defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.
 - b. To display the full **Protocol List**, click **Query** without entering any search criteria.

The results of this query are displayed on the **Protocol List** below the **Query Protocols** area.
 - c. Click **Query**.

The query results are displayed in the **Protocol List** below the **Query Protocols** area.
 - d. Select the check boxes next to the protocols you want to add to the application category.
 - e. Click **OK** to add the protocols to the application category you want to create.
12. Click **OK** to create the application category.

Modifying an application category

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.

NTA displays all application categories in the **Application Category List** in the main pane of the **Application Management** page.
4. Click the **Modify** icon  for the application category you want to modify.

The **Modify Application Category** page opens.
5. In the **Name** field, modify the name for the application category.
6. In the **Description** field, modify the description for the application category.

IMPORTANT:

After you create the application category **Type**, you cannot modify it but you can create a new definition with a revised **Type**.

If the application category type is **Application**, add or remove applications from the category.

7. To add applications, click **Add** next to the **Application List** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select applications to add to your category, you must first query the **Application List** as follows:

- a. In the **Query Applications** area of the dialog box, specify one or more of the following query criteria:
 - **Application**—Enter a partial or complete name for the applications you want to search for in the **Application** field.
 - **Pre-Defined**—From the **Pre-defined** list, click **Yes** to search for applications that are predefined. To filter for applications that are user-defined, select **No** from the list. To include system or predefined and user-defined applications, select **Not limited**.
- b. To display the full **Application List**, click **Query** without entering any search criteria.

The results of this query are displayed in the **Application List** below the **Query Applications** area. If the application you want to add does not exist in the **Application List**,

add it as a user-defined application. For more information about adding applications to NTA, see "[Managing applications](#)."

- c. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.

- d. Select the check boxes next to the applications you want to add to the application category.
- e. Click **OK** to add the applications to the application category you want to create.
- f. To delete an application from the list, highlight the application, click **Delete**, and then click **OK** to confirm the deletion.

If the application category type is **Protocol**, add or remove one or more protocols from the category.

8. Click **Add** next to the **Application List** field to add one or more protocols.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To populate this list to select protocols to add to your category, you must first query the **Protocol List** as follows:

- a. In the **Query Protocols** area of the dialog box, specify one or more of the following query criteria:
 - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
 - **Pre-Defined**—From the **Pre-defined** list, click **Yes** to search for predefined protocols. To filter for protocols that are user-defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.
 - b. To display the full **Protocol List**, click **Query** without entering any search criteria.

The results of this query are displayed on the **Protocol List** below the **Query Protocols** area.
 - c. Click **Query**.

The query results are displayed in the **Protocol List** below the **Query Protocols** area.
 - d. Select the check boxes next to the protocols you want to add to the application category.
 - e. Click **OK** to add the protocols to the application category you want to create.
 - f. To delete a protocol from the list, highlight the protocol, click **Delete**, and then click **OK** to confirm the deletion.
9. Click **OK** to accept your modifications to the application category.

Deleting application categories

You can delete predefined and user-defined application categories. Deleting application categories from NTA does not delete the data for associated application categories. The data for all deleted application categories are retained in the database in accordance with the NTA server configuration.

Deleting a single application category

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.

NTA displays all application categories in the **Application Category List** in the main pane of the **Application Management** page.
4. In the **Delete** field for the application category you want to delete, click the **Delete** icon .
5. Click **OK** to confirm the deletion of the selected application category.

The **Application Category List** will update to reflect the deletion of the selected application category.

Deleting application categories in batches

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Application Management** link.
3. In the upper left corner of the **Application Management** page, click the **Application Category** tab.

NTA displays all application categories in the **Application Category List** in the main pane of the **Application Management** page.

4. Select one or more application categories.
5. Click **Batch Delete**.
6. Click **OK** to confirm the deletion of the selected application categories.

Configuring NTA traffic analysis parameters

You can configure and tune many configuration parameters that define how data is analyzed and presented in NTA. This section describes the parameters that can be configured by an NTA administrator and the configuration settings.

Basic and advanced settings

To view and configure NTA basic and advanced configuration parameters:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Parameters** link.
NTA displays the configurable parameters in the main pane of the **Parameter Management** page.
3. To configure the basic settings:
 - **Report TopN**—Enter the number of entries you want analyzed and reported on for all TopN reports in the **Report TopN** field. The range for TopN entries is 1 to 50. After completing the configuration, click **OK** next to the parameter to enable the configuration.
 - **Log Lifetime**—Enter the number of days you want to retain NTA logs in the **Log Lifetime** field. The range for retaining logs is 1 to 1825 days (5 years). If you enable the data export function, the logs with log lifetime expirations are exported from the database to an external file. Use the log auditing tool to audit the traffic data of the exported file.
After completing the configuration, click **OK** next to the parameter to enable the configuration.
 - **Exported File Lifetime**—Enter the lifetime of the file to which the logs are exported. The lifetime of an exported file is the current time minus the time of logs in the file. It is set to 90 days by default. After completing the configuration, click **OK** next to the parameter to enable the configuration.
4. To configure the advanced settings:
 - **Max. Displayed Entries for Audit**—NTA enables you to search the original data source logs that were generated in a specific time period for traffic data containing specific ports and source and destination hosts. You can configure how many results NTA displays for a given search or audit in the **Max. Displayed Entries for Audit** parameter. Enter the number of search or audit results you want NTA to display in this field. The valid range of entries is 1 to 100000. After completing the configuration, click **OK** next to the parameter to enable the configuration.

- **Unknown Application Traffic Analysis**—NTA enables you to decide whether to analyze and report on applications that are unknown to NTA. Selecting **Enable** from the **Unknown Application Traffic Analysis** list will direct NTA to process and report on all applications that it cannot identify and label them as unknown applications. If you select **Disable**, NTA will discard any traffic for which it cannot identify the application. After completing the configuration, click **OK** next to the parameter to enable the configuration.
You can also add applications in NTA by using Layer 4 TCP or UDP port number, or by using Layer 7 regular expression pattern matching to identify applications that do not exist in NTA. For more information on adding applications, see "[Managing applications](#)."
- **Host Session Monitor**—The **Host Session Monitor** instructs NTA to process flow records on a host session basis. When you enable this feature, NTA will create a **Sessions** link located on the **Traffic Analysis and Audit** left navigation tree. This link contains reports for TopN session host statistics with drill-down capabilities to detailed session statistics for an individual host. Select **Enable** if you want to view TopN and individual host session statistics. Select **Disable** if you do not want to process and view host session statistics. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **ToS/MPLS Exp Traffic Analysis**—NTA provides statistical analysis and reporting of traffic based on ToS or MPLS Exp. To enable ToS or MPLS Exp analysis and reporting, select **Enable** from the **ToS/MPLS Exp Traffic Analysis** list. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **Baseline Analysis**—The Baseline Analysis feature provides an additional layer of analysis to NTA reports by including baseline trend data for a minimum of one week's worth of data. If sufficient data is available after this feature is enabled, a green trend line is displayed in the Traffic Trend graphs to represent the baseline data. Baseline data provides a useful comparison against current data to identify anomalies. Select **Enable** to include baseline analysis in NTA reports. Select **Disable** if you do not want to include baseline analysis in NTA reports. After completing the configuration, click **OK** next to the parameter to enable the configuration.

NOTE:

The baseline trend line is displayed seven days after the Baseline Analysis feature has been enabled.

- **Threshold Alarm**—The **Threshold Alarm** option allows you to configure alarm thresholds for interface traffic analysis tasks, interbusiness traffic analysis tasks, and host connection number. When the traffic or the number of host sessions exceeds the defined thresholds, an alarm notification is sent. Select **Enable** to add alarm notifications. Select **Disable** if you do not want to add alarm notifications. After completing the configuration, click **OK** next to the parameter to enable the configuration.
The **Threshold Alarm** option applies to all tasks globally. The options to configure thresholds are displayed when an interface traffic analysis task or interbusiness traffic analysis task is added or modified for those tasks that support thresholds. When you enable the Host Session Monitor feature, you can define thresholds for the number host sessions.
- **VPN Flux Detail Analysis**—The **VPN Flux Detail Analysis** option enables you to view traffic statistics for the interfaces in a VPN instance. Select **Enable** to view traffic for individual interfaces in a VPN instance. Select **Disable** if you want to view traffic statistics summarized for the VPN instance as a whole. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **Peak Traffic Analysis**—The **Peak Traffic Analysis** option enables you to view the peak rates of traffic analysis tasks and interfaces. Select **Enable** to view the peak rates of traffic analysis tasks and interfaces. Select **Disable** if you do not want to view the peak rates of traffic analysis tasks and interfaces. If you enable the Peak Traffic Analysis feature and select a time range in the **Query Time** of the **Traffic Query** area that is a minimum of six hours earlier than the current time, NTA displays the **Peak Rate** chart next to the **Traffic Trend** chart. After completing the configuration, click **OK** next to the parameter to enable the configuration.

- **Real Time Traffic**—The **Real Time Traffic** option enables NTA to automatically send query packets to obtain traffic statistics. This function can reduce the time delay caused by passively waiting for the traffic statistics packets. Select **Enable** if you want to use the **Real Time Traffic** function. Select **Disable** if you do not want to use this function. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **Enable TopN NTA Conversation Aggregation**—The **Enable TopN NTA Conversation Aggregation** option specifies whether to aggregate the TopN sessions. By default, NTA aggregates all sessions. With this feature enabled, NTA aggregates only information of the topN sessions by traffic. Information of other sessions is dropped. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **TopN NTA Conversations for Aggregation**—The **TopN NTA Conversations for Aggregation** option specifies the TopN value for the **NTA Conversation Aggregation TopN** field. After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **Data Collection Period for Topology Link Traffic**—The **Data Collection Period for Topology Link Traffic** option specifies the time duration during which topology link traffic statistics are collected. The time range is from 1 to 100000 hours, and the default value is 24 hours. For more information, see "[Collaborating with the platform topology](#)." After completing the configuration, click **OK** next to the parameter to enable the configuration.
- **DNS Setting**—The **DNS Setting** option allows you to enable or disable the DNS resolution function for NTA. After enabling this function, specify DNS server IP addresses. When a user queries the host information for an IP address, NTA uses the specified DNS servers to query the domain name for the IP address. You can specify only IPv4 addresses for DNS servers, and you can specify up to five DNS server IP addresses.
 - To enable the function, select **Enable** from the **DNS Setting** list.
 - To add a DNS server IP address, enter a DNS server IP address in the **DNS server IP** field, and then click **Add**. Repeat this operation to add more DNS server IP addresses.
 - To delete an existing DNS server IP address, select the IP address, and then click **Delete**.

After completing the configuration, click **OK** to enable the configuration.

Collaborating with the platform topology

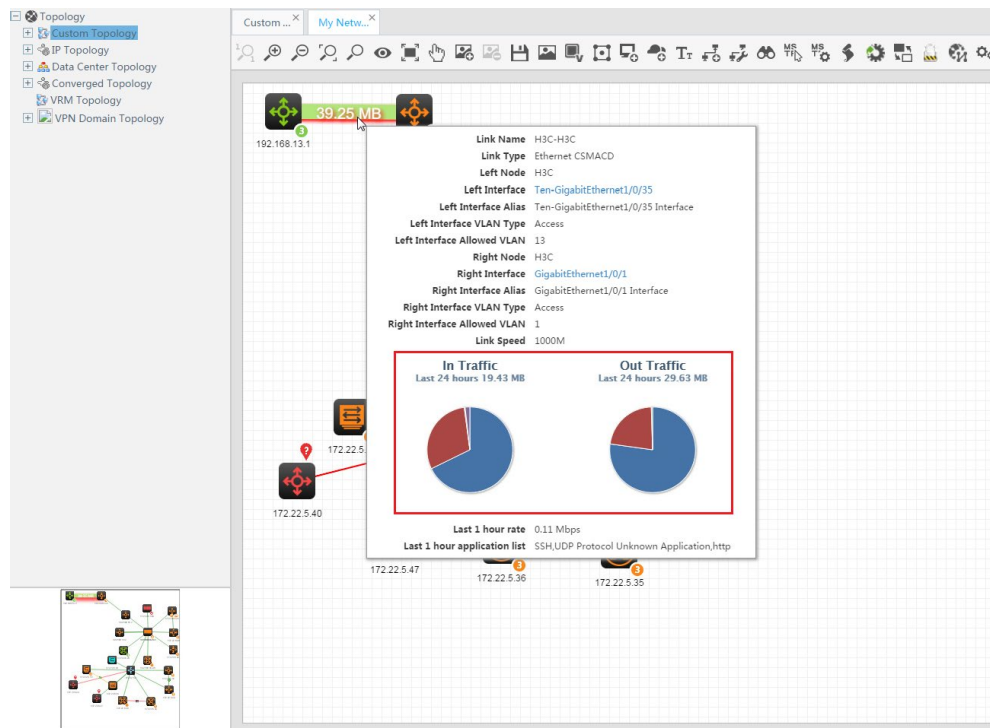
NTA can collaborate with the platform topology to display link traffic and traffic distribution in the platform custom topology. In the custom topology, click a device to view the following traffic statistics in the specified data collection period: link traffic, application traffic, and host task traffic.

Viewing application traffic of a link

In the platform custom topology, click the link of a device. You can view the following indexes in the specified period, as shown in [Figure 1](#):

- Total traffic.
- Inbound traffic.
- Outbound traffic.
- Top 5 applications.
- Average rate in the most recent 1 hour.
- Top 5 applications in the most recent hour.

Figure 1 Viewing application traffic of a link



NOTE:

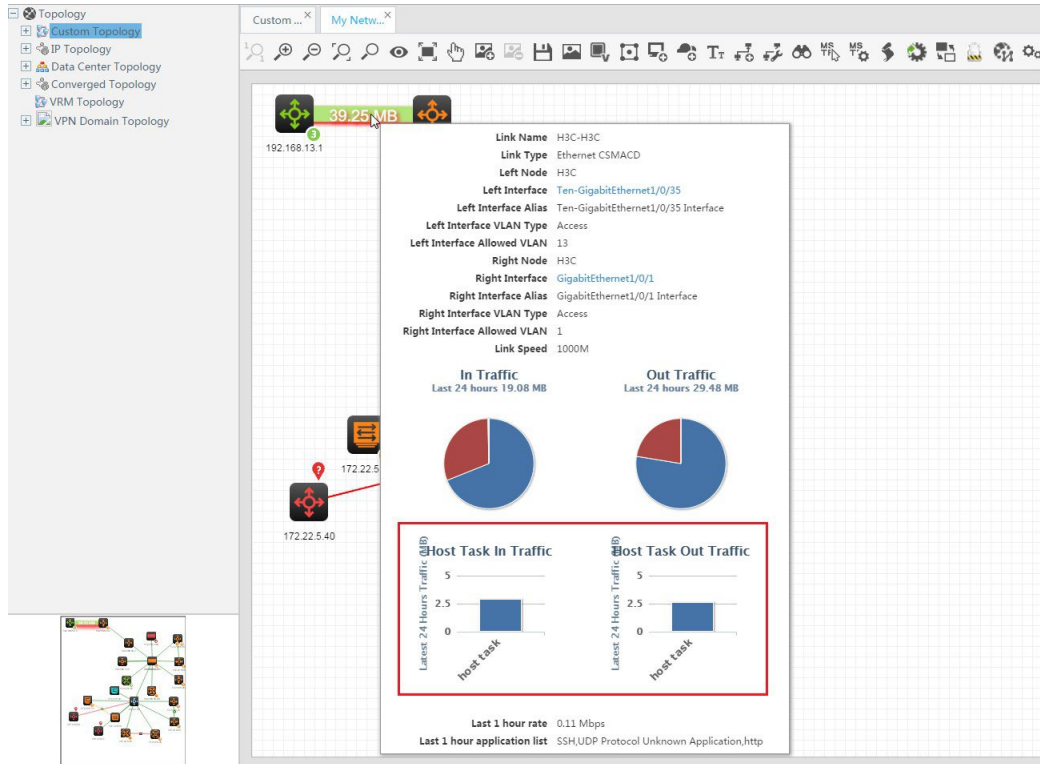
To view application traffic, you must add one or two interfaces of the link to the NTA interface traffic analysis task.

Click the link for an application in the pie chart. The traffic report for the application opens. For more information about the application report, see the application traffic trend and TopN application usage list described in "[Individual Application Reports](#)."

View host task traffic of a link

In the platform custom topology, click the link of a device. You can view the traffic of host tasks in the specified period, as shown in [Figure 2](#):

Figure 2 Viewing host task traffic of a link



NOTE:

To view host task traffic, you must add either of the two interfaces on the link to the NTA host traffic analysis task as the only monitoring interface for the task.

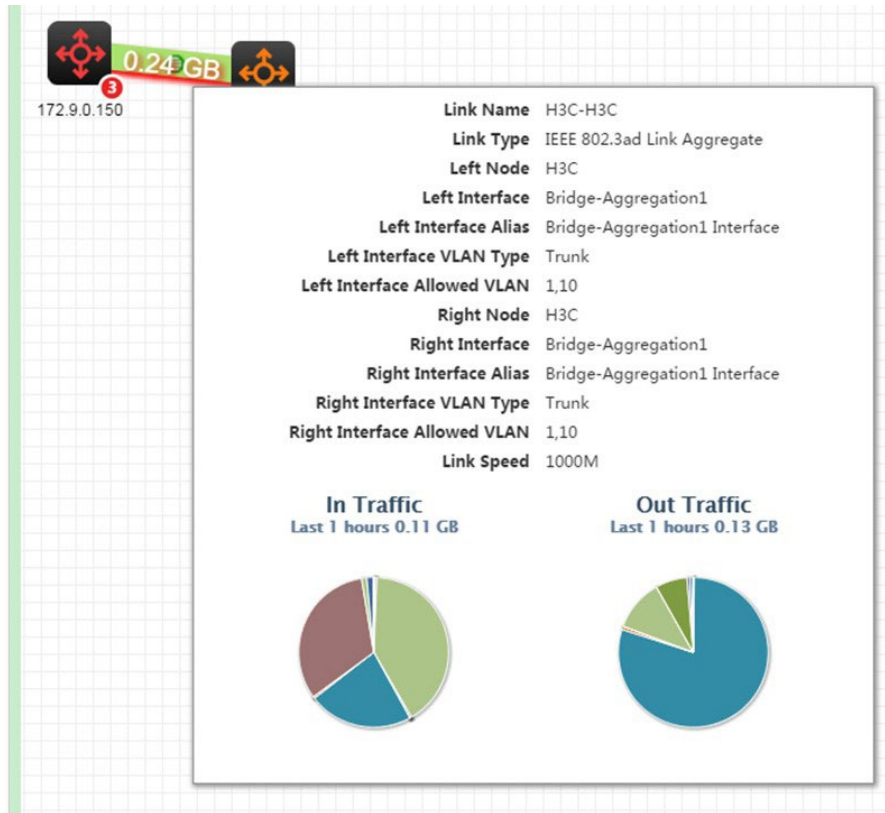
Click the host task traffic bar. The host task traffic page opens. For more information about the host task traffic, see "[Traffic reports](#)."

View aggregate interface application traffic

In the platform custom topology, click the aggregate link of a device. You can view the following indexes in the specified period, as shown in [Figure 3](#):

- Total traffic.
- Inbound traffic.
- Outbound traffic.
- Top 5 applications.

Figure 3 Viewing application traffic of an aggregate link



NOTE:

To view application traffic of an aggregate interface, you must add all aggregate interfaces at one or both ends of the link to the NTA interface traffic analysis task.

Using NTA filtering strategies

NTA is a NetStream v5/v9, NetFlow v5/v9 and sFlow v5 collection server, and is a centralized data collector and analyzer for devices that forward network flow records to it. Filter strategies in NTA enable you to define whether network flow records or the log packets that NTA receives are processed and analyzed by NTA or discarded. You can choose to process and analyze or discard packets based on their source or destination IP address, source or destination Layer 4 port number. You can also process or discard TCP, UDP, or ICMP traffic. Otherwise, analyze or discard traffic based on one or more combinations of source and destination IP address, port number and protocol.

Filter strategies consist of a name, description, default filter policy, and one or more filter conditions. Two types of filter policies are available: the **Discard** filter, which discards any packet that matches the filter conditions, and the **Receive** filter, which processes and reports on any packet that matches the filter conditions. The **Default Policy** defines how log packets are treated by default when the conditions of the packet do not match any of the filter conditions in the filter strategy.

A filter condition is a rule that defines the conditions under which log packets either are processed and analyzed or discarded. A filter strategy can have many filter conditions, but every filter strategy must have at least one filter condition. At least one of the filter conditions must contain a filter policy that does not match the default filter policy.

With filtering strategies, you can do the following:

- Tune which NetStream, NetFlow, or sFlow packets are processed and which are discarded.
- Filter by IP address and by port and protocol.

- Create multiple filter conditions for every filter strategy.

Every NTA server supports an unlimited number of filter strategies. For example, you can create filter strategies for every device or every VPN on every device that forwards NetStream, NetFlow, or sFlow traffic to NTA. Otherwise, create filter strategies by port number or traffic type across all devices that forward flow traffic to NTA. For example, you can create a simple filter that discards all ICMP traffic from NTA analysis and reporting.

This section describes NTA filtering features.

Viewing the filter strategy list

1. Select **Service > Traffic Analysis and Audit > Settings**.

2. Click the **Filter Strategy** link.

NTA displays all filter strategies in the **Filter Strategy List** in the main pane of the **Filter Strategy Management** page.

Filter strategy list contents

- **Name**—Contains the name for the associated filter strategy. The contents of this field link to the **Filter Strategy Details** for the associated filter strategy.
 - **Description**—Contains a description for the associated filter strategy.
 - **Modify**—Contains an icon  for modifying the associated filter strategy.
 - **Delete**—Contains an icon  for deleting the associated filter strategy.
3. To query NTA for the current **Filter Strategy List**, click **Refresh** in the upper left corner of the **Filter Strategy List**.

You can sort the **Filter Strategy List** by the **Name** and **Description** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing the filter condition list

Every filter strategy includes a filter condition list that contains all the filters for the associated filter strategy. From this list, you can view the configuration parameters of a filter condition, sort and delete filter conditions.

To view the filter condition list:

1. Select **Service > Traffic Analysis and Audit > Settings**.

2. Click the **Filter Strategy** link.

NTA displays all filter strategies in the **Filter Strategy List** in the main pane of the **Filter Strategy Management** page.

3. Click the name of the filter strategy to view the filter conditions list.

The list includes all filter conditions in the filter strategy.

Filter condition list contents

- **Priority**—Contains priority of the filter condition relative to the other filter conditions in the list.
- **Policy**—Contains the filter condition type for the associated filter. Two types of filter policies are available: the **Discard** filter, which discards any packet that matches the filter conditions and the **Receive** filter that processes and reports on any packet that matches the filter conditions.
- **Source Host**—Contains the IP address, if any, that is used to match the IP address contents of all IP packets processed by this filter condition.
- **Source Port**—Contains the Layer 4 port number that is used to match the source port contents of all IP packets processed by this filter condition.

- **Destination Host**—Contains the IP address, if any that is used to match the destination IP address contents of all IP packets processed by this filter condition.
- **Destination Port**—Contains the Layer 4 port number that is used to match the destination port contents of all IP packets processed by this filter condition.
- **Protocol**—Identifies the IP protocol for the associated filter condition. NTA supports TCP, UDP, ICMP and IPv6 ICMP protocols only.

Adding a filter strategy

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Filter Strategy** link.
NTA displays all filter strategies in the **Filter Strategy List** in the main pane of the **Filter Strategy Management** page.
3. Click **Add**.
The **Add Filter Strategy** page opens.
4. In the **Name** field, enter a name for this filter strategy.
The filter strategy name must be unique.
5. In the **Description** field, enter a brief description for this filter strategy.
Every filter strategy has a default filter policy and filter policies defined for every filter condition.
NTA provides two types of default filters: the default discard filter that discards any packet that does not match the filter condition list and the default receive filter that processes and reports on any packet that does not match the filter condition list. To use the default discard filter policy for the filter strategy, select **Discard** from the **Default Policy** list. To use the default receive filter policy for the filter strategy, select **Receive** from the list.
6. At the top of the filter condition list, click **Add** to add a filter condition.
The **Filter Condition Configuration** dialog box opens. You must add at least one filter condition to a filter strategy.
NTA supports two types of filters for each filter condition: the discard filter, which discards any packet that matches the filter conditions specified, and the receive filter that processes and reports on any packet that matches the filter conditions.
7. Select **Discard** from the **Policy** list if you want NTA to discard any packet that matches the specified filter conditions.
Select **Receive** from the list if you want NTA to process and include in reporting any packet that matches the filter conditions.



IMPORTANT:

At least one of the filter conditions you create must differ in policy from the **Default Policy**. For example, if you set **Receive** all packets as the default policy for the filter strategy, then you must create at least one filter condition that has **Discard** as its filter policy.

8. Enter the IP or IPv6 address and subnet mask in the **Source Host** field, if any, which are used to match the source IP address contents of all IP packets processed by this filter condition. This field is optional. Leaving this field blank directs NTA not to filter any packet by source address.
This field is optional and leaving this field blank directs NTA not to filter any packet by source address.

An IP address or an IP address and subnet mask for a range can be entered in dotted decimal notation or CIDR notation, using a backward slash (/) to separate the IP address from the subnet mask.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

A valid IPv4 address entry can be an IP segment:

1.1.1.1-1.1.1.100

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

A valid IPv6 address entry can be an IP segment:

a001:410:0:1::1-a001:410:0:1::100

9. Enter the Layer 4 port number in the **Source Port** field, if any, that is used to match the source port contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by source port number.

10. Enter the IP or IPv6 address in the **Destination Host** field, if any, that is used to match the destination IP address contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by destination address.

An IP address and subnet mask can be entered in dotted decimal notation or CIDR notation, using a backward slash (/) to separate the IP address from the subnet mask.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

11. Enter the Layer 4 port number in the **Destination Port** field, if any, that is used to match the destination port contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by destination port number.

12. To select a protocol to apply to this filter condition, highlight the protocol you want to use from the **Protocol** list.

Options are **TCP**, **UDP**, **ICMP** and **IPv6 ICMP**.

13. Click **OK** to create the filter condition.

14. Repeat steps 11 through 13 to add more conditions.

NTA prioritizes the processing of filter conditions based on their order of appearance in the **Filter Condition List**. NTA applies filter conditions on a first match first serve basis for all filter conditions. Filter conditions are matched based on the order of appearance in the filter condition list and filter conditions are applied from up to down. If a filter condition is matched, the data is processed according to the matched filter condition without applying the remaining filter conditions. If no filter condition is matched, the default policy is applied.

15. To reprioritize the filter conditions in the **Filter Condition List**, do one of the following:

- In the **Sort** field associated with the filter condition you want to move up in the list, click the **Move Up** icon .
 - In the **Sort** field associated with the filter condition you want to move down in the list, click the **Move Down** icon .
16. Click **OK** to create the filter strategy.
- After you create a filter strategy, you can apply it to one or more of the NTA servers listed in the **NTA Server List** under **Server Management**. For more information about adding a filter strategy to an NTA server, see ["Modifying an NTA server configuration."](#)

Modifying a filter strategy

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Filter Strategy** link.
NTA displays all filter strategies in the **Filter Strategy List** in the main pane of the **Filter Strategy Management** page.
3. Click the **Modify** icon  for a filter strategy.
The **Modify Filter Strategy** page opens.
4. In the **Name** field, modify the name of this filter strategy.
The filter strategy name must be unique.
5. In the **Description** field, modify the description for this filter strategy.
Every filter strategy has a default filter policy and filter policies defined for every filter condition.
NTA provides two types of default filters: the default **Discard** filter that discards any packet that does not match the filter condition list, and the default **Receive** filter that processes and reports on any packet that does not match the filter condition list. To use the default discard filter policy for the filter strategy, select **Discard** from the **Default Policy** list. To use the default receive filter policy for the filter strategy, select **Receive** from the list.
If you change the **Default Policy**, at least one of your filter conditions cannot contain the same policy type as the **Default Policy** you have configured for the filter strategy. If you modified the **Default Policy** from **Receive** to **Discard**, then you must have at least one filter condition that uses the **Receive** filter policy.
6. To add a filter condition to the existing filter condition list, click **Add** at the top of the filter condition list.
You must have at least one filter condition for a filter strategy.
The **Filter Condition Configuration** dialog box opens.
NTA supports two types of filters for each filter condition: the **Discard** filter, which discards any packet that matches the filter conditions specified, and the **Receive** filter that processes and reports on any packet that matches the filter conditions.
7. To discard any packet that matches the specified filter conditions, select **Discard** from the **Policy** list.
To process and include in reporting any packet that matches the filter conditions, select **Receive** from the list.



IMPORTANT:

At least one of the filter conditions you create must differ in policy from the **Default Policy**. For example, if you set **Receive** all packets as the default policy for the filter strategy, then you must create at least one filter condition that has **Discard** as its filter **Policy**.

8. Enter the IP address and subnet mask in the **Source Host** field, if any, which will be used to match the source IP address contents of all IP packets processed by this filter condition. This

field is optional and leaving this field blank directs NTA not to filter any packet by source address.

This field is optional and leaving this field blank directs NTA not to filter any packet by source address.

An IP address and subnet mask can be entered in dotted decimal notation or CIDR notation, using a backward slash (/) to separate the IP address from the subnet mask.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

9. Enter the Layer 4 port number in the **Source Port** field, if any, used to match the source port contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by source port number.

10. Enter the IP address in the **Destination Host** field, if any, used to match the destination IP address contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by destination address.

An IP address and subnet mask can be entered in dotted decimal notation or CIDR notation, using a backward slash (/) to separate the IP address from the subnet mask.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

11. Enter the Layer 4 port number in the **Destination Port** field, if any, used to match the destination port contents of all IP packets processed by this filter condition.

This field is optional and leaving this field blank directs NTA not to filter any packet by destination port number.

12. From the **Protocol** list, highlight the protocol you want to use to select a protocol to apply to this filter condition.

Options are **TCP**, **UDP**, **ICMP**, and **IPv6 ICMP**.

13. Click **OK** to create the filter condition.

Repeat steps 11 through 13 to add more conditions.

NTA prioritizes the processing of filter conditions based on their order of appearance in the **Filter Condition List**. NTA applies filter conditions on a first match first serve basis for all filter conditions. Filter conditions are matched based on the order of appearance in the filter

condition list and filter conditions are applied from up to down. If a filter condition is matched, the data is processed according to the matched filter condition without applying the remaining filter conditions. If no filter condition is matched, the default policy is applied.

14. Do one of the following:
 - o In the sort field associated with the filter condition you want to move up in the list, click the **Move Up** icon  to reprioritize the filter conditions in the **Filter Condition List**.
 - o In the sort field associated with the filter condition you want to move down in the list, click the **Move Down** icon  to reprioritize the filter conditions in the **Filter Condition List**.
15. To delete a filter condition, click the **Delete** icon .
16. Click **OK** to accept your changes to the filter strategy.

Deleting a filter strategy

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Filter Strategy** link.
NTA displays all filter strategies in the **Filter Strategy List** in the main pane of the **Filter Strategy Management** page.
3. Click the **Delete** icon  for a filter strategy.
4. Click **OK** to confirm the deletion of the filter strategy.

Database space management

The NTA Database Space feature provides current NTA database disk usage and usage trend statistics over the last twenty-four hours. Otherwise, query NTA for usage trends for the last 7 days, 30 days, or 3 months, or for a user-defined time range. This feature, when combined with the threshold and action parameters (**Usage Threshold of the Database Disk** and **When Database Disk Usage Reaches Threshold**, respectively) of an NTA server configuration, enables you to proactively manage disk space usage and ensure adequate disk space for uninterrupted NTA functioning.

The granularity of the database space usage information varies with the span of the query time. The longer the time span of the query, the coarser the granularity. The shorter the time span of the query, the finer the granularity. The finest granularity is 10 minutes. When the NTA service module and database are installed separately, this feature is not available.

This section describes the Database Space feature for viewing current NTA database disk space usage. For information on viewing and configuring the database threshold and action settings, see "[Managing NTA servers](#)."

Viewing current disk space usage statistics

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Database Space** link.
NTA displays all file and disk space usage statistics in the database space usage list in the main pane of the **Database Space** page.

Database space usage list contents

- **Server Name**—Contains the name of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server. The contents of this field are a link for viewing more detailed usage statistics for the associated server.
- **Server Description**—Contains a description for the associated NTA server.

- **Data File Usage**—Contains the most recent percent consumption of all available data files for the associated server. You can access more detailed statistics by clicking the link in the **Server Name** field.
- **Disk Usage**—Contains the current percent consumption of all available disk space allocated for the associated server.

Viewing database usage trend statistics

NTA enables you to view the NTA database usage over time.

To view the NTA disk space usage trends:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Database Space** link.

NTA displays all file and disk space usage statistics in the database space usage list in the main pane of the **Database Space** page.

3. Click the contents of the **Server Name** field for the NTA server whose statistics you want to view.

The database usage trends for the associated server are displayed.

By default, a graphical representation of database disk space usage over the last twenty-four hours is displayed in the **Database Space Usage Trend** graph.

NTA displays the tabular data for usage trends over the last twenty-four hours in the lower half of the page.

From the **Time** list in the **Query Database Space Usages** area of the page, select the time range for which you want to view database usage statistics to change the time range for this graph and table. Options are **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, and **Custom**.

4. To enter a user-defined time range, select **Custom** from the **Time** list.
 - **Start Time**—To autopopulate this field, click the **Calendar** icon . A popup calendar is displayed. Select the start date and time from the calendar. Adjust the hour and minute values through the slide bars.
 - **End Time**—To autopopulate this field, click the **Calendar** icon . A popup calendar is displayed. Select the end date from the calendar. Adjust the hour and minute values through the slide bars.
5. Click **Query**. The page displays the result of your query.
6. Click **Reset** to display the default 24-hour usage trend view.

Data export

The Data Export feature allows the NTA server to export the traffic data in the database to the external data files. An operator can use the auditing tool provided by NTA to audit the network traffic data in the data files. A data file can be saved on a server for up to 90 days, and is deleted automatically after 90 days.

After you enable data export, either log lifetime or data space alarm can trigger data export.

- **Log Lifetime**—NTA checks the lifetime of each log in the database at around 3:00 every day. A log whose lifetime expires is exported to a data file. The data export triggering condition always takes effect, regardless of whether data export is enabled. The log lifetime is set in the NTA system parameters. For information about modifying the log lifetime, see "[Configuring NTA traffic analysis parameters](#)."

- **Data space alarm**—With the **Trigger Data Export by Data Space Alarm** option selected, when the data space alarms occur, the NTA server automatically exports the oldest data day by day until the data space alarms are eliminated. The data space alarms are generated based on the data file usage and the usage of the disk where the database resides. An operator can modify the threshold for the usage of the disk where the database resides. For information about modifying the threshold, see "[Managing NTA servers](#)."

NTA can export only the data of IPv4 traffic, and cannot export the data of IPv6 traffic. The data of IPv6 traffic can only be deleted according to the triggering conditions.

Viewing the data export config list

1. Select **Service > Traffic Analysis and Audit > Data Export**.

The **Data Export Config List** is displayed in the main pane of the **Data Export** page.

Data Export Config List contents

- **Server Name**—Contains the name of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server.
- **Server IP**—Contains the IP address of the NTA server. By default, this contains the loopback address of the local server when NTA is deployed on the master server.
- **Status**—This field indicates whether data export is enabled for the NTA server. Options are **Enabled** and **Disabled**.
- **Last Time of Export**—Last time when the NTA server exported data.
- **Data Export Log**—Contains an icon  for viewing the data export logs of the related NTA server.
- **Modify**—Contains an icon  for modifying the data export configuration of the related NTA server.

Querying the data export logs

1. Select **Service > Traffic Analysis and Audit > Data Export**.

The **Data Export Config List** is displayed in the main pane of the **Data Export** page.

2. To view the data export logs of an NTA server, click the **Data Export Log** icon .

Data Export Log List

- **Date of Exported Data**—Date when the exported data is generated.
 - **Table Name**—Exported table name of the database.
 - **File Name**—Name of the exported file.
 - **Exported Time**—Time when the data export is performed.
 - **Count**—Number of entries in the exported file.
 - **Export Result**—Result of the export.
3. Specify the following query criterion:
 - **Date of Exported Data**—Enter the time range for the data export logs. Enter the start time in the **From** field and enter the end time in the **To** field in YYYY-MM-DD format. Or, click the input boxes and manually select the start time and end time on calendar that is displayed.
 4. Click **Query** to view the data export logs matching the criteria. Click **Reset** to clear all query criteria.

Modifying the data export configuration

1. Select **Service > Traffic Analysis and Audit > Data Export**.
The **Data Export Config List** is displayed in the main pane of the **Data Export** page.
2. Click the **Modify** icon .
3. Select the **Enable Data Export** option to enable the data export function.
After you enable the data export function, you can configure the **Trigger Data Export by Data Space Alarm**, **Path of Exported File**, and **Enable FTP Upload** parameters.
If you do not select the **Trigger Data Export by Data Space Alarm** option, the NTA server can export data according to only the log lifetime. With the **Trigger Data Export by Data Space Alarm** option selected, when the data space alarms occur, the NTA server automatically exports the oldest data day by day until the data space alarms are eliminated.
4. Enter the absolute path of the exported file on the NTA server.
5. Select **Enable FTP Upload** and configure the following parameters to upload the exported files to an FTP server as needed:
 - **FTP Server IP**—Enter the IPv4 address of the FTP server.
 - **FTP Port**—Enter the port number of the FTP server, which must be the same as the port setting on the FTP server. The default is 21.
 - **FTP Main Directory**—Enter the FTP main directory. For example, **/home/transfer**. Make sure the FTP user has read and write permissions to this directory.
 - **FTP Username**—Enter the FTP username.
 - **FTP Password**—Enter the FTP user password.
 - **Delete the file after saving it through FTP**—Select this option to enable the system to delete the original files from the export directory after they are uploaded to the FTP server. If you do not select this option, the original files are still kept in the export directory after the upload.
6. Click **OK** to complete modifying the data export configuration.

Auditing the exported data

NTA provides an auditing tool. An operator can use the log auditing tool to audit the traffic data of the exported file. The auditing tool depends on JRE. To guarantee normal operation of the auditing tool, make sure you have downloaded the latest JRE.

To audit the exported data:

1. From the top navigation bar, select **Service > Traffic Analysis and Audit > Data Export**.
The **Data Export Config List** is displayed in the main pane of the **Data Export** page.
2. Click **Log File Audit** to download and start the auditing tool.
The auditing tool can perform only general audit for the exported data. Use the auditing tool in the same way as you use the auditing tool of UBA. For information about using an auditing tool, see *HPE Intelligent Management Center v7.3 User Behavior Auditor Administrator Guide*.

Anomaly detection management

NTA collects statistics on traffic flow records and compares the statistics with the thresholds in the anomaly detection templates. If a threshold is crossed, NTA issues an alarm.

NTA has a series of predefined anomaly detection templates. You cannot add or delete templates, but you can modify them.

The anomaly detection templates fall into two categories: templates that use the same parameters and templates that use anomaly type-specific parameters.

The following templates use the same parameters:

• TCP Null Scan	• TCP Fin Scan	• TCP Syn Fin Scan
• TCP Xmas Scan	• UDP Bomb Attack	• Snork Attack
• UDP Flood Attack	• Invalid ToS	• Land Attack
• Invalid IP Protocol	• Corrupt IP Option	• Time Stamp IP Option
• Source Route IP Option	• Record Route IP Option	• Security IP Option
• Stream ID IP Option	• Fragmented ICMP Packet	• ICMP Redirects
• ICMP Destination Unreachable	• ICMP Request Excess	• ICMP Reply Excess
• ICMP Source Quench	• ICMP Parameter Problem	• ICMP Time Exceeded

The following templates use anomaly type-specific parameters:

- DNS Rogue Hack
- Ping of Death Attack
- Large ICMP Packet
- DHCP Offer Packet

Viewing the anomaly detection list

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Anomaly Detection** link.
NTA displays **Anomaly Detection List** and **Basic Configuration** in the **Anomaly Detection** page.
3. Modify the basic configuration for anomaly detection:
 - **Time Window**—Select the time window mode for generating anomaly alarms:
 - **Fixed Time Window**—Select this option to take time as a series of fixed-length time windows. Anomaly detection generates only one alarm within every time window duration.
 - **Sliding Time Window**—Select this option to use sliding time windows. The start point of a sliding time window is the time when the last anomaly alarm was generated. After an alarm is generated, anomaly detection does not generate another alarm for the same attack within the specified time duration.

For your selection to take effect, click **OK** next to the parameter.
 - **Window Size**—Set the size of the time window, in the range of 1 to 10 minutes. For your selection to take effect, click **OK** next to the parameter.
4. View the **Anomaly Detection List**:
 - **Name**—Anomaly that NTA can detect.
 - **Description**—Description of the anomaly, name of the anomaly detection template.
 - **Threshold**—Anomaly threshold. When this threshold is crossed, NTA sends an alarm.
 - **Alarm Level**—Level of the alarm, **Critical** by default.
 - **Enable**—Whether anomaly detection is enabled for the item.
 - **Modify**—To modify the anomaly detection template, click the **Modify** icon .

Modifying an anomaly template that uses the common parameters

This section explains how to modify anomaly templates that use the common parameters.

To modify the TCP Fin Scan template:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Anomaly Detection** link.
NTA displays **Anomaly Detection List** and **Basic Configuration** in the **Anomaly Detection** page.
3. Click the **Modify** icon  for **TCP Fin Scan**.
The **Modify Anomaly Detection** page opens. The name and description settings cannot be changed.
4. Adjust the alarm threshold.
NTA issues an alarm when the number of detected TCP FIN Scan packets reaches or exceeds the threshold.
5. Select an alarm level. Options are **Critical**, **Major**, **Minor**, **Warning**, and **Info**.
6. Select whether to enable anomaly detection for TCP FIN Scan packets.
7. Click **OK**.

Modifying an anomaly template that uses anomaly type-specific parameters

This section describes the anomaly templates that use anomaly type-specific parameters and common parameters.

DNS Rogue Hack

NTA uses the IP addresses of valid DNS servers to determine which packets are from valid DNS servers. The DNS Rogue Hack template uses one specific parameter:

- **Host IP**—Enter the IP address and, optionally, the network mask of a valid DNS server in this field and click **Add** to add an entry to the **Host IP List**.

The **Host IP List** displays the IP addresses of all valid DNS servers. To remove a DNS server from the list, select its IP address and click **Delete**.

Ping of Death Attack

NTA determines whether a ping packet is valid based on its size. The Ping of Death Attack template uses one specific parameter:

- **Packet Size**—Enter the size threshold for ping packets.

If the size of a ping packet exceeds the threshold, NTA considers a Ping of Death attack occurred and issues an alarm.

Large ICMP Packet

NTA determines whether an ICMP packet is valid based on its size. The Large ICMP Packet template uses one specific parameter:

- **Packet Size**—Enter the size threshold for ICMP packets.

If the size of an ICMP packet exceeds the threshold, NTA considers a Large ICMP Packet anomaly occurred.

DHCP Offer Packet

NTA uses the IP addresses of valid DHCP servers to determine which packets are from valid DHCP servers. The DHCP Offer Packet template uses the following parameters:

- **Host IP**—Enter the IP address and, optionally, the network mask of a valid DHCP server in this field and click **Add** to add an entry to the **Host IP List**.

The **Host IP List** displays the IP addresses of all valid DHCP servers. To remove a DHCP server from the list, select its IP address and click **Delete**.

- **Monitor Date**—Select the days for DHCP packet monitoring. Options are:
 - **Monday**
 - **Tuesday**
 - **Wednesday**
 - **Thursday**
 - **Friday**
 - **Saturday**
 - **Sunday**
- **Start Time/End Time**—Enter the monitoring time range during the monitoring day, in hh:mm format.

Host session monitoring

This chapter provides information on Host Session Monitoring in NTA, beginning with how NTA analyzes network flow records to report on network traffic from host session perspective. This chapter looks at the reporting options for host session monitoring and reviews configuration issues around host session monitoring and the reports they generate. This chapter concludes with a survey of the summary reports for all NTA servers and a look at the more granular reports for the devices configured in NTA server.

Host session monitoring overview

NTA analyzes network flow data for host sessions. Devices configured on an NTA server send flow data to the server. The NTA server parses the flow data and provides statistics on device host sessions and NTA server sessions. NTA then generates an NTA host session report according to the statistical data of all NTA servers. NTA allows you to set threshold alarms for host sessions. If you want to generate alarms based on the data collected by devices configured on NTA servers, set the threshold alarm function in the device host sessions monitor. By setting the threshold alarm parameters, you can quickly identify the hosts that have an abnormal number of connections on the network.

Host session monitoring reporting

After you enable the Host Session Monitor feature in the NTA traffic analysis parameters, NTA creates a **Sessions** entry under the **Traffic Analysis and Audit** area of the left navigation tree. Click the **Sessions** link to view the host session report of all NTA servers.

To view the host session report of a single NTA server, move your mouse pointer to the shortcut menu icon **>>>** next to the **Sessions** link. The **Sessions** shortcut menu displays the names of all NTA servers. Click the link for a name to view the host session report of a single NTA server.

To view the host session report of a device attached to an NTA server, click the **Expand** icon **▶** next to an NTA server on the shortcut menu to display the devices which send traffic statistics packets to the NTA server. Click the device name link for a device to view the host session report of a single device.

Host session monitoring configuration considerations

Host session monitoring is a global configuration. By default, NTA does not provide statistics on host sessions. Therefore, you must enable this feature in the NTA traffic analysis parameters. For instructions, see "[Configuring NTA traffic analysis parameters](#)."

You must enable network flow data on the devices you want to monitor and report on using NTA.

Managing host session monitoring

After host session monitoring is enabled, NTA can process, analyze, and report on network flow data. This section explains how to set threshold alarm parameters for host sessions in NTA.

Setting threshold alarm parameters for host sessions

You can generate alarms based on data collected by devices configured on NTA servers by setting the threshold alarm parameters for device host sessions.

To set threshold alarm parameters:

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. Move your mouse pointer to the shortcut menu icon  next to the **Sessions** link. The **Sessions** shortcut menu displays the names of all NTA servers.
3. Click the **Expand** icon  next to an NTA server on the shortcut menu to display the devices which send traffic statistics packets to the NTA server.
4. Click the device name for which you want to set the threshold alarm.
The host session report page is displayed.
5. Click the **Threshold** icon  located at the upper right corner of the host session report page. The **Threshold Alarm Settings** dialog box is displayed.
6. Select **Enable** from the **Threshold Alarm** list to generate alarms based on the data collected by this device and the thresholds you configured. Select **Disable** if you do not want to generate alarms.
If you selected **Enable**, the page displays the threshold alarm configuration parameters.
7. Configure the alarm threshold settings.
 - o **Trigger**—Define the conditions under which the threshold is triggered. This option has two configuration parameters: the duration and the number of times the threshold must be exceeded.
The duration defines the amount of time in which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the duration from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3**.
 - o **Threshold**—Enter the threshold value that must be exceeded before NTA generates an alarm.
 - o **Severity**—This field indicates the severity level of the triggered threshold alarms. The value must be **Major**.
 - o **Discard Length**—This field specifies the time interval in which a triggered alarm will not be re-sent. Select the time interval from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
8. Click **OK**.

Viewing host session monitor reports

NTA provides different levels of reports for host sessions. The highest level provides summary reports for the host sessions of all NTA servers. You access these reports by clicking the **Sessions** branch of the left navigation tree under the **Traffic Analysis and Audit** area.

NTA also provides more granular reports, including the summary host session report for each NTA server and the summary host session report for each device. Move your mouse pointer to the shortcut menu icon  next to the **Sessions** link. The **Sessions** shortcut menu displays the entries to these reports.

This section describes the report options available for host sessions. It also describes navigating to the host sessions report, summary reports available for all NTA servers configured in NTA, and reports and features available for NTA server host sessions and device host sessions.

Navigating to the host session monitor reports

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. To view summary reports for the host sessions of all NTA servers, click **Sessions** under the **Traffic Analysis and Audit** area.
3. To view the summary data for the host sessions of a single NTA server, move your mouse pointer to the shortcut menu icon >>> next to the **Sessions** link. The **Sessions** shortcut menu displays the names of all NTA servers. Click the name link for a NTA server to view the summary host session number data of the NTA server.
4. To view the summary host session number data of a device attached to an NTA server, click the **Expand** icon ▶ next to an NTA server on the shortcut menu to display the devices that send traffic statistics packets to the NTA server. Click the device name link for a device to view the summary host session number data of the device.

Summary reports for host sessions

Summary reports are the highest-level reports for all NTA server host sessions. You access these reports by clicking **Sessions** of the left navigation tree under the **Traffic Analysis and Audit** area.

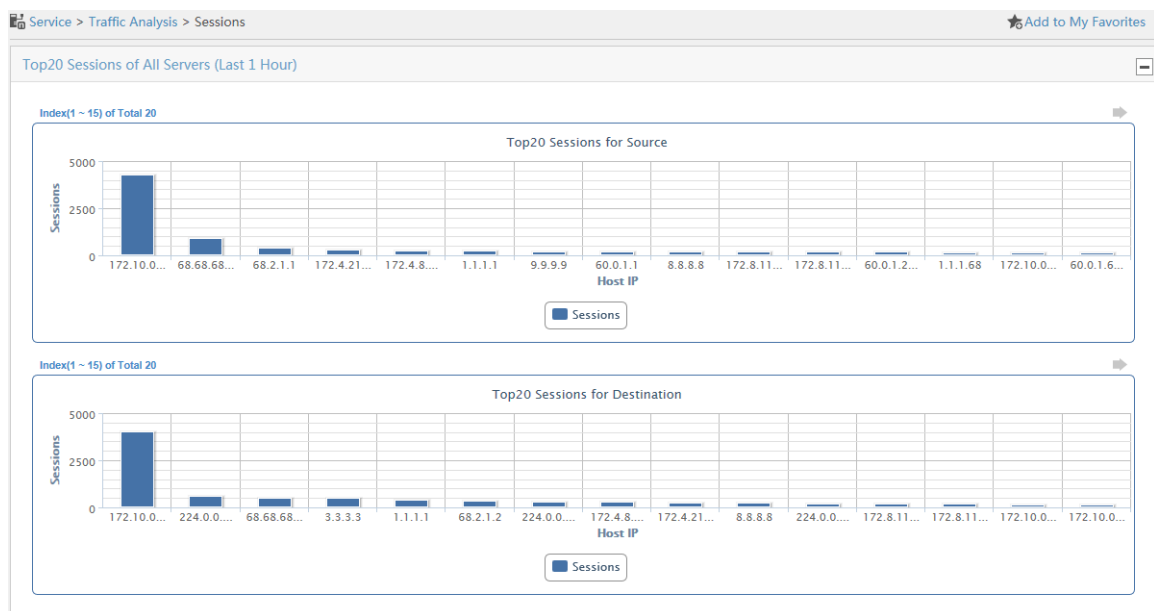
TopN Sessions Of All Servers (Last 1 Hour)

This graph displays host sessions in the last hour for the source and destination hosts of all NTA servers. It has two bar charts:

- **TopN Sessions for Source** provides statistics on sessions for the source hosts of all NTA servers.
- **TopN Sessions for Destination** provides statistics on sessions for the destination hosts of all NTA servers.

Access this graph by clicking **Sessions** of the left navigation tree. NTA can automatically adjust the number of bars displayed in the graph according to the window size of the browser. To view the bars that are not displayed in the current graph, click the **Page Up** icon ◀ or **Page Down** icon ▶ at the upper right of the graph.

Figure 4 TopN Sessions of All Servers (Last 1 Hour)



TopN Sessions of Selected Servers (Last 1 Hour)

The graph is displayed only when NTA is deployed on multiple servers in distributed mode. The graph displays the number of source and destination host sessions of one or more NTA servers in the last hour. The display effect is the same as the **TopN Sessions of All Server** report.

By default, the graph does not display the number of host sessions of any NTA server. The graph displays the number of host sessions of NTA servers after you specify one or more NTA servers.

To specify NTA servers:

1. Click the **Select Server** link at the upper right of the **TopN Sessions of Selected Servers** title bar.

The **Choose Server** dialog box opens.

2. Click the boxes next to the NTA server names to select NTA servers you want to view in this report.
3. Click **OK**.

The page will update to display the **TopN Sessions of Selected Servers** reports for the selected NTA servers.

Detailed reports for host sessions

NTA provides a suite of reports for viewing the host sessions data from different perspectives.

Individual NTA server host session report includes two lists for source and destination host sessions in a NTA server. The two lists include the source and destination host IP address, number of sessions for the associated source or destination, and the maximum session generation rate by the source or destination. The host IP address is a link for navigating to the host session details report.

Device host session report includes two lists for source and destination host sessions in a device. The two lists include the source and destination host IP address, number of sessions for the associated source or destination, and the maximum session generation rate by the source or destination. The host IP address is a link for navigating to the host session details report.

Host session details report includes the total sessions for host in 1 minute and the data samples for host sessions generate per second.

Individual NTA Server Host Sessions Report

This report contains two lists for the source or destination host sessions on an NTA server. The lists provide the source or destination host IP address, the sessions for the associated source or destination, and the maximum session generation rate, in seconds, by the source or destination. The host IP address is a link for navigating to the host session details report.

Query Sessions

NTA allows you to change the filter criteria for the individual NTA server host sessions report. You can change the default settings for source or destination session pair information to customize the lists displayed in the **Query Sessions** area.

To change the filter criteria for the report:

1. Enter one or more of the following search criteria:
 - o **Source**—Enter the IP address or address range. To enter the IP address for a single interface, use dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- **Destination**—Enter the IP address or address range. To enter the IP address for a single interface, use dotted decimal notation.
- 2. To change the default time range for the tables on this page, select the time range from the **Query Time** list in the **Query Sessions** area. Options are:
 - **Last 1 minutes**
 - **Last 2 minutes**
 - **Last 5 minutes**
 - **Last 10 minutes**
 - **Last 30 minutes**
 - **Last 1 hours**
 - **Last 3 hours**
 - **Last 6 hours**
 - **Start Time**—Displays the start time for the report.
 - **End Time**—Displays the end time for the report.
- 3. Click **Display**.

The page displays the results of your query.

TopN Sessions List

The individual NTA server host sessions report contains two lists:

- **TopN Sessions List for Source** lists the source host IP address, the number of sessions for the associated source, and the maximum session generation rate by the source host. The host IP address is a link for navigating to the host session details report.
- **TopN Sessions List for Destination** lists the destination host IP address, the number of sessions for the associated destination, and the maximum session generation rate by the destination host. The host IP address is a link for navigating to the host session details report.

Figure 5 TopN Sessions List

Top20 Sessions List for Source			Top20 Sessions List for Destination		
Source	Sessions	Average Rate (sessions/second)	Destination	Sessions	Average Rate (sessions/second)
172.10.0.60	7	0.03	224.0.0.6	15	0.08
172.10.0.71	6	0.03	224.0.0.5	10	0.08
172.200.0.2	5	0.03	255.255.255.255	4	0.02
0.0.0.0	4	0.02	169.254.255.255	2	0.02
169.254.142.30	2	0.02	1.1.1.1	1	0.02
1.1.1.60	1	0.02			
60.0.1.60	1	0.02			
60.5.0.3	1	0.02			
172.5.0.1	1	0.02			
172.10.0.1	1	0.02			
172.10.0.72	1	0.02			
172.10.0.73	1	0.02			
172.200.0.3	1	0.02			

For more information about the host session details report, see "[Host Session Details Report](#)."

Device Host Sessions Report

This report contains two lists for source or destination host sessions on a device. The lists provide the source or destination host IP address, the number of sessions for the associated source or destination, and the maximum session generation rate by the source or destination. The host IP address is a link for navigating to the host session details report.

Query Sessions

NTA allows you to change the filter criteria for the device host session report. You can change the default settings for source or destination session pair information to customize the lists displayed in the **Query Sessions** area.

1. Enter one or more of the following search criteria:
 - o **Source**—Enter the IP address or address range. To enter the IP address for a single interface, use dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/64
 - o **Destination**—Enter the IP address or address range. To enter the IP address for a single interface, use dotted decimal notation.
2. To change the default time range for the tables on this page, select the time range from the **Query Time** list in the **Query Sessions** area. Options are:
 - o **Last 1 minutes**
 - o **Last 2 minutes**
 - o **Last 5 minutes**
 - o **Last 10 minutes**
 - o **Last 30 minutes**
 - o **Last 1 hours**
 - o **Last 3 hours**
 - o **Last 6 hours**
 - o **Start Time**—Displays the start time for the report.
 - o **End Time**—Displays the end time for the report.
3. Click **Display**.
The page displays the results of your query.

TopN Sessions List

The device host sessions report contains two lists:

- **TopN Sessions List for Source** lists the source host IP address, the number of sessions for the associated source, and the maximum generated session rate by the source host. The host IP address is a link for navigating to the host session details report.
- **TopN Sessions List for Destination** lists the destination host IP address, the number of sessions for the associated destination, and the maximum generated session rate by the destination host. The host IP address is a link for navigating to the host session details report.

Figure 6 TopN Sessions List

Top20 Sessions List for Source			Top20 Sessions List for Destination		
Source	Sessions	Average Rate (sessions/second)	Destination	Sessions	Average Rate (sessions/second)
172.10.0.60	8	0.03	224.0.0.6	17	0.08
172.10.0.71	8	0.03	224.0.0.5	10	0.08
172.200.0.2	4	0.03	255.255.255.255	3	0.02
0.0.0.0	3	0.02	1.1.1.1	2	0.02
1.1.1.60	2	0.02	169.254.255.255	2	0.02
169.254.142.30	2	0.02			
60.0.1.60	1	0.02			
60.5.0.3	1	0.02			
172.5.0.1	1	0.02			
172.10.0.1	1	0.02			
172.10.0.72	1	0.02			
172.10.0.73	1	0.02			
172.200.0.3	1	0.02			

Host Session Details Report

The host session details report includes the **Session Trend** line chart and the **Session Details** list. To view the report, click the source or destination host IP address link on the **TopN Sessions List** in the individual NTA server host sessions report or the device host sessions report. The time range of the data in the host session details report is the same as that of the individual NTA server host sessions report or the device host sessions report. For example, when the time range of the device host sessions report is last one hour, the time range of the host session details report is also last one hour.

Session Trend

The **Session Trend** line chart provides the total number of sessions for the selected host in one minute.

Figure 7 Session Trend



To return to the individual NTA server host sessions report or device host sessions report, click **Back** located in the upper right of this chart.

Session Details

The **Session Details** list displays host sessions for the selected time range. It lists the timestamp, the total number of sessions in 1 minute, and the average rate for selected host sessions generated per second.

Figure 8 Session Details

Session Details 		
Time	Sessions	Average Rate (sessions/second)
2015-11-23 11:41:00	66	1.10
2015-11-23 11:42:00	33	0.55
2015-11-23 11:43:00	44	0.73
2015-11-23 11:44:00	60	1.00
2015-11-23 11:45:00	55	0.92
2015-11-23 11:46:00	94	1.57
2015-11-23 11:47:00	71	1.18
2015-11-23 11:48:00	53	0.88

Interface monitoring

This chapter of the NTA administrator guide provides information on interface monitoring in NTA, including how NTA analyzes network flow records report on network traffic from an interface perspective. This chapter describes the reporting options for interface traffic analyses and reviews configuration issues around interface monitoring and traffic analysis tasks and the reports they generate. This chapter also explains the process for adding interface traffic analysis tasks, including instructions for adding, modifying, and deleting tasks from NTA. It provides a survey of the summary reports for all interface tasks and a look at the more granular reports for an individual interface traffic analysis task.

Interface traffic analysis overview

Interface traffic analysis tasks analyze network flow data by the interfaces you specify in interface traffic analysis tasks. NTA will parse all network flow data and provide various statistical views of traffic that was observed for the interfaces configured in an interface traffic analysis task. For example, NTA will provide source and destination host information reporting by interface, displaying the rate of traffic attributed to specific source or destination hosts that were observed sending or receiving traffic across the selected interface.

In general, the NTA interface traffic analysis tasks provide traffic statistics for the interfaces configured in every interface traffic analysis task. The interface traffic reports include rate of traffic for all interfaces in all tasks, for all interfaces in each task, and for individual interfaces in a task. Interface statistics include traffic rate by application, source host, destination host, and a session or source/destination host pair. These reports are organized into multiple layers from summarized information for all tasks to detailed reporting for specific interfaces configured for an individual interface traffic analysis task.

Interface traffic analysis reporting overview

After you create the first interface traffic analysis task, NTA creates an entry called **Interface Traffic Analysis Task**  under the area **Traffic Analysis and Audit** on the left navigation tree.

Click **Interface Traffic Analysis Task** on the left navigation tree to view the summary report for all interface traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to the **Interface Traffic Analysis Task**. The **Interface Traffic Analysis Task** shortcut menu displays all interface traffic analysis tasks created in NTA. Click the name of a task to view the interface traffic analysis report of the task.

To view the interface traffic analysis report of an interface in an interface traffic analysis task, click the **Expand** icon  next to the task on the shortcut menu to display the all interfaces in the task. Click the name of an interface to view the interface traffic analysis report of the interface.

The summary interface traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides summarized average rate per second reporting for all interfaces specified in all interface traffic analysis tasks summarized by task. Each bar in the graph is a link to more detailed reporting for the selected task. This includes traffic, application, source, destination, and session statistics:
 - **Traffic**—Reports found under the **Traffic** tab for interface reporting display the average inbound and outbound rate per second, TopN by ToS, and the individual data samples for all interfaces for the selected task or for an individual interface in a task.
 - **Application**—Reports found under the **Application** tab for interface reporting display percentage of application traffic generated by all interfaces in a task and average rate of application traffic for all interfaces in the selected task or for an individual interface in a task.

- **Source**—Reports found under the **Source** tab for interface reporting include inbound and outbound reports that display the percentage of traffic generated by the TopN source hosts and volume and percentage of traffic generated for each of the TopN source hosts for all interfaces in the selected task or for an individual interface in a task.
- **Destination**—Reports found under the **Destination** tab for interface reporting include inbound and outbound reports that display the percentage of traffic generated by the TopN destination hosts and volume and percentage of traffic generated for each of the TopN destination hosts for all interfaces in the selected task or for an individual interface in a task.
- **Session**—Reports found under the **Session** tab for interface reporting include inbound and outbound reports that display the percentage of traffic generated by the TopN source and destination host pairs and volume and percentage of traffic generated for each of the TopN source and destination host pairs for all interfaces in the selected task or for an individual interface in a task.
- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—This set of line charts provides per second average traffic rate summarized by interface traffic analysis task for inbound and outbound traffic for all interfaces for the selected task or for an individual interface in a task. A set of pie charts reveals the distribution of traffic for the TopN applications, with one chart each for inbound and outbound traffic.
- **Summary List (Last 1 Hour)**—This list provides per second traffic rate and percentage of traffic statistics summarized by interface traffic analysis task for inbound and outbound traffic for all interfaces in all tasks.

Interface traffic analysis configuration considerations

When adding interfaces to a task, you need to consider several things. The most important decision to make is which interfaces belong to each task—this determines how NTA groups interfaces for analysis, reporting, and navigation purposes. Viewing statistics in juxtaposition to each other provides another level of analysis and interpretation of data. Additional considerations follow:

- By default, NTA does not monitor any interfaces. You must create a task for every interface or group of interfaces on which you want to monitor and report.
- You define how NTA groups interfaces for analysis and reporting purposes. NTA presents interface traffic analysis tasks in The NTA left navigation system and provide summarized interface reporting based on the way you have organized interfaces into tasks.
- You can add one or more interfaces from one or more devices into a single task. You are not limited to adding interfaces from a single device into one task. However, an interface can only belong to one task.
- Consider how you want to analyze, access, and view interface data, and then structure your tasks around it. For example, if you want to view interface traffic statistics by geography, then group interfaces into tasks organized by location. Otherwise, group interfaces by function. For example, you can group all network ingress and egress interfaces into a single task. This enables you to compare the traffic statistics for interfaces that perform a similar function. Otherwise, group all interfaces associated with an application or a group of applications or a business service into a single task. Another option is to create a single task for every device, and add all the interfaces from that device whose statistics you want to view into the task. Also, you can create tasks organized by support team so that operators have simplified access to reporting for the devices and interfaces they manage.
- Add only those interfaces whose statistics you want to view. Do not add all the interfaces on a device unless you want to view reporting for all interfaces. Adding interfaces for which you do not want to view statistics only clutters NTA interface navigation. This makes it more difficult for you to find the interface for which you do want to view data.
- When you add interfaces to a task, NTA presents a list of all interfaces that NTA knows about. This list is generated from the devices that have been added to NTA using the Device Management feature. If the interfaces you want to add are not displayed on this list and if they are not already included in another interface traffic analysis task, it is most likely because the

device has not been added to NTA or it has not been selected in the NTA server configuration found under Server Management. For more information about selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

- If you do not add an interface to a task, NTA does not report on it.
- You can add an interface to only one task. Careful planning of tasks and documenting them will be a valuable aid to you when you begin creating tasks and to help identify to which task an application has been added.
- You must enable network flow data on the devices and for the interfaces you want to monitor and report on using NTA.

Managing interface traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA does not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need. This section describes the process for adding, modifying, or removing interface traffic analysis tasks in NTA.

Viewing a traffic analysis task

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view the NTA traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

Task list contents

- **Task Name**—Name of the task. This field is a link to the **Traffic Analysis Task Details** page for the task.
 - **Task Description**—Description for the task.
 - **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **Baseline Analysis**—This parameter is displayed when the Baseline Analysis feature is enabled in NTA parameters. This feature provides an additional layer of analysis to reports provided by NTA by including baseline trend data when data has been collected for a minimum of one week.
 - **Modify**—Contains an icon  for modifying the associated task.
 - **Delete**—Contains an icon  for deleting the associated task.
3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** in the upper left corner of the **Traffic Analysis Task List**.

You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. The column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing interface traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the contents in the **Task Name** field of the **Traffic Analysis Task List** whose **Task Type** is **Interface** to view the details for an individual task.

Traffic analysis task details

- **Task Name**—Contains the name of the task.
- **Task Description**—Contains the description for the associated task.
- **Server**—Contains the name or IP address of the NTA server.
- **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
- **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by the associated traffic analysis task.
- **VLAN/VXLAN Analysis**—Indicates whether VLAN/VXLAN traffic analysis is enabled.
- **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
- **Enable Automatic Anomaly Detection Based On The Baseline**—Indicates whether automatic detection of traffic anomaly based on the baseline is enabled for the task. This parameter is displayed only when baseline analysis is enabled.
- **Threshold Alarm**—Indicates whether the Threshold Alarm feature is enabled for the task.
- **Baseline Threshold Setting**—Displays parameters of the baseline threshold setting. This area is displayed only when baseline analysis is enabled. The **Baseline Threshold Setting** area includes the following parameters:
 - **Baseline Upper/Lower Threshold**—Indicates the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Indicates under what condition the threshold is triggered. This condition has two configuration parameters, the time interval, and the number of times that the threshold must be met.
 - **In Threshold**—Indicates the percentage threshold for inbound traffic that must be met before NTA generates an alarm.

- **Out Threshold**—Indicates the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
 - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
 - **Threshold Alarm Settings**—Displays parameters of the threshold alarm setting. This area is displayed only when baseline analysis is enabled. If you enabled the Threshold Alarm feature, the page shows the **Threshold Alarm Settings** configuration parameters. The parameters include:
 - **Direction**—Indicates which direction you want to apply the threshold, **In**, **Out** or **In/Out**.
 - **Trigger**—Indicates under what conditions the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - **In Threshold**—Specifies the threshold value or amount of inbound traffic that must be exceeded before NTA generates an alarm. This field is displayed only when the **Direction** field is set to **In** or **In/Out**.
 - **Out Threshold**—Specifies the threshold value or amount of outbound traffic that must be exceeded before NTA generates an alarm. This field is displayed only when the **Direction** field is set to **Out** or **In/Out**.
 - **Severity**—Specifies the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specifies the time interval in which a triggered alarm is not sent again.
 - **Interface Information**—This table contains a list of interfaces, their aliases, IP addresses, maximum transmission rate, device name, and device IP address for all interfaces providing traffic for this traffic analysis task.
4. Click **Back** to return to the **Traffic Analysis Task List**.

Adding an interface traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.
The **Add Traffic Analysis Task** page opens.
4. Next to **Interface** on the **Select Task Type** area, click the option to add an interface traffic analysis task.
5. Click **Next**.
The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.
The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. In the **Task Description** field, enter a description for this task.
8. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.

9. To select the operator groups that have access to the analysis and reports provided by this interface task, click **Select** next to the **Reader** field.
The **Choose Operator Group** dialog box opens.
 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box located in the upper left corner of the column label field for all boxes.
 - b. Click **OK** to accept your operator group selection. The operator groups you selected are displayed in the **Reader** field.
10. Select **Enable** from the VLAN/VXLAN analysis list as needed. After enabling this feature, you can view the VLAN or VXLAN traffic details for the interface in the interface traffic analysis report.
11. From the **Baseline Analysis** list, select **Enable** to enable baseline analysis for the reports generated by this task. If you select **Disable** to disable baseline analysis, go to step 14.
If you selected **Enable** from this list, the baseline trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.
If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature has not been enabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
12. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.
NTA automatically detects and generates alarms for traffic anomaly according to the baseline.
13. Specify whether to enable the Threshold Alarm feature.
 - From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure, and select **Disable** if you do not want to generate alarms.
 - If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.
14. Configure the baseline threshold settings.
 - **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
 - **In Threshold**—Indicates the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
 - **Out Threshold**—Indicates the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.

- **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
15. Configure the threshold alarm settings.
- **Direction**—Define to which traffic you want to apply the threshold.
 - Select **In** if you want to apply the threshold to inbound traffic only.
 - Select **Out** if you want to apply the threshold to outbound traffic only.
 - Select **In/Out** if you want to apply the threshold to both inbound and outbound traffic. The default setting is **In/Out**.
 - **Trigger**—Define under what conditions the threshold is triggered. This option has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
 - **In Threshold**—Enter the threshold value or amount of inbound traffic that must be exceeded before NTA generates an alarm in the **In Threshold** field. Select % from the list located next to the **In Threshold** field, if you want NTA to calculate the inbound traffic as a percent of total available inbound bandwidth. Otherwise, select the rate of traffic for the selected interfaces from the list. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
 - **Out Threshold**—Enter the threshold value or amount of outbound traffic that must be exceeded before NTA generates an alarm in the **Out Threshold** field. Select % from the list next to the **Out Threshold** field, if you want NTA to calculate the outbound traffic as a percent of total available outbound bandwidth. Otherwise, select the rate of traffic for the selected interfaces from the list. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
16. To select one or more interfaces that will provide network flow data, click **Select** above the **Interface Information** list.

You must add at least one interface to an interface traffic analysis task. For considerations about organizing interfaces into tasks, see "[Interface traffic analysis configuration considerations](#)."

The **Add Interface** page is displayed.

Obtain interfaces automatically or configure them manually.

To obtain interfaces automatically:

- a. At the top of the **Add Interface** page, click the **Obtain Automatically** tab.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.
- c. Click **OK** to accept your interface selection.

When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.

To configure interfaces manually:

- a. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.

The page will update to display the configuration options for manually adding an interface to a traffic analysis task.

- b. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.
- c. In the **Interface Alias** field, enter the alias for the interface.

Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.

- d. From the **Device** list, select the device to which the interface belongs.

For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.

For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- e. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.

You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.

- f. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.
- g. Under the **View Management** area on the left navigation tree, click **Device View**.

The **Device List – All** is displayed. This list displays all devices in INC.

- h. Locate the device for which you want to view interface details.
- i. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.

The **Device Details** page opens.

- j. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.

The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.

- k. In the **Max. Speed** field, enter the maximum speed of the interface.
- l. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.

 IMPORTANT:

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

m. Click **OK**.

17. Click **OK** to create the interface traffic analysis task.

After you create an interface traffic analysis task, NTA creates an entry called  **Interface Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for all interface traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **Interface Traffic Analysis Task**. The **Interface Traffic Analysis Task** shortcut menu displays all interface traffic analysis tasks created in NTA. Click the name of a task to view the interface traffic analysis report of the task.

Click the **Expand** icon  next to a task on the shortcut menu to display all interfaces in the task. Click the name of an interface to view the interface traffic analysis report of the interface.

For information about accessing and viewing interface traffic analysis reports, see "[Viewing interface traffic analysis reports](#)."

 IMPORTANT:

You must also configure NetStream, NetFlow, or sFlow traffic from the configured interfaces to the NTA server. For instructions, see the device configuration guides.

Modifying an interface traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  associated with the interface traffic analysis task you want to modify.
The **Modify Traffic Analysis Task** page opens.
4. Modify the name for this task in the **Task Name** field.
The task name must be unique.
5. Modify the description for this task in the **Task Description** field.
6. Select the NTA NetStream, NetFlow, or sFlow collection server from the **Server** list.
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add new operator groups that have access to the analysis and reports provided by this interface task, click **Select** next to the **Reader** field.
The **Operator Group List** dialog box opens.
 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
 - b. Click **OK** to accept the new additions to operator group.
The operator groups you selected are displayed in the **Reader** field.
 - c. To revoke operator group access to the results of this interface traffic analysis task, highlight the groups in the **Reader** field you want to remove.

- d. Click **Delete**.
- e. Click **OK** to confirm the deletion of the selected operator groups from the task.
The **Reader** list is updated to reflect the deleted operator group changes.
8. Select **Enable** from the VLAN/VXLAN analysis list as needed. After enabling this feature, you can view the VLAN or VXLAN traffic details for the interface in the interface traffic analysis report.
9. From the **Baseline Analysis** list, select **Enable** to enable baseline analysis for the reports generated by this task. If you select **Disable**, go to step 11.
If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.
If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature has not been enabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
10. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.
NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.
11. Specify whether to enable the Threshold Alarm feature.
 - From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure.
 - From the **Threshold Alarm** list, select **Disable** if you do not want to generate alarms.
 If you selected **Enable** from the **Threshold Alarm** list, the page will update to display the **Threshold Alarm Settings** configuration parameters.
12. Configure the baseline threshold settings.
 - **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
 - **In Threshold**—Indicates the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
 - **Out Threshold**—Indicates the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
13. Configure the threshold alarm settings.

- **Direction**—Define to which traffic you want to apply the threshold.
 - Select **In** if you want to apply the threshold to inbound traffic only.
 - Select **Out** if you want to apply the threshold to outbound traffic only.
 - Select **In/Out** if you want to apply the threshold to both inbound and outbound traffic. The default setting is **In/Out**.
 - **Trigger**—Define under what conditions the threshold is triggered. This option has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
 - **In Threshold**—Enter the threshold value or amount of inbound traffic that must be exceeded before NTA generates an alarm in the **In Threshold** field. Select % from the list next to the **In Threshold** field, if you want NTA to calculate the inbound traffic as a percent of total available inbound bandwidth. Otherwise, select the rate of traffic for the selected interfaces from the list. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
 - **Out Threshold**—Enter the threshold value or amount of outbound traffic that must be exceeded before NTA generates an alarm in the **Out Threshold** field. Select % from the list next to the **Out Threshold** field, if you want NTA to calculate the outbound traffic as a percent of total available outbound bandwidth. Otherwise, select the rate of traffic for the selected interfaces from the list. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
14. Above the **Interface Information** list, click **Select** to add one or more interfaces that provide network flow data.
- You must have at least one interface configured for an interface traffic analysis task. The **Add Interface** page opens.
- To add interfaces, you can obtain them automatically or configure them manually.
- a. To add interfaces automatically to the task, click the **Obtain Automatically** tab at the top of the **Add Interface** page.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.
 - b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.

- c. Click **OK** to accept your interface selection.

When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.

- d. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.

The page will update to display the configuration options for manually adding an interface to a traffic analysis task.

- e. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.

- f. In the **Interface Alias** field, enter the alias for the interface.

Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.

- g. From the **Device** list, select the device to which the interface belongs.

For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.

For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- h. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.

You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.

- i. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.

- j. Under the **View Management** area on the left navigation tree, click **Device View**.

The **Device List – All** is displayed. This list displays all devices in INC.

- k. Locate the device for which you want to view interface details.

- l. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.

The **Device Details** page opens.

- m. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.

The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.

- n. In the **Max. Speed** field, enter the maximum speed of the interface.

- o. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.

 IMPORTANT:

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

- p. Click **OK** to add the interface manually.

15. To remove an interface from an interface traffic analysis task, click the **Delete** icon  associated with the interface you want to remove.
16. Click **OK** to accept your modifications the interface traffic analysis task.

Deleting an interface traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  associated with the interface traffic analysis task you want to delete.
4. Click **OK** to confirm the deletion of the selected interface traffic analysis task.
The **Traffic Analysis Task List** reflects the removal of the deleted task.

Adding an interface traffic analysis task by using the detection function

NTA can perform traffic detection on device interfaces. After you add a traffic analysis task, NTA automatically detects interfaces with traffic but without any traffic analysis task. You can view these interfaces and create new traffic analysis tasks for them or add them to the existing traffic analysis tasks.

Viewing the detected interfaces

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. Move your mouse pointer to the shortcut menu icon  next to  **Interface Traffic Analysis Task** under the **Traffic Analysis and Audit** area.

The **Interface Traffic Analysis Task** shortcut menu is displayed.

3. Click **Unconfigured Interfaces in IP address**, where the *IP address* argument represents the NTA server IP address.

The **Interface Information** list displays all interfaces that have traffic but have no traffic analysis task.

Interface Information list contents

- **Device Name**—Name of the device where the interface resides.
- **Device IP**—IP address of the device where the interface resides.
- **Interface Alias**—Alias of the interface.
- **Interface Description**—Description of the interface.
- **Interface Index**—Index of the interface.
- **In Traffic (latest 1 hour)**—Inbound traffic on the interface in the latest one hour.
- **Out Traffic (latest 1 hour)**—Outbound traffic on the interface in the latest one hour.

Adding a new traffic analysis task for interfaces

1. Select the boxes next to the interfaces on the **Interface Information** list.
2. Click **Create New Task**.
The **Add Traffic Analysis Task** page opens. The interface list displays the interfaces you selected in step 1.

3. Configure parameters for the traffic analysis task.
For more information about the configuration, see "[Adding an interface traffic analysis task](#)."

Adding interfaces to an existing traffic analysis task

1. Select the boxes next to the interfaces on the **Interface Information** list.
2. Click **Add to Existing Task**.
The **Add Traffic Analysis Task** page opens. The interface list displays the interfaces you selected in step 1.
3. Select the option next to the target interface traffic analysis task.
4. Click **OK**.

Viewing interface traffic analysis reports

NTA provides various levels of reporting for all traffic analysis tasks. The highest level provides summarized reporting for all tasks of the same type whether the task type is interface, VLAN/VXLAN, probe, application, host, VPN, interbusiness or BGP AS. These reports are accessed by clicking the highest level entry of the left navigation tree under the **Traffic Analysis and Audit** area. To view summarized reporting for all interface tasks, click the  **Interface Traffic Analysis Task** entry of the left navigation tree.

NTA also provides more detailed reporting for individual tasks, including reports for every interface configured in an interface traffic analysis task. NTA groups individual tasks by type. All interface tasks branch can be found on the **Interface Traffic Analysis Task** menu.

To view the **Interface Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to  **Interface Traffic Analysis Task**. The shortcut menu displays all interface traffic analysis tasks created in NTA. Click the name of a task to view the interface traffic analysis report of the task. Click the **Expand** icon  next to a task on the shortcut menu to display all interfaces in the task. Click the name of an interface to view the interface traffic analysis report of the interface.

This section describes the reporting options available for interface traffic analysis tasks. It also describes the process for navigating to interface traffic analysis tasks, the summary reports available for interface tasks, and the reports and features available for an interface traffic analysis task.

Navigating to the interface traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Under the **Traffic Analysis and Audit** area of the left navigation tree, click the  **Interface Traffic Analysis Task** entry to view summary reporting for all interface tasks.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to  **Interface Traffic Analysis Task**.
The **Interface Traffic Analysis Task** shortcut menu displays all interface traffic analysis tasks created in NTA. Click the name of a task to view the interface traffic analysis report of the task.
4. To view the interface traffic analysis report of an interface in an interface traffic analysis task, click the **Expand** icon  next to the task on the shortcut menu to display the all interfaces in the task. Click the name of an interface to view the interface traffic analysis report of the interface.

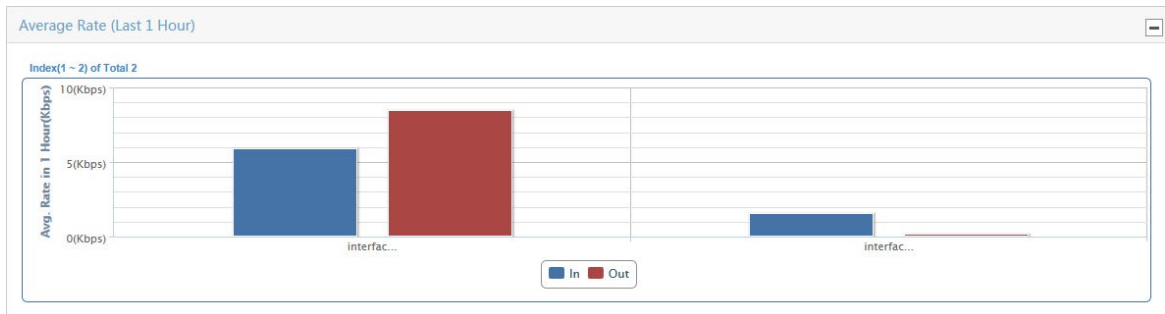
Summary reports for all interface tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **Interface Traffic Analysis Task** entry of the left navigation tree under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

Average Rate (Last 1 Hour)

The **Average Rate (Last 1 Hour)** bar graph summarizes the average rate of traffic for all interfaces in every interface traffic analysis task, grouped by task for the last hour. You can access this graph by clicking the  **Interface Traffic Analysis Task** entry of the left navigation tree. The bars in the graph link to the detailed reports for the selected task.

Figure 9 Average Rate (Last 1 Hour)



Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

The report of the traffic trend and topN application for selected task includes four subreports. **Traffic Trend – In**, **Traffic Trend – Out**, **TopN Application – In**, and **TopN Applications – Out**.

Figure 10 Traffic Trend and TopN Application for Selected Task



The **Traffic Trend – In** line chart provides the summarized average rate of inbound traffic for all interfaces in the selected interface traffic analysis task for the last hour.

The **Traffic Trend – Out** line chart provides the summarized average rate of outbound traffic for all interfaces in the selected interface traffic analysis task for the last hour.

The **TopN Application – In** pie chart displays the distribution of inbound traffic for the TopN applications for all Interfaces in the selected traffic analysis task for the last hour.

The **TopN Applications – Out** pie chart displays the distribution of outbound traffic for the TopN applications for all interfaces in the selected traffic analysis task for the last hour.

No data is graphed on these charts until you specify a task.

1. To select the task, click the **Select Task** link in the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar.
The **Choose NTA Task** dialog box opens.
2. Select the check box next to the interface task for which you want to view this report.
3. Click **OK**.
The page displays the **Traffic Trend – In**, **Traffic Trend – Out**, **TopN Application – In**, and **TopN Application – Out** reports for the selected task.

Summary List (Last 1 Hour)

The **Summary List** provides inbound and outbound traffic rates and percentage of traffic statistics summarized by interface task for the last hour.

1. Click the  **Interface Traffic Analysis Task** entry from the left navigation tree.
Summary list contents
 - **Task Name**—Contains the name of the interface traffic analysis task. The contents of this field link to reports for the associated task.
 - **In Rate**—Provides the inbound traffic rate for all interfaces configured for the associated task.
 - **Avg. Link Utilization**—Provides the percent of average link utilization for inbound traffic by all interfaces in the associated task.
 - **Out Rate**—Provides the outbound traffic rate for all interfaces configured for the associated task.
 - **Avg. Link Utilization**—Provides the percent of average link utilization for outbound traffic by all interfaces in the associated task.
 - **Traffic Log Audit**—Contains the  **Traffic Log Audit** icon of the interface traffic analysis task. The icon of this field is a link to the **Traffic Log Audit** result page.
2. The **Add** button at the top of the **Summary List** provides a shortcut to the **Add Interface Traffic Analysis Task** page. For more information about adding interface traffic analysis tasks, see "[Adding an interface traffic analysis task.](#)"
3. Click **Refresh** to update the reports with the most recent data.
4. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.

- g. Click **Export**.

Detailed reports for an interface traffic analysis task

NTA provides a suite of reports for viewing interface data from different perspectives. Reports for interfaces are organized into the following reporting groups:

- **Traffic report**—Provides overall traffic statistics, including ToS/MPLS Exp flux statistics for all interfaces in a task for the selected time range.
- **Application report**—Provides rate of traffic statistics by application that enable you to get detailed reports for an individual application.
- **Source report**—Provides rate and percentage distribution of traffic by source host for all interfaces in a task for the selected time range.
- **Destination report**—Provides rate and percentage distribution of traffic by destination host for all interfaces in a task for the selected time range.
- **Session report**—Provides rate and percentage distribution of traffic for source and destination pairs for all interfaces in a task for the selected time range.

Source, destination, and session reports enable you to get detailed traffic reports for an individual host and session.

Traffic reports

Traffic reports for interface tasks provide overall traffic statistics for all interfaces configured in an interface traffic analysis task or for an individual interface in a task.

Traffic reports for an interface traffic analysis task have the **Traffic Trend** line chart that provides average inbound and outbound traffic rates for all interfaces in the selected traffic analysis task. This chart provides average link utilization, maximum link utilization, average rate, minimum average rate, maximum average rate, and total traffic volume statistics in a tabular format. The statistics are for both inbound traffic and outbound traffic of the associated task.

Traffic reports for an interface task have a tabular view of total traffic volume and percentage of total traffic volume grouped by ToS/MPLS Exp for both inbound and outbound traffic in the **TopN Traffic List for ToS/MPLS Exp** table.

Traffic reports for an interface task use a **TopN VLAN/VXLAN Traffic List** to display inbound and outbound traffic volumes and percentages for the TopN VLAN/VXLAN traffic.

Traffic reports for an interface task have the **Flux Distribute In Interface** stacked bar chart that graphs the average rate of both inbound and outbound traffic for every interface configured in the task.

Traffic reports for an interface task have the **Interface Flux Trend** line chart that provides average inbound and outbound traffic rates for selected interfaces configured in the selected traffic analysis task.

The reports have the **Traffic Details** list that provides the data collection samples that include timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic. NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an interface task, click the **Traffic** tab to view traffic reports for the selected interface traffic analysis task.

Query traffic

NTA enables you to change the filter criteria for interface reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed.

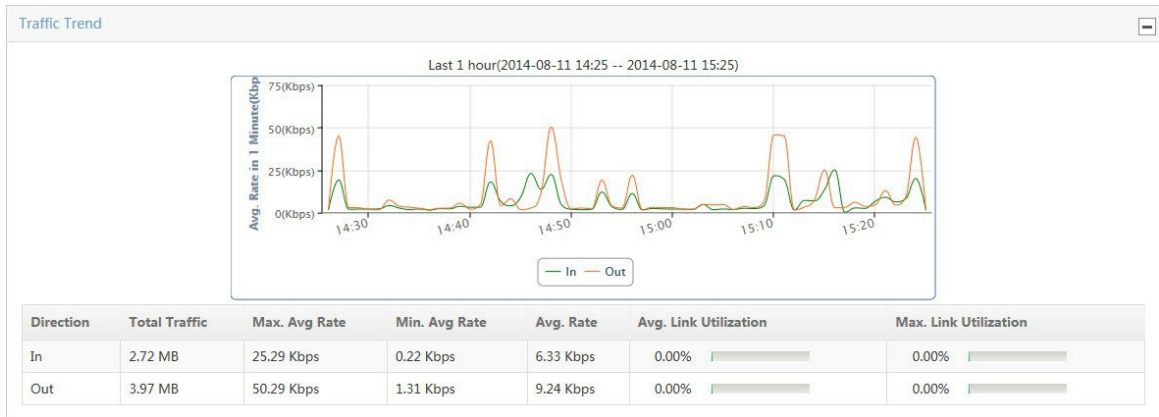
1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7**

- days, Last 30 days, Last 3 months, or Custom.** Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
 3. Specify the following query criteria:
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
 4. Click **OK**.
The page displays the results of your query.
 5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.
 - g. Click **Export**.

Traffic Trend – Average

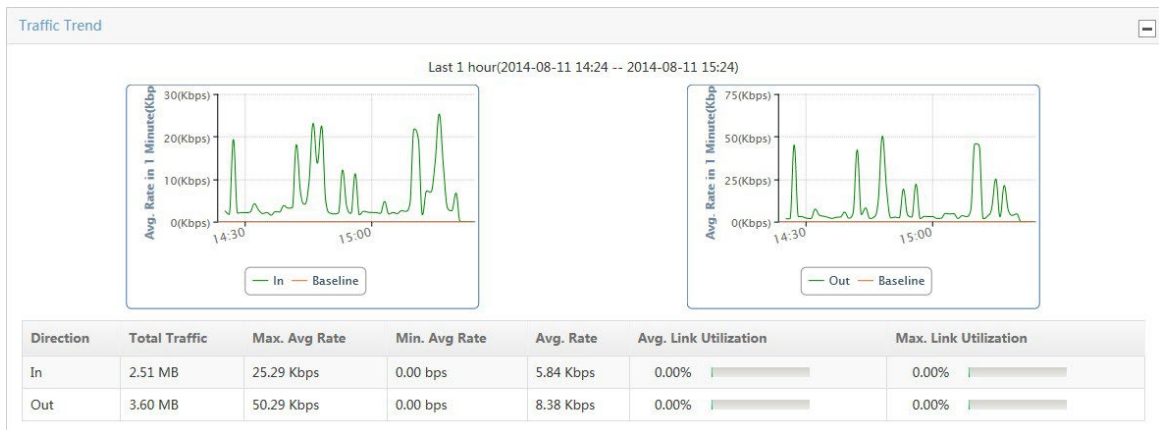
The **Traffic Trend** combination line chart provides average inbound and outbound traffic rates for all interfaces in the selected traffic analysis task or for a specific interface in an interface task. This chart also provides total traffic volume statistics, maximum average, minimum average, average, and link use in a tabular format for both inbound and outbound traffic for the associated task or interface for the selected time range. If more than one interface exists for the selected task, these statistics reflects traffic for all interfaces configured in a task.

Figure 11 Traffic Trend



If the selected traffic analysis task enabled the Baseline Analysis feature, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. The green line indicates the average incoming or outgoing traffic rate, and the orange line indicates the baseline. For more information about configuring the Baseline Analysis feature for the interface traffic analysis task, see ["Adding an interface traffic analysis task."](#)

Figure 12 Traffic Trend with Baseline



To view these charts for a specific interface, click the bar in the **Flux Distribute In Interface** graph for the interface whose report you want to view. For more information on the Flux Distribute In Interface report, see ["Flux Distribute in Interface."](#)

By default, the **Traffic Trend** chart displays statistics for the previous hour.

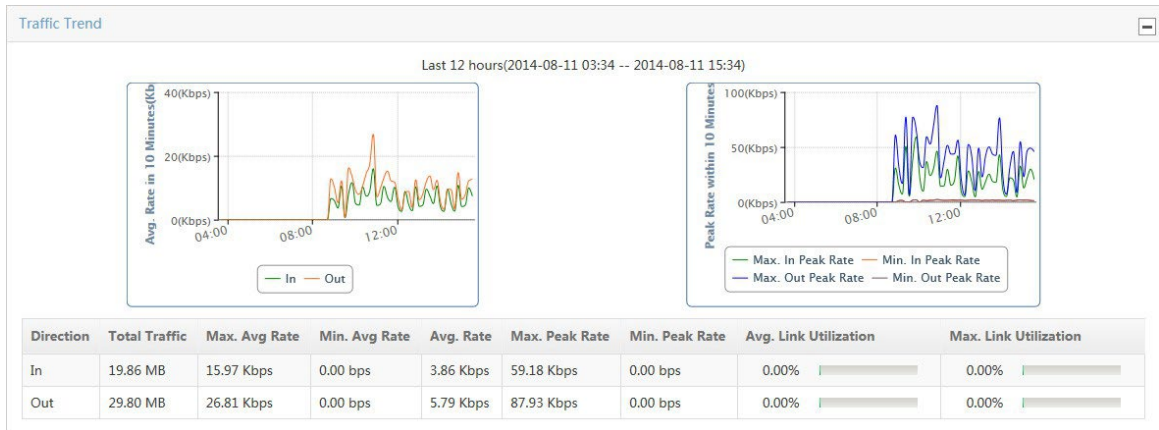
- To view data for an earlier period, click **Previous** in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** in the upper right corner of the **Traffic Trend** chart.

Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range for both inbound and outbound traffic. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

Figure 13 Peak Rate



If the Baseline Analysis feature is enabled for the selected traffic analysis task, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. NTA displays the **Max./Min. In Peak Rate** chart and **Max./Min. Out Peak Rate** chart under the **Traffic Trend** chart. For more information about configuring the Baseline Analysis feature for the interface traffic analysis task, see "[Adding an interface traffic analysis task.](#)"

Figure 14 Peak Rate with Baseline



To view these charts for an individual interface, click the bar in the **Flux Distribute In Interface** graph for the interface whose report you want to view. For more information on the Flux Distribute In Interface report, see "[Flux Distribute in Interface.](#)"

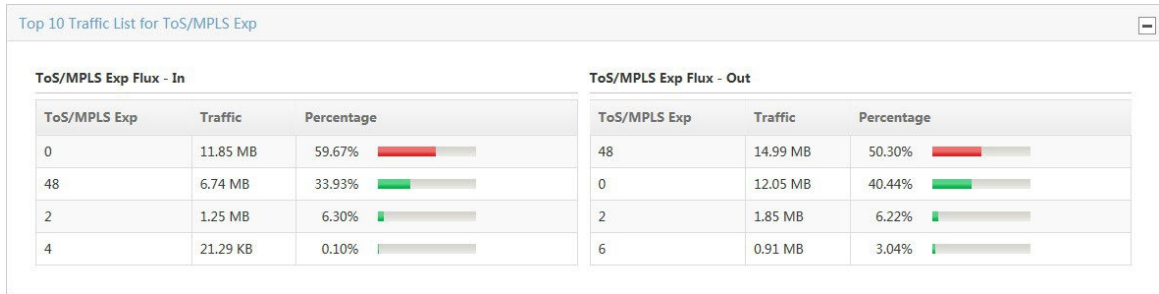
By default, the **Traffic Trend** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** in the upper right corner of the **Traffic Trend** chart.

TopN Traffic List for ToS/MPLS Exp

The **TopN Traffic List for ToS/MPLS Exp** provides administrators with a tabular view of total traffic volume and percentage of total traffic volume grouped by ToS or MPLS Exp for both inbound and outbound traffic for the selected time range for an interface traffic analysis task or for a selected interface in a task.

Figure 15 TopN Traffic List for ToS/MPLS Exp



To view this chart for an individual interface, click the bar in the **Flux Distribute In Interface** graph for the interface for which you want to view this report. For more information about the Flux Distribute In Interface report, see ["Flux Distribute in Interface."](#)

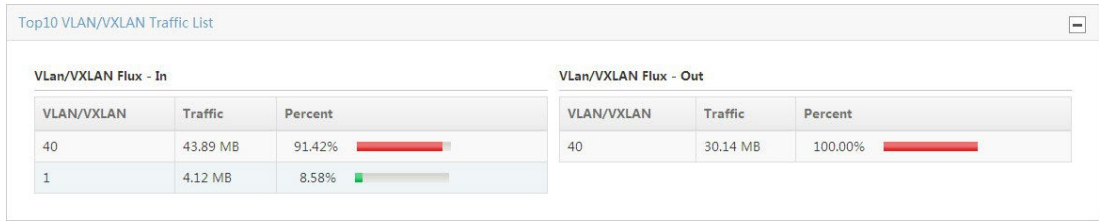
TopN VLAN/VXLAN Traffic List

The **TopN VLAN/VXLAN Traffic List** provides the **VLAN/VXLAN Traffic-Incoming** and **VLAN/VXLAN Traffic-Outgoing** charts.

The **VLAN/VXLAN Traffic-Incoming** chart displays the TopN VLAN/VXLAN traffic received on all interfaces in the traffic analysis task. The chart displays the **VLAN/VXLAN ID**, **Traffic**, and **Percent**.

The **VLAN/VXLAN Traffic-Outgoing** chart displays the TopN VLAN/VXLAN traffic sent out all interfaces in the traffic analysis task. The chart displays the **VLAN/VXLAN ID**, **Traffic**, and **Percent**.

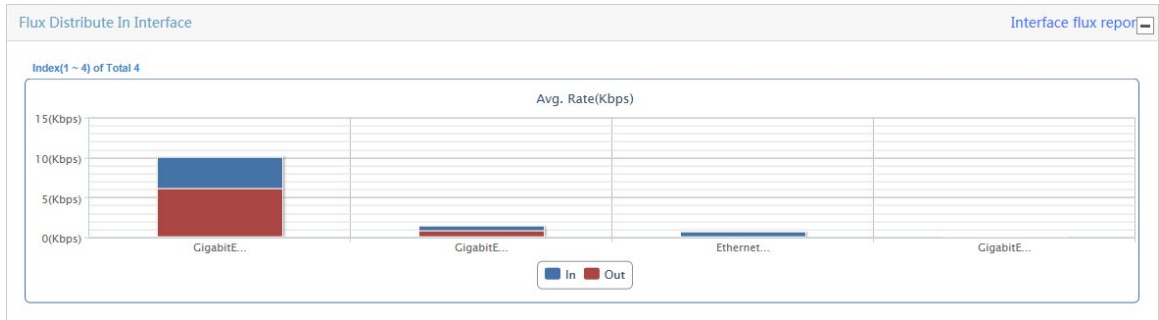
Figure 16 TopN VLAN/VXLAN Traffic List



Flux Distribute in Interface

If the task you selected has multiple interfaces configured for it, the **Flux Distribute In Interface** stacked bar chart displays the average rate of both inbound and outbound traffic for every interface configured in the task for the selected time range. The bars in the graph link to the reports for the selected interface.

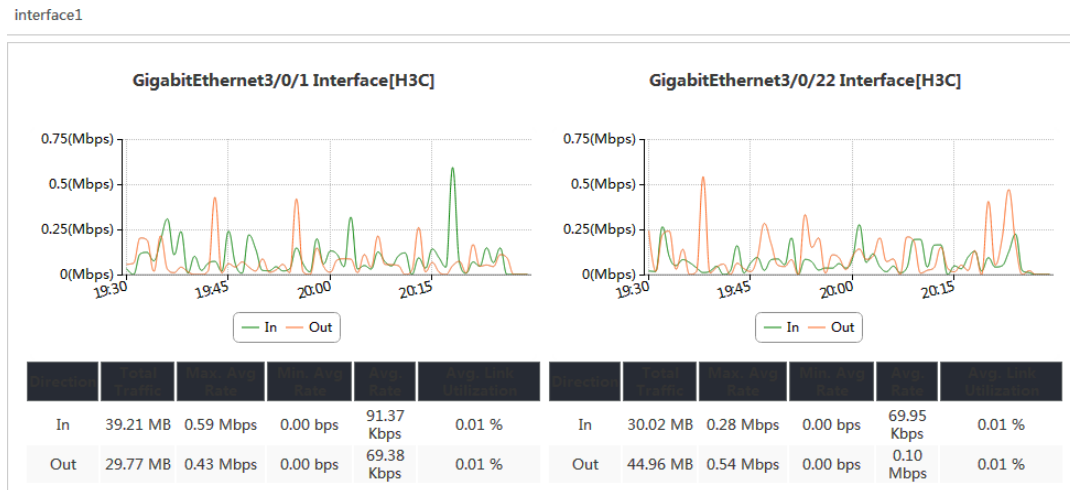
Figure 17 Flux Distribute in Interface



This chart is displayed only when the selected task has more than one interface selected.

To view the interface flux report for each interface for the selected time range, click **Interface flux report** at the upper right corner of the **Flux Distribute In Interface** window. The line chart for each interface displays the inbound and outbound traffic. The line chart for each interface also provides total traffic, maximum average rate, minimum average rate, average rate, and link utilization in a tabular format.

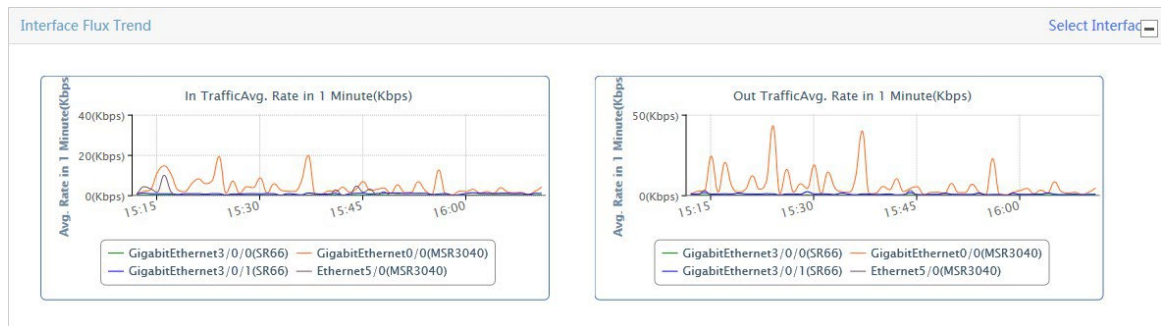
Figure 18 Interface Flux



Interface Flux Trend

The **Interface Flux Trend** line graph provides the average traffic trend for the selected interfaces.

Figure 19 Interface Flux Trend



No data will be graphed on these line charts until you specify one or more interfaces.

1. To select the interface, click the **Select Interface** link in the upper right corner of the **Interface Flux Trend** title bar.

The **Choose Interface** dialog box is displayed.

2. Select the check boxes next to the interfaces for which you want to view this report.
3. Click **OK**.

The page displays the **Interface Flux Trend** reports for the selected interfaces.

Traffic Details

The **Traffic Details** list provides the data collection samples for traffic statistics based on the report time range for the selected interface traffic analysis task or for a selected interface in a task. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic. Click **Show Flux** or **Hide Flux** to show or hide the **Traffic** columns in the **Traffic Details** list.

Figure 20 Traffic Details

Traffic Details					
Hide Flux					
Traffic - In			Traffic - Out		
Time	Traffic	Rate	Time	Traffic	Rate
2016-11-01 10:03:00	1.62 MB	0.23 Mbps	2016-11-01 10:03:00	4.45 MB	0.62 Mbps
2016-11-01 10:04:00	1.64 MB	0.23 Mbps	2016-11-01 10:04:00	10.95 MB	1.53 Mbps
2016-11-01 10:05:00	4.13 MB	0.58 Mbps	2016-11-01 10:05:00	23.79 MB	3.33 Mbps
2016-11-01 10:06:00	0.17 MB	23.20 Kbps	2016-11-01 10:06:00	0.34 MB	48.00 Kbps
2016-11-01 10:07:00	87.89 KB	12.00 Kbps	2016-11-01 10:07:00	1.44 MB	0.20 Mbps
2016-11-01 10:08:00	0.80 MB	0.11 Mbps	2016-11-01 10:08:00	3.11 MB	0.44 Mbps
2016-11-01 10:09:00	2.32 MB	0.32 Mbps	2016-11-01 10:09:00	2.26 MB	0.32 Mbps
2016-11-01 10:10:00	5.04 MB	0.70 Mbps	2016-11-01 10:10:00	15.11 MB	2.11 Mbps
2016-11-01 10:11:00	0.80 MB	0.11 Mbps	2016-11-01 10:11:00	1.60 MB	0.22 Mbps

To view this chart for an individual interface, click the bar in the **Flux Distribute In Interface** graph for the interface for which you want to view this report.

For more information on the **Flux Distribute In Interface** report, see "[Flux Distribute in Interface](#)."

Application Reports

Application reports provide traffic statistics by application, by protocol, and by application category for all interfaces in a task or for an individual interface in a task, with information to the details for an individual application, protocol, or application category.

Application reports for an interface traffic analysis task have the **Application List**, which provides a list of applications observed for all interfaces in the selected interface traffic analysis task or for a selected interface in a task. This list includes total volume of traffic for the associated application, rate of traffic observed on all interfaces generated by the associated application. This report also provides capabilities for in-depth additional reports for the selected application.

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all interfaces in the selected traffic analysis task or for an individual interface in a task.

Protocol reports for an interface traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all interfaces in the selected interface traffic analysis task or for a selected interface in a task. This list includes total volume of traffic for the associated protocol, rate of traffic, and the percentage of all observed traffic observed on all interfaces generated by the associated protocol. This report also provides capabilities for additional in-depth reports for the selected protocol.

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocols observed for all interfaces in the selected traffic analysis task or for a selected interface in a task. Protocol reports also have traffic lists and trend reports for individual protocols.

Application category reports for an interface traffic analysis task have the **Application Category List**, which provides a list of the application categories observed for all interfaces in the selected interface traffic analysis task or for a selected interface in a task. This list includes total volume of traffic for the associated application categories, rate of traffic observed on all interfaces generated by the associated application category. This report also provides capabilities for in-depth additional reports for the selected application category.

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all interfaces in the selected traffic analysis task or for an interface in a selected task. Application category reports also have traffic lists and trend reports for the individual application categories.

As with all the report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for an interface task, click the **Application** tab to

view application reports for the selected interface traffic analysis task, and set the **Query Type** to **Application** as described in "Query applications."

Application reports display reports organized by the list of applications in NTA. NTA provides many system-defined applications and NTA also supports user defined applications. For more information about applications in NTA, see "Managing applications." This section describes the reports available for applications.

Query applications

To view reports by application, you must configure the filter criteria for application reports. The application query option enables you to change the default settings for query type, application, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application** from the **Query Type** list.
The page displays the report for Layer 4 through Layer 7 applications.
3. Specify the following query criterion:
 - o **Application**—To select the application you want to search for, click **Select** next to the **Application** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select the applications you want to search for, you must first query the **Application List** as follows:

- a. Specify one or more of the following criteria in the **Query Applications** area:
 - **Application**—Enter a partial or complete name for the applications you want to search for in the **Application** field.
 - **Pre-defined**—From the **Pre-defined** list, select **Yes** to search for applications that are predefined. To filter for applications that are user-defined, select **No** from the list. To include system, predefined, and user-defined applications, select **Not limited**.
- b. To display the full **Application List**, click **Query** without entering any search criteria.
- c. Click **Query**.
The query results are displayed in the **Application List** below the **Query Applications** area.
- d. Select the check boxes next to the applications for which you want to search.
- e. Click **OK** to add the applications to the filter.

The applications you selected are displayed in the **Application** field.

Click **Clear** next to the **Application** field to clear all selected applications.

- **Start Time**—Enter the start time of the time range, in format of YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.

4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.
 - g. Click **Export**.

Application List

The **Application List** provides a list of the applications observed for all interfaces in the selected interface traffic analysis task or for a single interface in a task for the selected time range. This list includes the application name, a link for viewing the ports for all unknown applications, total volume of traffic for the associated application, rate of traffic, and the percentage of traffic on all interfaces generated by the associated application. The application name in the **Application** field is a link to reports for the selected application.

Figure 21 Application List

Application List					
Application ↕	Unknown Applications	In Traffic ▼	In Speed ↕	Out Traffic ↕	Out Speed ↕
snmp		0.44 MB	1.03 Kbps	0.56 MB	1.29 Kbps
Telnet		0.31 MB	0.72 Kbps	0.71 MB	1.65 Kbps
UDP Protocol Unknown Application		0.21 MB	0.49 Kbps	81.99 KB	0.19 Kbps
bgp		41.83 KB	95.18 bps	49.22 KB	0.11 Kbps
TCP Protocol Unknown Application		28.80 KB	65.55 bps	59.54 KB	0.14 Kbps
bootps		20.82 KB	47.38 bps	0.00 B	0.00 bps
echo		17.23 KB	39.20 bps	28.09 KB	63.91 bps
netbios-ns		1.60 KB	3.64 bps	0.00 B	0.00 bps

1-8 of 13. Page 1 of 2.

< << 1 2 >> > 8 ▼

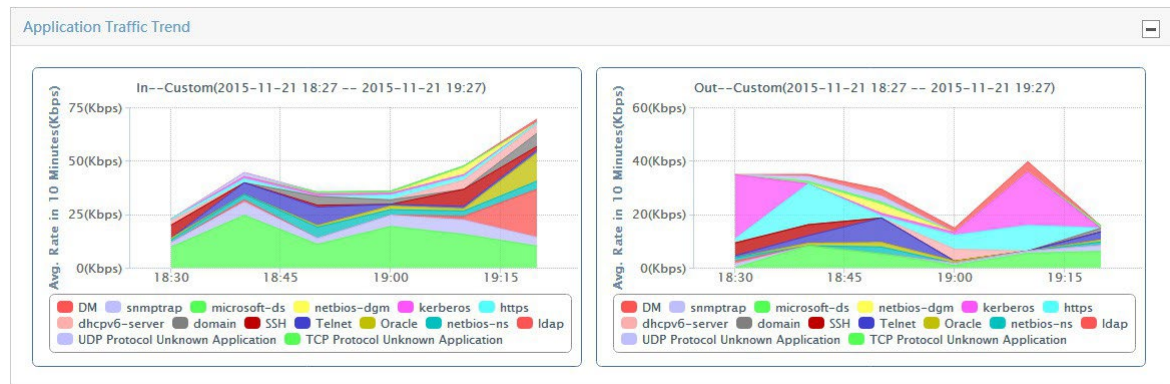
Select **8**, **15**, **50**, **100**, **200**, or **1000** on the lower right of the main pane to configure how many items per page you want to view.

Click the name of an application to view the report for the application. For more information about the report for each individual application, see "[Individual Application Reports](#)."

Application Traffic Trend

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all interfaces in the selected traffic analysis task or for an interface in a task for the selected time range. If more than one interface exists for the selected task, these statistics reflect traffic for all interfaces configured in a task.

Figure 22 Application Traffic Trend – In/Out



Individual Application Reports

NTA provides traffic trend statistics for the individual applications that were observed on the interfaces for a selected task. Individual application reports have the **Application Traffic Information** report that displays the average rate of traffic for the selected application and a source and destination host list that identifies which source and destinations contributed the greatest volume of traffic for the selected application.

Individual application reports also have the **TopN Application Usage List** for source and destination hosts, and reports for unknown TCP and UDP applications.

Unknown applications are those applications for which the Layer 4 TCP or UDP port number has not been assigned a name and is not included as an application in NTA. For more information about assigning names to TCP or UDP ports and adding them as applications to NTA, see ["Managing applications."](#)

To view individual application reports for an interface task or for a single interface in an interface task, click the name in the **Application** field of the **Application List** report for the application for which you want to view this report.

To view unknown application reports for an interface task or for a single interface in an interface task, click the icon  in the **Unknown Applications** field of the **Application List** report for the application for which you want to view this report.

For more information about **Application List**, see ["Application List."](#)

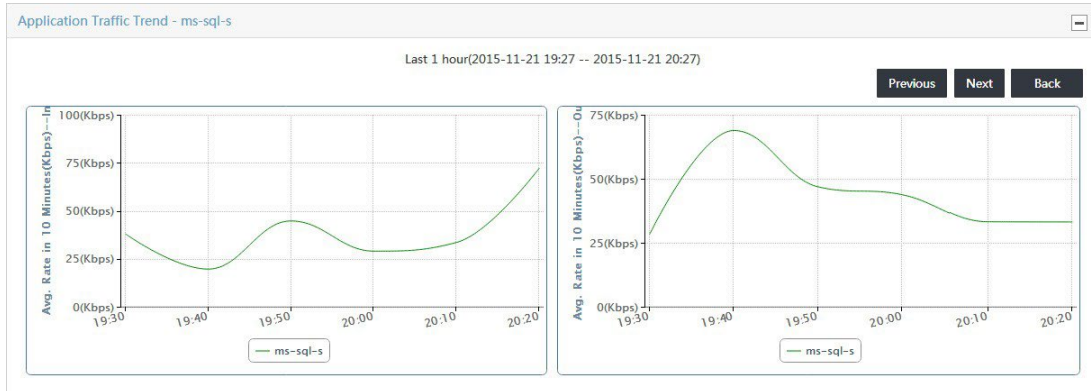
Application Traffic Trend

The **Application Traffic Trend** graph provides average rate of traffic for an individual application for all interfaces in the selected traffic analysis task or for an individual interface in a task. If more than one interface exists for the selected task, this chart reflects traffic for all interfaces configured in a task.

By default, the **Traffic Trend Report** graph displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.

Figure 23 Traffic Trend for an Individual Application



TopN application usage list

The TopN application usage list includes **Source Host List – In/Out** and **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or for an interface in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or for an interface in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

Figure 24 TopN Application Usage List

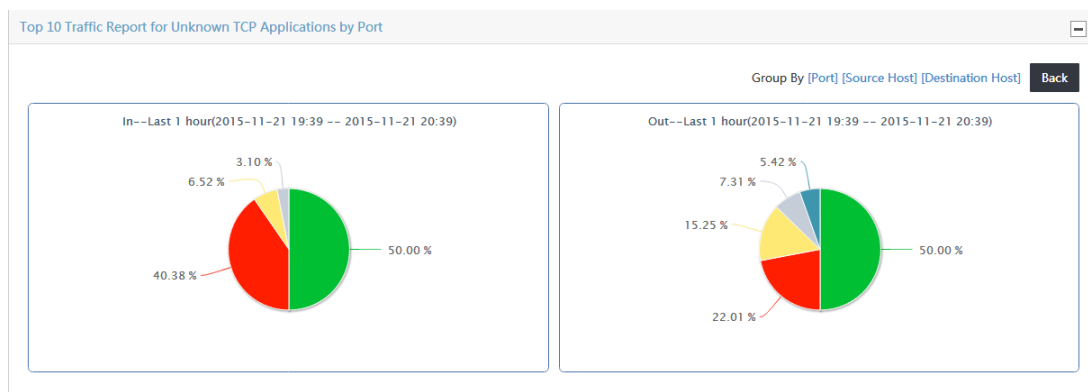
Top 10 Application Usage List - ms-sql-s					
Source Host List - In			Source Host List - Out		
Source Host IP Address	Traffic	Percentage	Source Host IP Address	Traffic	Percentage
 172.4.8.88	10.66 MB	62.40%	 172.4.8.88	11.74 MB	77.76%
 192.168.40.150	6.42 MB	37.60%	 192.168.40.150	3.36 MB	22.24%
Destination Host List - In			Destination Host List - Out		
Destination Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 192.168.40.150	10.66 MB	62.40%	 192.168.40.150	11.74 MB	77.76%
 172.4.8.88	6.42 MB	37.60%	 172.4.8.88	3.36 MB	22.24%

TopN Traffic Report for Unknown TCP/UDP Application by Port

The **TopN Traffic Report for Unknown TCP/UDP Application by Port – In/Out** provides the distribution of traffic by TCP or UDP port number for all application traffic that cannot be attributed to an application or protocol for all interfaces in the selected traffic analysis task for the selected time range. NTA enables you to change how the traffic is grouped.

To group by port, select **Port** located in the upper right corner of the **TopN Traffic Report for Unknown TCP/UDP Application by Port** area of the page. To group by source host, select **Source Host**. To group by destination host, select **Destination Host**. Click **Back** to return to the main **Application** report page.

Figure 25 TopN Traffic Report for Unknown Application by Port



TopN Traffic List for Unknown TCP/UDP Application by Port

The **TopN Traffic List for Unknown TCP/UDP Application by Port – In/Out** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic observed on all interfaces in the selected interface traffic analysis task for the selected time range.

This list has the TCP or UDP port number, total volume of traffic for the associated application port, rate of traffic, and the percentage of all observed traffic generated for the unknown application. The port number is a link to individual reports for the selected port. The icon  in the **Define Application** field is a link for adding the selected port as a Layer 4 application to NTA. For more information about managing applications in NTA, see "[Managing applications](#)."

Figure 26 TopN Traffic List for Unknown TCP/UDP Application by Port

Top 10 Traffic List for Unknown TCP Applications by Port									
In					Out				
Port	Traffic	Rate	Define Application	Percentage	Port	Traffic	Rate	Define Application	Percentage
49154	0.89 MB	2.08 Kbps		50.00%	49154	1.21 MB	2.83 Kbps		50.00%
52130	0.72 MB	1.68 Kbps		40.38%	52113	0.53 MB	1.24 Kbps		22.01%
53077	0.12 MB	0.27 Kbps		6.52%	53077	0.37 MB	0.86 Kbps		15.25%
52113	56.64 KB	0.13 Kbps		3.10%	52130	0.18 MB	0.41 Kbps		7.31%
					53051	0.13 MB	0.31 Kbps		5.42%

Traffic Trend Report for Unknown TCP/UDP Applications by Port

To view this report for an interface task, click the link in the **Port** field of the **TopN Traffic List for Unknown TCP Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **Traffic Trend** line chart provides the average rate for an individual unknown application for all interfaces in the selected traffic analysis task. If more than one interface exists for the selected task, this chart reflects traffic for all interfaces configured in a task. Click **Back** to return to the **Unknown Application Traffic Information** page.

Figure 27 Traffic Trend Report for Unknown Applications by Port



TopN Traffic Details List for Unknown TCP/UDP Applications by Port

To view this report for an interface task, click the link in the **Port** field of the **TopN Traffic List for Unknown TCP Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source host.

Figure 28 TopN Traffic Details for Unknown Applications by Port

Top 10 Traffic Details List for Unknown TCP Applications by Port - 1000				
Source Host	Destination Host	Traffic	Rate	Percentage
172.4.0.207	172.10.0.77	47.58 KB	0.11 Kbps	51.37%
172.4.0.201	172.10.0.77	18.12 KB	41.24 bps	19.57%
172.10.0.28	172.10.0.77	17.30 KB	39.38 bps	18.68%
172.2.0.11	172.10.0.77	9.45 KB	21.50 bps	10.20%
172.3.0.28	172.10.0.77	0.16 KB	0.36 bps	0.17%

Protocol reports

Protocol reports display traffic rate trend reports organized by the list of protocols predefined in NTA. Protocol reports have the **Protocol List**, which provides a list of protocols observed for all interfaces in the selected interface traffic analysis task or for an interface in a task. This report also provides capabilities for additional in-depth reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average inbound and outbound traffic rates for all protocols observed for all interfaces in the selected traffic analysis task or for an interface in a task. Protocol reports also have traffic lists and trend reports for individual protocols.

As with all the report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for an interface task, click the **Application** tab to view application reports for the selected interface traffic analysis task, and set **Query Type** to **Protocol** as described in "[Query protocols](#)." For more information about protocols in NTA, see "[Managing protocols](#)." This section describes the reports available for protocols.

Query protocols

To view reports by protocol, you must configure the filter criteria for application reports. NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, protocol, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.

2. Select **Protocol** from the **Query Type** list.

The page displays the report for protocols.

3. Specify the following query criterion:

- o **Protocol**—Next to the **Protocol** field, click **Select** to select the protocol for which you want to search.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the protocol you want to search for, you must first query the **Protocol List** as follows:

- a. Specify one or more of the following query criteria in the **Query Protocols** area:
 - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
 - **Pre-defined**—To search for protocols that are predefined, select **Yes** from the **Pre-defined** list. To filter for protocols that are user-defined, select **No** from the list. To include system, predefined, or user-defined protocols, select **Not limited**.
- b. To display the full **Protocol List**, click **Query** without entering any search criteria.
- c. Click **Query**. The query results are displayed in the **Protocol List** below the **Query Protocols** area.
- d. Select the check boxes next to the protocols for which you want to search.
- e. Click **OK** to add the protocol to the filter. The protocols you selected are displayed in the **Protocol** field.

Click **Clear**, located next to the **Protocol** field, to clear all selected protocols.

- **Start Time**—Enter the start time of the time range, in format of YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.

- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the protocol report, click the icon  in the upper right corner of the protocol report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for protocols.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

- a. To print this report, click the **Print** icon  on the toolbar.
- b. From **Page Range**, select the page range.
- c. To export the data, click **Export**.
- d. To export this report, click the **Export** icon  on the toolbar.
- e. Select the export file format from the **File Format** list. Options are:
 - **PDF**

- XLS
- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

f. From **Page Range**, select the page range.

g. Click **Export**.

Protocol List

The **Protocol List** provides a list of the protocols observed for all interfaces in the selected interface traffic analysis task or for an interface in a task for the selected time range. This list has the protocol name, total volume of traffic for the associated protocol, rate of traffic and the percentage of traffic on all interfaces generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.

Figure 29 Protocol List

Protocol List				
Protocol ↕	In Traffic ↕	In Speed ↕	Out Traffic ↕	Out Speed ↕
UDP	1.33 MB	3.10 Kbps	1.53 MB	3.56 Kbps
TCP	0.87 MB	2.03 Kbps	2.47 MB	5.76 Kbps
OSPF	0.50 MB	1.15 Kbps	51.27 KB	0.12 Kbps
ICMP	0.39 MB	0.91 Kbps	0.41 MB	0.96 Kbps
AH	23.16 KB	52.70 bps	0.16 MB	0.38 Kbps
GRE	8.20 KB	18.67 bps	0.00 B	0.00 bps
1-6 of 6, Page 1 of 1.				
< << 1 >> > 50				

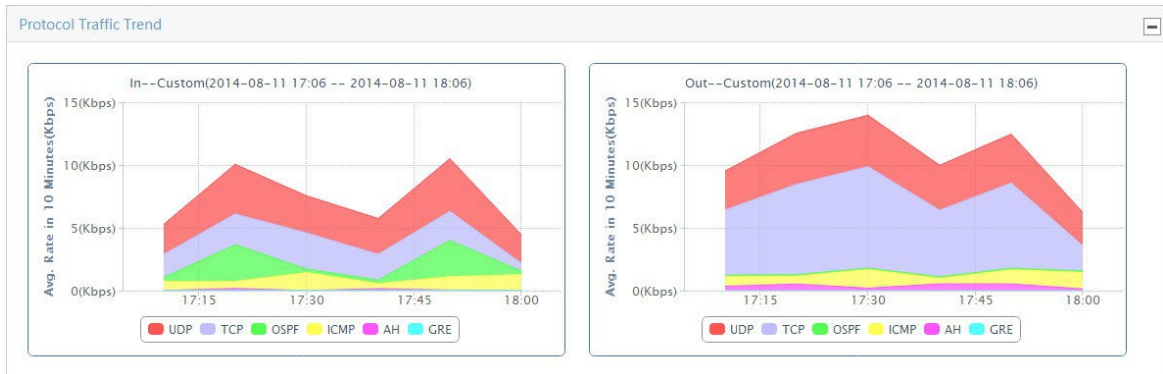
Select **8**, **15**, **50**, **100**, **200**, or **1000** from the lower right of the main pane to configure how many items per page you want to view.

Click the name of a protocol to see the report for the individual protocol. For more information about the reports for each individual protocol, see "[Individual protocol reports](#)."

Protocol traffic trend

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocols observed for all interfaces in the selected traffic analysis task or for an interface in a task for the selected time range. If more than one interface exists for the selected task, these statistics reflects traffic for all interfaces configured in a task.

Figure 30 Protocol Traffic Trend – In/Out



Individual protocol reports

NTA provides traffic trend statistics for the individual protocol that were observed on the interfaces for a selected task. Individual protocol reports have the **Protocol Traffic Trend** report that displays the average rate of traffic for the selected protocol and a source and destination host list that identifies which source and destination hosts contribute the greatest volume of traffic for the selected protocol. Individual protocol reports also have the **TopN Protocol Usage List** source and destination hosts.

To view individual protocol reports for an interface task or for a single interface in an interface task, click the name in the **Protocol** field of the **Protocol List** report for the protocol for which you want to view this report. For more information about the **Protocol List**, see "[Protocol List](#)."

Protocol Traffic Trend

The **Protocol Traffic Trend – In/Out** graph provides the average rate for an individual protocol for all interfaces in the selected traffic analysis task or for an interface in a task. If more than one interface exists for the selected task, this chart reflects traffic for all interfaces configured in a task.

By default, the **Protocol Traffic Trend – In/Out** report graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 31 Traffic Trend for an Individual Protocol – In/Out



TopN Protocol Usage List

The **TopN Protocol Usage List** includes the **Source Host List – In/Out** and **Destination Host List – In/Out** lists.

Figure 32 TopN protocol usage list

Top 10 Protocol Usage List - TCP					
Source Host List - In			Source Host List - Out		
Source Host IP Address	Traffic	Percentage	Source Host IP Address	Traffic	Percentage
 172.8.112.93	84.90 KB	9.52% 	 172.10.0.69	2.11 MB	85.93% 
 172.8.112.5	77.09 KB	8.64% 	 68.68.68.68	0.27 MB	11.04% 
 172.8.111.36	72.37 KB	8.11% 	 9.9.9.9	46.75 KB	1.86% 
 172.8.112.45	71.32 KB	7.99% 	 68.2.1.1	19.28 KB	0.77% 
 172.8.112.34	70.79 KB	7.93% 	 1.1.1.68	10.14 KB	0.40% 
 172.8.112.2	69.92 KB	7.84% 			
 172.20.0.24	68.76 KB	7.71% 			
 172.8.112.75	52.39 KB	5.87% 			
 172.8.112.76	50.70 KB	5.68% 			
 172.8.112.7	46.18 KB	5.18% 			
Other Hosts	0.22 MB	25.53% 			
Destination Host List - In			Destination Host List - Out		
Destination Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 172.10.0.69	0.76 MB	87.11% 	 172.8.112.93	0.25 MB	10.28% 
 68.68.68.68	49.62 KB	5.56% 	 172.8.111.36	0.21 MB	8.61% 
 9.9.9.9	45.85 KB	5.14% 	 172.8.112.45	0.21 MB	8.60% 
 68.2.1.1	19.50 KB	2.19% 	 172.8.112.2	0.21 MB	8.59% 
			 172.20.0.24	0.21 MB	8.59% 
			 172.8.112.5	0.21 MB	8.58% 
			 172.8.112.34	0.21 MB	8.58% 
			 3.3.3.3	0.18 MB	7.30% 
			 172.8.112.75	0.11 MB	4.44% 
			 172.8.112.76	0.11 MB	4.39% 
			Other Hosts	0.54 MB	22.03% 

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or for a selected interface in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task for the selected time range. This list has the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

Application category reports

Application category reports display traffic rate trend reports organized by the application categories in NTA. Application category reports for an interface traffic analysis task have the **Application Category List**, which provides a list of the application categories observed for all interfaces in the selected interface traffic analysis task. This list has total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic observed on all interfaces generated by the associated application category. This report also provides capabilities for additional in-depth reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all interfaces in the selected traffic analysis task. Application category reports also have traffic lists and trend reports for the individual application categories.

As with all the report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for an interface task, click the **Application** tab to view application reports for the selected interface traffic analysis task, and set **Query Type** to **Application Category** as described in "[Query application categories](#)."

NTA provides many system-defined application categories and also supports user-defined application categories. For more information about application categories in NTA, see "[Managing application categories](#)." This section describes the reports available for application categories.

Query application categories

To view reports by application category, you must configure the filter criteria for application category reports.

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application Category** from the **Query Type** list.
The page displays the report for application categories.
3. Specify the following query criterion:
 - o **Application Category**—Next to the **Application Category** field, click **Select** to select the application category for which you want to search.

The **Query Application Categories** dialog box displays an empty **Application Category List**.

To select the application categories you want to search for, you must first query the **Application Category List** as follows:

- a. Specify one or more of the following query criteria in the **Query Application Categories** area:
 - **Application Category**—Enter a partial or complete name for the application categories you want to search for in the **Application Category** field.
 - **Pre-defined**—To search for application categories that are predefined, select **Yes** from the **Pre-defined** list. To filter for application categories that are user-defined, select **No** from the list. To include system or predefined and user-defined application categories, select **Not limited**.
- b. To display the full **Application Category List**, click **Query** without entering any search criteria.
- c. Click **Query**.
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
- d. Select the check boxes next to the application categories for which you want to search.
- e. Click **OK** to add the application categories you have selected to the filter.
The application categories you selected are displayed in the **Application Category** field.
Click **Clear**, located next to the **Application Category** field, to clear all selected application categories.
 - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.

4. Click OK.

The page displays the results of your query.

Application Category List

The **Application Category List** provides a list of the application categories observed for all interfaces in the selected interface traffic analysis task or for an interface in a task for the selected time range. This list has the application category name, total volume of traffic for the associated application category, rate of traffic, and the percentage of traffic on all interfaces generated by the associated application category. The application category name in the **Application Category** field is a link to reports for the selected application category.

Figure 33 Application Category List

Application Category List				
Application Category ↕	In Traffic ↕	In Speed ↕	Out Traffic ↕	Out Speed ↕
File Service	1.25 MB	2.92 Kbps	0.21 MB	0.50 Kbps
Remote Management	2.46 MB	5.72 Kbps	3.70 MB	8.63 Kbps
Enterprise Application	6.02 MB	14.02 Kbps	5.66 MB	13.20 Kbps
HTTP	10.33 MB	24.07 Kbps	21.06 MB	49.08 Kbps
Network Management	15.48 MB	36.08 Kbps	12.08 MB	28.15 Kbps
Database Application	19.65 MB	45.79 Kbps	20.86 MB	48.61 Kbps
Other Application Category	17.63 MB	41.08 Kbps	14.07 MB	32.79 Kbps
1-7 of 7. Page 1 of 1.				

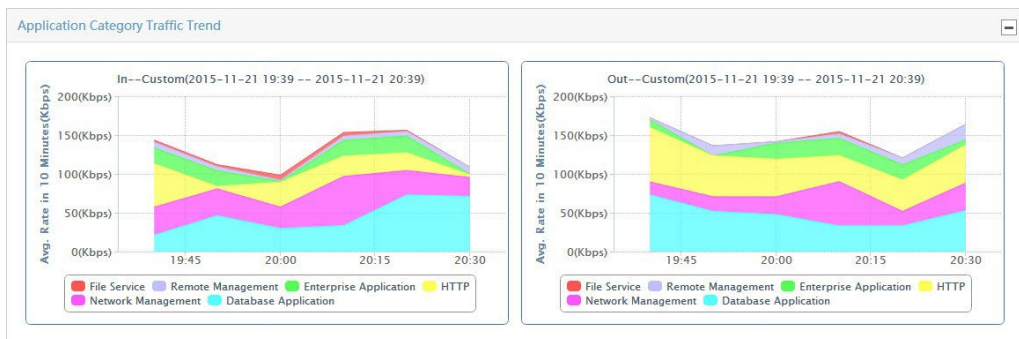
Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

Click the name of an application category to view the report for the individual application category. For more information about the report for each individual application category, see "[Individual application category reports.](#)"

Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all application categories observed for all interfaces in the selected traffic analysis task or for an interface in a task for the selected time range. If more than one interface exists for the selected task, these statistics reflects traffic for all interfaces configured in a task.

Figure 34 Application Category Traffic Trend – In/Out



Individual application category reports

NTA provides traffic trend statistics for the individual protocol categories observed on the interfaces for a selected task. Individual protocol category reports have the **Application Category Traffic Trend** report that displays the average rate of traffic for the selected application category. Individual application category reports also have the **TopN Application Category Usage List** that identifies the TopN source and destination hosts.

To view application category reports for an interface task or for a single interface in an interface task, click the name in the **Application Category** field of the **Application Category List** report for the application category for which you want to view this report. For more information about **Application Category List**, see "[Application Category List](#)."

Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** graph provides the average rate for an individual application category for all interfaces in the selected traffic analysis task or for an individual interface in a task. If more than one interface exists for the selected task, this chart reflects traffic for all interfaces configured in a task. By default, this graph displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.

Figure 35 Application Category Traffic Trend Report for an Individual Application Category – In/Out



TopN Application Category Usage List

The **TopN Application Category Usage List** includes **Source Host List – In/Out** and **Destination Host List – In/Out** lists.

Figure 36 TopN Application Category Usage List

Top 10 Application Category Usage List - Network Management					
Source Host List - In			Source Host List - Out		
Source Host IP Address	Traffic	Percentage	Source Host IP Address	Traffic	Percentage
 172.4.21.10	56.55 KB	6.62% 	 172.10.0.69	1.29 MB	100.00% 
 172.8.112.45	49.47 KB	5.79% 			
 172.8.112.93	49.41 KB	5.79% 			
 172.8.111.36	48.16 KB	5.64% 			
 172.8.112.2	48.14 KB	5.64% 			
 172.20.0.24	47.37 KB	5.55% 			
 172.8.112.5	41.80 KB	4.89% 			
 172.4.8.88	36.62 KB	4.29% 			
 172.8.112.24	35.61 KB	4.17% 			
 172.8.112.34	35.58 KB	4.17% 			
Other Hosts	0.40 MB	47.46% 			
Destination Host List - In			Destination Host List - Out		
Destination Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 172.10.0.69	0.83 MB	100.00% 	 172.8.112.93	75.79 KB	5.73% 
			 172.8.111.36	75.17 KB	5.68% 
			 172.8.112.45	74.98 KB	5.67% 
			 172.4.21.10	74.87 KB	5.66% 
			 172.8.112.2	74.78 KB	5.65% 
			 172.20.0.24	69.45 KB	5.25% 
			 172.8.112.5	64.56 KB	4.88% 
			 172.8.112.34	50.50 KB	3.82% 
			 172.4.8.88	41.08 KB	3.11% 
			 172.8.112.78	40.37 KB	3.05% 
			Other Hosts	0.67 MB	51.50% 

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or an individual interface for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source.

The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or an interface for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The

host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

Source reports

Source reports include inbound and outbound reports. Both reports have a **TopN Traffic Report for Source Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN source hosts for all interfaces in the selected traffic analysis task or for an interface in a task. Both reports also have the **TopN Traffic List for Source Host**, which provides a list of the TopN source hosts measured by volume of traffic observed on all interfaces in the selected traffic analysis task or for an interface in a task. The pie chart contains a link to traffic reports for the selected host.

The list also contains a link to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the host query. As with all report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an interface task, click the **Source** tab to view traffic reports for the selected interface traffic analysis task.

Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed under the **Source** tab.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Source Host**—In the **Source Host** field, enter the IP address or address range.
To enter the IP address for a single interface, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/64
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**

- RTF
- XLSX
- PPTX
- HTML
- JRXML

f. From **Page Range**, select the page range.

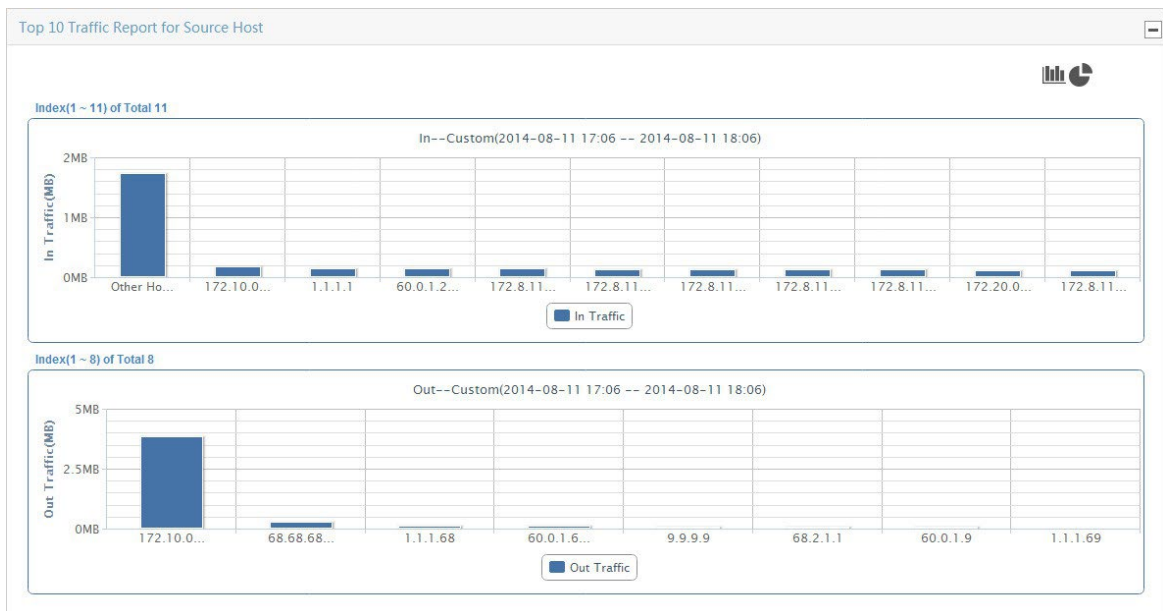
g. Click **Export**.

TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host – In/Out** bar chart displays the TopN source hosts with the most inbound/outbound traffic on all interfaces in a certain period of time in a selected interface traffic analysis task. Click a bar in the bar chart to view the traffic analysis report of each source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of the TopN source hosts on all interfaces in the selected traffic analysis task or on an interface in a task for the selected time range. The slices of the pie chart link to traffic reports for the selected host.

Figure 37 TopN Traffic Report for Source Host – In/Out



TopN Traffic List for Source Host

The **TopN Traffic List for Source Host – In/Out** provides a list of the TopN source hosts measured by volume of inbound/outbound traffic observed on all interfaces in the selected interface traffic analysis task or for an interface in a task for the selected time range. This list has the source interface IP address, total volume of traffic for the associated source, rate of traffic, and the percentage of all observed traffic generated by the source. The IP address is a link to reports for the selected source.

The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the query.

Figure 38 TopN Traffic List for Source Host- In/Out

Top 10 Traffic List for Source Host					
In			Out		
Generate Chart			Generate Chart		
Source	Traffic	Percentage	Source	Traffic	Percentage
172.4.8.88	10.26 MB	15.96%	172.4.8.88	13.72 MB	19.19%
192.168.40.150	9.17 MB	14.25%	192.168.40.150	6.59 MB	9.22%
192.168.40.180	4.94 MB	7.68%	192.168.40.180	5.68 MB	7.94%
192.168.40.25	4.66 MB	7.25%	192.168.20.24	5.47 MB	7.65%
192.168.40.186	3.57 MB	5.56%	192.168.40.186	4.73 MB	6.61%
192.168.1.135	3.52 MB	5.48%	192.168.40.118	4.19 MB	5.86%
192.168.20.24	3.50 MB	5.44%	192.168.40.21	3.37 MB	4.71%
10.153.0.114	2.50 MB	3.89%	192.168.40.165	3.03 MB	4.24%
192.168.40.80	1.55 MB	2.40%	192.168.40.104	2.50 MB	3.49%
10.153.0.61	1.44 MB	2.23%	192.168.40.201	1.74 MB	2.44%
Other Hosts	19.22 MB	29.87%	Other Hosts	20.49 MB	28.65%

Traffic trend report for source host

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Trend Report for Source Host** line chart provides the average rate of traffic for the selected source host. By default, the **Traffic Trend Report for Source Host** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.

Figure 39 Traffic Trend Report by Source Host



Traffic details

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Details** for a source host table provides two lists:

- The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and destination hosts, and the percentage of all traffic observed for this source and destination hosts.

- The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

Figure 40 Traffic Details

Traffic Details					
Top 10 Destination Hosts Communicating with the Source Host			Top 10 Applications Communicating with the Source Host		
Destination	Traffic	Percentage	Application Name	Traffic	Percentage
 192.168.40.150	10.26 MB	100.00% 	ms-sql-s	10.26 MB	100.00% 

Destination reports

Destination reports include inbound and outbound reports. Both reports have a **TopN Traffic Report for Destination Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN destination hosts for all interfaces in the selected traffic analysis task or for an interface in a task. Both reports also have the **TopN Traffic List for Destination Host**, which provides a list of the TopN destination hosts measured by volume of traffic observed on all interfaces in the selected traffic analysis task or for an interface in a task. The pie chart contains a link to traffic reports for the selected host.

The list also contains a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and a link to the results of the host query. As with all report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an interface task, click the **Destination** tab to view traffic reports for the selected interface traffic analysis task.

Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed under the **Destination** tab.

1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the destination report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single Interface, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

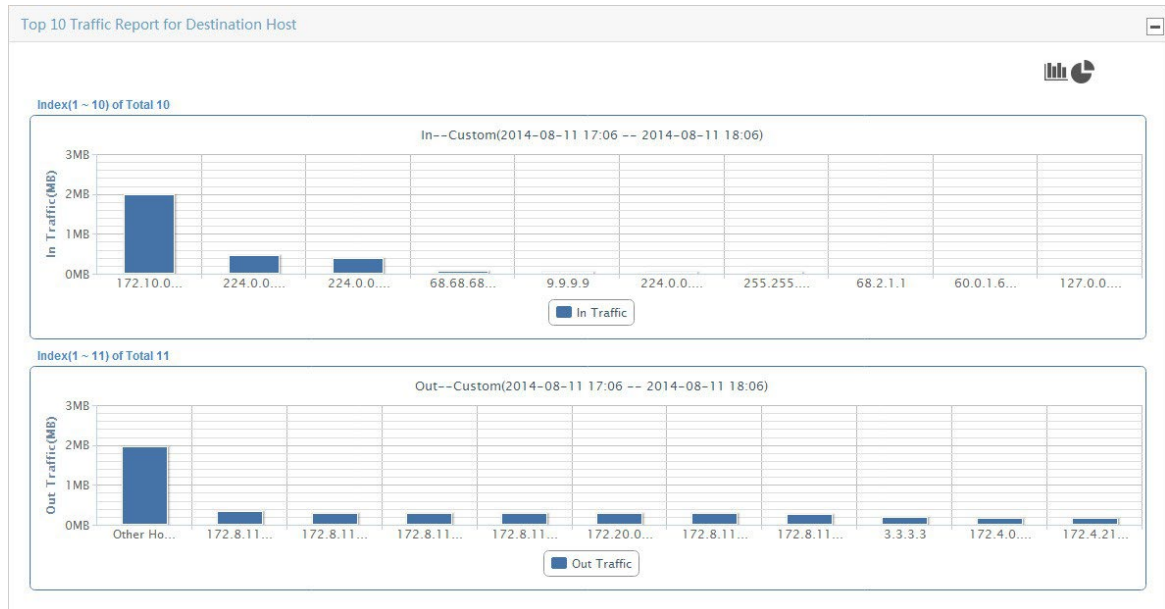
- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
- a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.
 - g. Click **Export**.

TopN traffic report for destination host

The **TopN Traffic Report for Destination Host – In/Out** bar chart displays the TopN destination hosts with the most inbound/outbound traffic on all interfaces in a certain period of time in a selected interface traffic analysis task. Click a bar in the bar chart to view the traffic analysis report of each destination host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of TopN destination hosts on all interfaces in the selected traffic analysis task for the selected time range. Each pie chart slice is a link to the traffic report of the selected destination host.

Figure 41 TopN Traffic Report for Destination Host – In/Out



TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host – In/Out** provides a list of the TopN destination hosts measured by volume of inbound/outbound traffic observed on all interfaces in the selected interface traffic analysis task for the selected time range. This list has the destination IP address, total volume of traffic generated by the associated destination Interface, rate of traffic, and the percentage of all observed traffic generated by the destination Interface.

The IP address is a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a destination host query and a link to the results of the query.

Figure 42 TopN Traffic List for Destination Host- In/Out

Top 10 Traffic List for Destination Host					
In Generate Chart			Out Generate Chart		
Destination	Traffic	Percentage	Destination	Traffic	Percentage
 192.168.40.150	10.49 MB	16.17%	 192.168.40.150	14.47 MB	20.17%
 172.4.8.88	5.97 MB	9.20%	 192.168.40.25	9.65 MB	13.45%
 192.168.40.180	5.76 MB	8.88%	 192.168.20.24	7.46 MB	10.40%
 192.168.20.24	3.86 MB	5.95%	 172.4.8.88	6.30 MB	8.77%
 172.4.95.18	3.52 MB	5.43%	 192.168.40.180	5.81 MB	8.09%
 192.168.40.21	2.65 MB	4.08%	 192.168.1.135	4.30 MB	5.99%
 192.168.40.186	2.62 MB	4.04%	 192.168.40.186	3.90 MB	5.43%
 192.168.1.135	2.47 MB	3.80%	 10.153.0.114	3.37 MB	4.70%
 192.168.40.130	2.41 MB	3.72%	 192.168.40.170	2.65 MB	3.69%
 192.168.40.22	2.29 MB	3.53%	 192.168.40.104	2.34 MB	3.26%
Other Hosts	22.82 MB	35.19%	Other Hosts	11.52 MB	16.05%

Traffic trend report for destination host

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.

Figure 43 Traffic Trend Report for Destination Host



Traffic details

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Details** for a destination host table provides two lists:

- The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.
- The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

Figure 44 Traffic Details

Top 10 Source Hosts Communicating with the Destination Host			Top 10 Applications Communicating with the Destination Host		
Source	Traffic	Percentage	Application Name	Traffic	Percentage
172.8.99.21	69.78 KB	26.54%	snmp	0.11 MB	41.62%
172.8.112.48	36.12 KB	13.74%	ICMP Protocol Application	86.63 KB	32.95%
172.8.112.79	34.96 KB	13.30%	UDP Protocol Unknown Application	20.00 KB	7.61%
172.4.0.201	22.97 KB	8.74%	TCP Protocol Unknown Application	19.16 KB	7.29%
172.8.112.26	22.10 KB	8.41%	echo	17.58 KB	6.69%
172.4.0.207	20.21 KB	7.69%	FTP	5.52 KB	2.10%
172.10.0.69	8.20 KB	3.12%	Telnet	2.14 KB	0.82%
172.10.0.30	6.88 KB	2.62%	SSH	1.59 KB	0.60%
172.8.112.138	6.80 KB	2.59%	http	0.86 KB	0.33%
172.10.0.28	3.24 KB	1.23%			
Other Hosts	31.62 KB	12.03%			

Session reports

A session is a unique source and destination host pair. Session reports include inbound and outbound reports. Both reports have the **TopN Traffic Report for Session Host** pie chart. The pie chart displays the distribution of the traffic generated by the TopN session hosts for all interfaces in the selected traffic analysis task or for an interface in a task for the selected time range. Both reports also have the **TopN Traffic List for Session Host**, which provides a list of the TopN session hosts measured by volume of traffic observed on all interfaces in the selected interface traffic analysis task or for an interface in a task. The pie chart contains a link to traffic reports for the selected session.

The list also contains a link to reports for the selected session host. The host query icon  next to the **Source Host** and **Destination Host** IP address is a link for initiating a host query and a link to the results of the host query. As with all report types for an interface task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an interface task, click the **Session** tab to view traffic reports for the selected interface traffic analysis task.

Query Sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the session report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - **Source Host**—In the **Source Host** field, enter the IP address or address range. To enter the IP address for a single Interface, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/64
 - **Destination Host**—In the **Destination Host** field, enter the IP address or address range. To enter the IP address for a single Interface, enter the IP address using dotted decimal notation.
 - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.

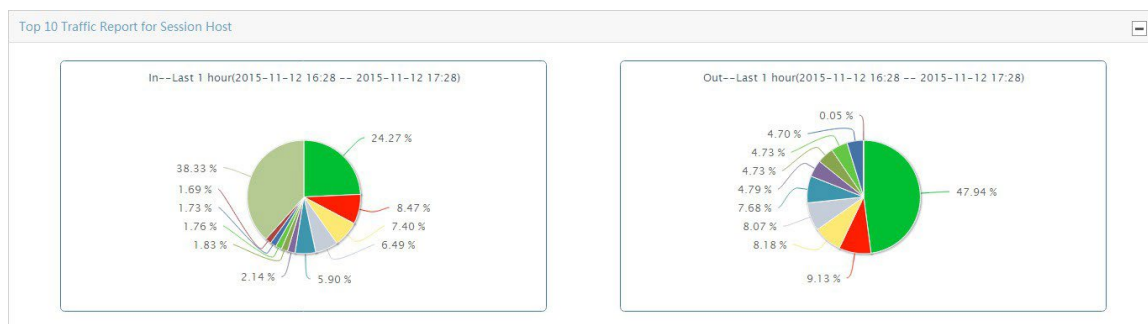
The page displays the results of your query.

5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - PDF
 - XLS
 - CSV
 - DOCX
 - RTF
 - XLSX
 - PPTX
 - HTML
 - JRXML
 - f. From **Page Range**, select the page range.
 - g. Click **Export**.

TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host – In/Out** pie chart displays the distribution of inbound/outbound traffic for TopN source and destination session pairs for all interfaces in the selected traffic analysis task or for an interface in a task for the selected time range. Each pie chart slice is a link to traffic reports for the selected source and destination session pair.

Figure 45 TopN Traffic Report for Session Host – In/Out



TopN Traffic List for Session Host

The **TopN Traffic List for Session Host – In/Out** provides a list of the TopN session source and destination pairs measured by volume of inbound/outbound traffic observed on all interfaces in the selected interface traffic analysis task for the selected time range. This list includes the source and destination IP addresses, total volume of traffic generated by the source and destination session pair, rate of traffic, and the percentage of all observed traffic generated between the source and destination session pair.

The icon  in the **Details** field is a link for viewing reports for the selected session or source/destination pair. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link to the results of the query.

Figure 46 TopN Traffic List for Session Host – In/Out

Top 10 Traffic List for Session Host											
In						Out					
Generate Chart						Generate Chart					
Source Host	Destination Host	Traffic	Percentage	Details	Topology	Source Host	Destination Host	Traffic	Percentage	Details	Topology
172.8.99.21	172.10.0.77	0.52 MB	24.27%			172.10.0.35	224.0.0.18	0.28 MB	47.94%		
172.4.0.201	172.10.0.77	0.18 MB	8.47%			172.5.0.68	224.0.0.2	53.64 KB	9.13%		
172.4.0.207	172.10.0.77	0.16 MB	7.40%			172.10.0.1	224.0.0.5	48.11 KB	8.18%		
172.10.0.35	224.0.0.18	0.14 MB	6.49%			172.10.0.78	224.0.0.5	47.43 KB	8.07%		
172.8.112.11	172.10.0.77	0.13 MB	5.90%			172.10.0.77	224.0.0.5	45.15 KB	7.68%		
172.8.11.105	172.10.0.77	46.62 KB	2.14%			172.10.0.88	224.0.0.5	28.19 KB	4.79%		
172.8.112.89	172.10.0.77	39.80 KB	1.83%			172.5.0.1	224.0.0.5	27.81 KB	4.73%		
172.8.112.9	172.10.0.77	38.21 KB	1.76%			172.200.0.1	224.0.0.5	27.81 KB	4.73%		
172.8.112.41	172.10.0.77	37.54 KB	1.73%			172.200.99.5	224.0.0.5	27.62 KB	4.70%		
172.8.112.177	172.10.0.77	36.69 KB	1.69%			172.5.0.200	172.5.0.255	0.15 KB	0.03%		
Other Hosts	Other Hosts	0.81 MB	38.33%			Other Hosts	Other Hosts	0.12 KB	0.02%		

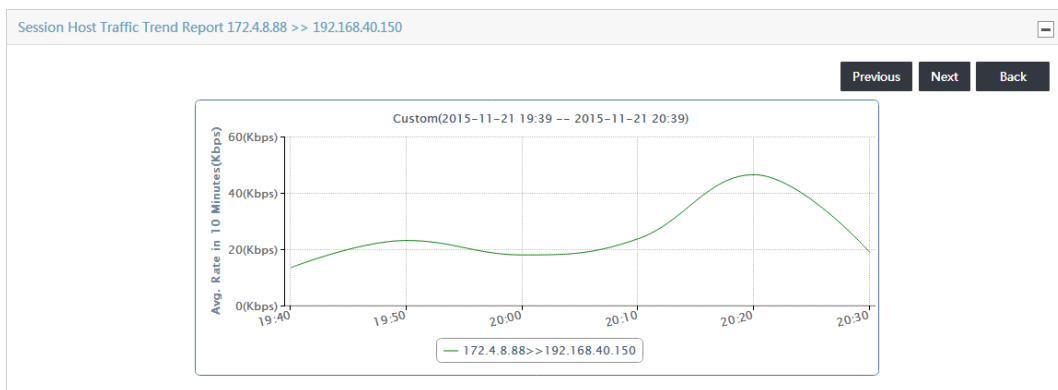
Session Host Traffic Trend Report

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Host Traffic Trend Report** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.

Figure 47 Session Host Traffic Trend Report



TopN Applications for Session Host

To view this report for an interface task or for an interface in a task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

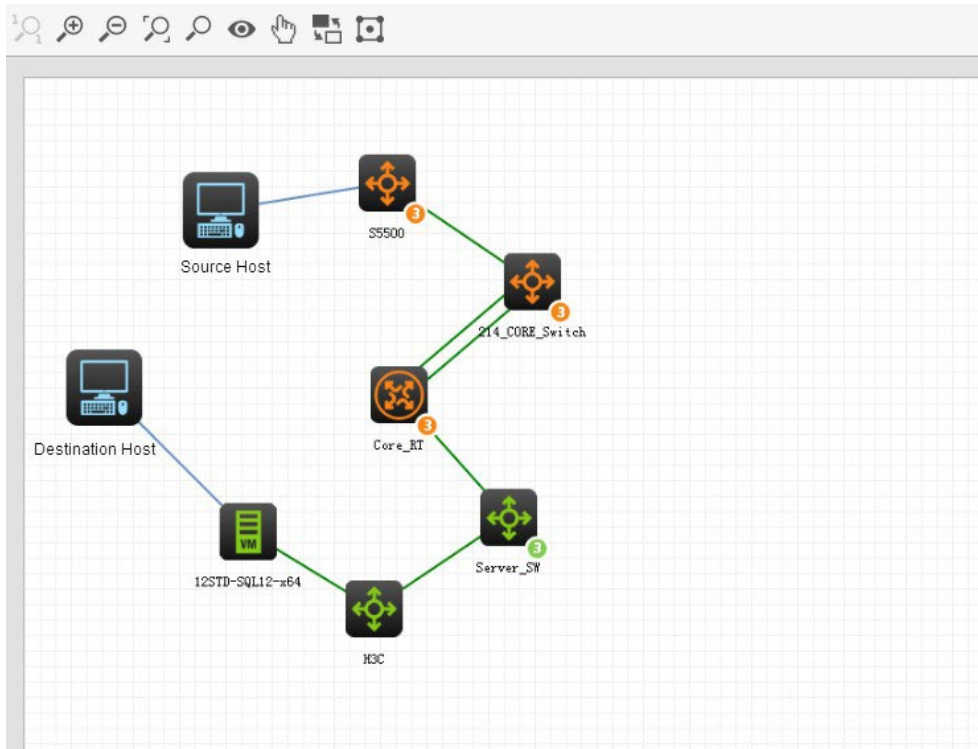
Figure 48 TopN Applications for Session Host

Top 10 Applications for Session Host 172.4.8.88 >> 192.168.40.150		
Application Category	Traffic	Percentage
ms-sql-s	10.26 MB	100.00%

Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source host and destination host, as shown in [Figure 49](#).

Figure 49 Session host topology



! IMPORTANT:

When each node between the source and destination hosts exists in INC, the topology displays a complete link. Otherwise, a virtual cloud icon  is displayed in the link between the two hosts, instead of nodes between the two hosts.

The following describes topology map toolbar operations.

-  Displays the network in its original proportion.
-  Enables you to zoom in on the topology view.
-  Enables you to zoom out on the topology view.
-  Enables you to fit the contents of the topology view into the window.
-  Enables you to magnify the contents on the topology view.
-  Provides a separate bird's eye view window of the topology map.

-  Enables you to grab and move one or multiple objects in the topology view within the confines of the pane. Click the icon to switch to the **Pointer Tool** icon  , which allows you to move the entire topology view within the confines of the pane.
-  Allows you to display or hide grids. The grids is under the background picture.
-  Enables you to organize icons according to a pre-defined structure to the topology view. Options for organizing topology views include union length, tree, star, ring or grid.

VLAN/VXLAN monitoring

This chapter of the NTA administrator guide provides information on VLAN/VXLAN monitoring in NTA, including how NTA analyzes network flow records report on network traffic from VLAN or VXLAN perspective. This chapter describes the reporting options for VLAN/VXLAN traffic analyses and reviews configuration issues around VLAN/VXLAN monitoring and traffic analysis tasks and the reports they generate. This chapter also describes the process for adding VLAN/VXLAN traffic analysis tasks, including instructions for adding, modifying, and deleting tasks from NTA. It also provides a survey of the summary reports for all VLAN/VXLAN tasks and a look at the more granular reports for an individual VLAN/VXLAN traffic analysis task.

VLAN/VXLAN traffic analysis overview

VLAN/VXLAN traffic analysis tasks analyze network flow data by the VLAN or VXLAN you specify in VLAN/VXLAN traffic analysis tasks. NTA parses all network flow data and provides statistical views of traffic in a VLAN/VXLAN traffic analysis task. For example, NTA provides source and destination host information reporting by VLAN or VXLAN, displaying the rate of traffic attributed to specific source or destination hosts that send or receive traffic from the selected VLAN or VXLAN.

In general, the NTA VLAN/VXLAN traffic analysis tasks provide traffic statistics for the VLAN or VXLAN configured in every VLAN/VXLAN traffic analysis task. The VLAN/VXLAN traffic reports include rate of traffic for all VLANs or VXLANs in all tasks, for all VLANs or VXLANs in each task, and for individual VLANs or VXLANs in a task. VLAN/VXLAN statistics include traffic rate by application, source host, destination host, and a session or source/destination host pair. These reports are organized in layers from summarized information for all tasks to detailed reporting for specific VLANs or VXLANs configured for an individual VLAN/VXLAN traffic analysis task.

To use VLAN/VXLAN traffic analysis, follow these guidelines:

- To collect VLAN/VXLAN traffic statistics, the traffic direction (incoming or outgoing) must be identified. Otherwise, the traffic is counted repeatedly. NTA globally controls the direction of VLAN or VXLAN traffic through parameter management. By default, the incoming VLAN/VXLAN traffic statistics are collected.
- VLAN traffic analysis is available on only devices supporting sFlow. The NetFlow and NetStream traffic statistics packets do not carry VLAN tags.
- Devices used to analyze VXLAN traffic must support NetStream v9.

VLAN/VXLAN traffic analysis reporting overview

After you create the first VLAN/VXLAN traffic analysis task, NTA creates an entry called  **VLAN/VXLAN Traffic Analysis Task** under the **Traffic Analysis and Audit** area on the left navigation tree.

Click **VLAN/VXLAN Traffic Analysis Task** on the left navigation tree to view the summary report for all VLAN/VXLAN traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **VLAN/VXLAN Traffic Analysis Task**. The **VLAN/VXLAN Traffic Analysis Task** shortcut menu displays all VLAN/VXLAN traffic analysis tasks created in NTA. Click the name of a task to view the VLAN/VXLAN traffic analysis report of the task.

To view the traffic analysis report of a VLAN or VXLAN in a VLAN/VXLAN traffic analysis task, click the **Expand** icon  next to the task on the shortcut menu to display all VLANs or VXLANs in the task. Click the name of a VLAN or VXLAN to view the VLAN/VXLAN traffic analysis report of the individual VLAN or VXLAN.

The summary VLAN/VXLAN traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides summarized average rate per second reporting for all VLANs or VXLANs specified in all VLAN/VXLAN traffic analysis tasks summarized by task. Each bar in the graph is a link to more detailed reporting for the selected task. Each of these report types includes several reports for the selected task:
 - **Traffic**—Reports include traffic trends that display the average inbound or outbound rate per second, TopN by ToS, and the individual data samples for all VLANs or VXLANs for the selected task or for a VLAN or VXLAN in a task.
 - **Application**—Reports include a table displaying percentage of application traffic generated by all VLANs or VXLANs in a task and a graph displaying average rate of application traffic for all VLANs or VXLANs in the selected task or for an individual VLAN or VXLAN in a task.
 - **Source**—Reports include a pie chart displaying the percentage of traffic generated by the TopN source hosts and a table displaying volume and percentage of traffic generated for each of the TopN source hosts for all VLANs or VXLANs in the selected task or for an individual VLAN or VXLAN in a task. The pie chart is a link to more detailed reporting for the selected host.
 - **Destination**—Reports include a pie chart displaying the percentage of traffic generated by the TopN destination hosts and a table displaying volume and percentage of traffic generated for each of the TopN destination hosts for all VLANs or VXLANs in the selected task or for an individual VLAN or VXLAN in a task. The contents of the pie chart link to more detailed reporting for the selected host.
 - **Session**—Reports include a pie chart displaying the percentage of traffic generated by the TopN source and destination host pairs and a table displaying volume and percentage of traffic generated for each of the TopN source and destination host pairs for all VLANs or VXLANs in the selected task or for an individual VLAN or VXLAN in a task. The contents of the pie chart link to more detailed reporting for the selected session.
- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—Provides per second average traffic rate summarized by VLAN/VXLAN traffic analysis task for inbound or outbound traffic for all VLANs or VXLANs for the selected task or for an individual VLAN or VXLAN in a task. A second set of pie charts reveals the distribution of traffic for the TopN applications, with one chart for inbound traffic and one chart for outbound traffic.
- **Summary List (Last 1 Hour)**—Provides per second traffic rate and the last hour traffic statistics summarized by VLAN/VXLAN traffic analysis task for inbound or outbound traffic for all VLANs or VXLANs in all tasks.

VLAN/VXLAN traffic analysis configuration considerations

When you add a VLAN or VXLAN to a task, you must decide which VLAN or VXLAN belongs to each task. This determines how NTA groups the VLANs or VXLANs for analysis, reporting, and navigation purposes. Viewing statistics in juxtaposition to each other provides an additional layer of analysis and interpretation of data. You must also consider the following:

- By default, NTA does not monitor any VLANs or VXLANs. You must create a task for every VLAN or VXLAN, or group of VLANs or VXLANs, which you want to monitor and report on.
- You define how NTA groups VLANs or VXLANs for analysis and reporting purposes. NTA presents VLAN/VXLAN traffic analysis tasks in the NTA left navigation system and provides summarized VLAN/VXLAN reporting based on the way you have organized VLANs or VXLANs into tasks.
- You can add one or more VLANs or VXLANs from one or more devices into a single task. You are not limited to adding VLANs or VXLANs from a single device into one task. As a best practice, add one VLAN or VXLAN to only one VLAN/VXLAN traffic analysis task to facilitate collecting traffic statistics.
- Add only VLANs or VXLANs whose statistics you want to view. Do not add all VLANs or VXLANs on a device unless you want to view reporting for all VLANs or VXLANs.

- When you add a VLAN/VXLAN traffic analysis task, you must specify the devices and VLANs/VXLANs for which traffic statistics are analyzed and collected. When you select devices, NTA presents a list of all devices that NTA knows about. This list is generated from the devices added to NTA using the Device Management feature. If the devices you want to add are not displayed on this list, and if they are not included in another traffic analysis task, it is likely that the device has not been added to NTA or it has not been selected in the NTA server configuration in Server Management. For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)." If the VLAN management module is deployed, VLAN information is configured automatically on devices from the VLAN management module, and you only need to select the target VLANs. Otherwise, you must manually configure the target VLANs. VXLANs must be manually configured.
- If you do not add a VLAN or VXLAN to a task, NTA will not report on it.
- Careful planning and documenting of VLAN/VXLAN tasks is valuable to help identify the task to which an application has been added when you begin creating tasks.
- Enable sFlow on devices and interfaces, and send traffic data to NTA. Only devices supporting sFlow can collect VLAN traffic statistics.
- To collect VXLAN traffic, first configure NetStream settings on the device that supports NetStream v9.

Managing VLAN/VXLAN traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA will not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need.

Viewing VLAN/VXLAN traffic analysis tasks

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view the NTA traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

Traffic Analysis Task list contents

- **Task Name**—Name of the task. This field is a link to the **Traffic Analysis Task Details** page for the task.
- **Task Description**—Description for the task.
- **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
- **Baseline Analysis**—Displayed when the Baseline Analysis feature is enabled in NTA parameters. The Baseline Analysis feature provides an additional layer of analysis to NTA reports by including baseline trend data that has been collected for a minimum of one week.

- **Modify**—Contains an icon  for modifying the associated task.
 - **Delete**—Contains an icon  for deleting the associated task.
3. To view NTA for the most recent **Traffic Analysis Task List**, click **Refresh** in the upper left corner of the **Traffic Analysis Task List**.
- You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label that allows you to toggle between the sort options specific to each field.

Viewing VLAN/VXLAN traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. To view the details of a VLAN/VXLAN traffic analysis task, click the name of a task of the **VLAN/VXLAN** task type.
Traffic analysis task details page
 - **Task Name**—Name of the task.
 - **Task Description**—Description of the task.
 - **Server**—Name or IP address of the NTA server.
 - **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **VLAN Type**—Type of the VLAN. Options are **VLAN** and **VXLAN**.
 - **Statistics Direction**—Direction of the VLAN or VXLAN traffic whose statistics are collected by NTA. Options are **In** and **Out**.
 - **Reader**—INC operator groups that have been granted access to view the reports generated by the associated traffic analysis task.
 - **Baseline Analysis**—Whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
 - **VLAN/VXLAN Information**—Displays information about the VLAN/VXLAN traffic statistics that are collected and analyzed in the VLAN/VXLAN analysis tasks. The VLAN/VXLAN information includes the VLAN/VXLAN ID and VLAN/VXLAN name.
 - **Device Information**—Displays information about the device traffic statistics that are collected and analyzed in the VLAN/VXLAN analysis tasks. The device information includes the device name and device IP. Only traffic sent from these devices can be collected and analyzed by NTA.
4. Click **Back** to return to the **Traffic Analysis Task List**.

Adding a VLAN/VXLAN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.

The **Add Traffic Analysis Task** page is displayed.
4. To add a VLAN/VXLAN traffic analysis task, select **VLAN/VXLAN** in the **Select Task Type** area.
5. Click **Next**.

The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.

The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. Enter a description for this task in the **Task Description** field.
8. Select the NTA sFlow or NetStream collection server from the **Server** list.

Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
9. Select **VLAN** or **VXLAN** from the VLAN type list.
10. Select the statistics direction. Options are **In** and **Out**.
11. To select the operator groups that have access to the analysis and reports provided by this VLAN/VXLAN task, click **Select** next to the **Reader** field. The **Choose Operator Group** dialog box is displayed.
 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for each operator group to which you want to allow access. To select all operator groups, select the check box in the upper left corner of the column label field.
 - b. Click **OK** to accept your operator group selection.

The operator groups you selected are displayed in the **Reader** field.
12. To enable baseline analysis for the reports generated by this task, select **Enable** from the **Baseline Analysis** list.

If you select **Enable**, the baseline trendline is displayed on graphs approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week of data collection, and is adjusted as more data is collected.

To disable baseline analysis, select **Disable**.

If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is not enabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
13. To specify the VLANs or VXLANs for which traffic statistics are collected and analyzed, click **Select**. Options are automatic and manual. After configuring the VLANs or VXLANs, click **Add**. The information for the VLANs or VXLANs is displayed on the VLAN/VXLAN list.
 - o **Auto**—NTA uses the VLAN management module to obtain the VLAN information in the network. Select the VLANs for which traffic statistics are collected and analyzed. For more information about the VLAN management module,

- o **Manual**—Manually enter the IDs and names of VLANs or VXLANs for which traffic statistics are collected and analyzed.
14. On the **Device List**, select the devices for which the traffic statistics are collected and analyzed.
 15. Click **OK** to create the VLAN/VXLAN traffic analysis task.

When you create a VLAN/VXLAN traffic analysis task, NTA creates an entry called  **VLAN/VXLAN Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the VLAN/VXLAN traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **VLAN/VXLAN Traffic Analysis Task**. The **VLAN/VXLAN Traffic Analysis Task** shortcut menu displays all VLAN/VXLAN traffic analysis tasks created in NTA. Click the name of a task to view the VLAN/VXLAN traffic analysis report of the task.

Click the **Expand** icon  next to a VLAN/VXLAN traffic analysis task on the shortcut menu to display all VLANs or VXLANs in the task. Click the name of a VLAN or VXLAN to view the VLAN/VXLAN traffic analysis report of the individual VLAN or VXLAN.

For more information on accessing and viewing VLAN/VXLAN traffic analysis reports, see "[Viewing VLAN/VXLAN traffic analysis reports](#)."

 IMPORTANT:

You must also configure sFlow traffic from the configured devices to the NTA server. For instructions, see the device configuration guides.

Modifying a VLAN/VXLAN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  associated with the VLAN/VXLAN traffic analysis task you want to modify.
The **Modify Traffic Analysis Task** page is displayed.
4. Modify the task name in the **Task Name** field.
The task name must be unique.
5. Modify the task description in the **Task Description** field.
6. Select the NTA sFlow or NetStream collection server from the **Server** list.
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server.
If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. Select **VLAN** or **VXLAN** from the VLAN type list.
8. Select the statistics direction. Options are **In** and **Out**.
9. To add new operator groups that have access to the analysis and reports provided by this VLAN/VXLAN task, click **Select** next to the **Reader** field. The **Operator Group List** dialog box is displayed.
 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for each operator group to which you want to grant access.
To select all operator groups, select the check box in the upper left corner of the column label field.

- b. Click **OK** to accept the additions to operator group.
The selected operator groups are displayed in the **Reader** field.
 - c. To revoke operator group access to the results of this VLAN/VXLAN traffic analysis task, highlight the groups you want to remove in the **Reader** field.
 - d. Click **Delete**.
 - e. Click **OK** to confirm the deletion of the selected operator groups from the task.
The **Reader** list is updated to reflect the deleted operator group changes.
10. To enable baseline analysis for the reports generated by this task, select **Enable** from the **Baseline Analysis** list. To disable baseline analysis, select **Disable**. If you select **Enable**, the baseline analysis trendline is displayed on graphs approximately seven days after the creation of the task. Initially the baseline trendline displays statistics based on the first week of data collection and is adjusted as more data is collected.
- If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is not enabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
11. To specify the VLANs or VXLANs for which traffic statistics are collected and analyzed, click **Select**. Options are automatic and manual.
- o **Auto**—NTA uses the VLAN management module to obtain the VLAN information in the network. Select the VLANs for which traffic statistics are collected and analyzed. For more information about the VLAN management module,
 - o **Manual**—Manually enter the IDs and names of VLANs or VXLANs for which traffic statistics are collected and analyzed.
- After configuring the VLANs or VXLANs, click **Add**. The information for the VLANs or VXLANs is displayed on the VLAN/VXLAN list. To remove a VLAN or VXLAN from a VLAN/VXLAN traffic analysis task, click the **Delete** icon  for the VLAN or VXLAN you want to remove.
12. On the **Device List**, select the devices for which the traffic statistics are collected and analyzed.
13. Click **OK** to accept modifications to the VLAN/VXLAN traffic analysis task.

Deleting a VLAN/VXLAN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the VLAN/VXLAN traffic analysis task you want to delete.
4. Click **OK** to confirm the deletion of the selected VLAN/VXLAN traffic analysis task.
The **Traffic Analysis Task List** is updated to reflect the removal of the deleted task.

Viewing VLAN/VXLAN traffic analysis reports

NTA provides levels of reporting for all traffic analysis tasks. The highest level provides summarized reporting for all tasks of the same type. The task types are interface, VLAN/VXLAN, probe, application, host, VPN, interbusiness or BGP AS. To access these reports, click the highest level entry on the left navigation tree in the **Traffic Analysis and Audit** area. To view summarized reporting for all VLAN/VXLAN tasks, click the  **VLAN/VXLAN Traffic Analysis Task** entry on the left navigation tree.

NTA also provides more detailed reporting for individual tasks, including reports for every VLAN or VXLAN configured in a VLAN/VXLAN traffic analysis task. NTA groups individual tasks by type. All VLAN/VXLAN tasks can be found on the **VLAN/VXLAN Traffic Analysis Task** menu.

To view the **VLAN/VXLAN Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to the  **VLAN/VXLAN Traffic Analysis Task**. The shortcut menu displays all VLAN/VXLAN traffic analysis tasks created in NTA. Click the name of a task to view the VLAN/VXLAN traffic analysis report of the task. Click the **Expand** icon  next to a task on the shortcut menu to display all VLANs or VXLANs in the VLAN/VXLAN traffic analysis task. Click the name of a VLAN or VXLAN to view the VLAN/VXLAN traffic analysis report of the individual VLAN or VXLAN.

This section describes the reporting options available for VLAN/VXLAN traffic analysis tasks, the process for navigating to VLAN/VXLAN traffic analysis tasks, the summary reports available for VLAN/VXLAN tasks, and the reports and features available for VLAN/VXLAN traffic analysis tasks.

Navigating to VLAN/VXLAN traffic analysis reports

1. Click the **Service** tab.
2. To view summary reporting for all VLAN/VXLAN tasks, click the  **VLAN/VXLAN Traffic Analysis Task** entry in the **Traffic Analysis and Audit** area on the left navigation tree.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to the  **VLAN/VXLAN Traffic Analysis Task**.
The **VLAN/VXLAN Traffic Analysis Task** shortcut menu displays all VLAN/VXLAN traffic analysis tasks created in NTA. Click the name of a task to view the VLAN/VXLAN traffic analysis report of the task.
4. To view the VLAN/VXLAN traffic analysis report of a VLAN or VXLAN in a VLAN/VXLAN traffic analysis task, click the **Expand** icon  next to a task on the shortcut menu to display the all VLANs or VXLANs in the VLAN/VXLAN traffic analysis task. Click the name of a VLAN or VXLAN to view the VLAN/VXLAN traffic analysis report of the individual VLAN or VXLAN.

Summary reports for all VLAN/VXLAN traffic analysis tasks

Summarized reports are the highest level of reporting for all tasks of the same type. To access these reports, click the  **VLAN/VXLAN Traffic Analysis Task** entry on the left navigation tree in the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

Average rate (last 1 hour)

The **Average Rate (Last 1 Hour)** bar graph summarizes the average rate of traffic for all VLANs or VXLANs in every VLAN/VXLAN traffic analysis task, grouped by task during the last hour. The bars in the graph are links to the detailed reports for the selected task.

Figure 50 Average Rate (Last 1 Hour)



Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

The **Traffic Trend** line chart and the **TopN Application for selected task** pie chart:

- The **Traffic Trend** line chart summarizes the average rate of inbound or outbound traffic for all VLANs or VXLANs in the selected VLAN/VXLAN traffic analysis tasks during the last hour.
- The **TopN Application** pie chart displays the distribution of inbound or outbound traffic for the TopN applications for all VLANs or VXLANs in the selected VLAN/VXLAN traffic analysis task during the last hour.

Figure 51 Traffic Trend and TopN Application for Selected Task (Last 1 Hour)



No data is graphed on these charts until you specify a task.

1. To select the task, click **Select Task** in the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar.
The **Choose NTA Task** dialog box is displayed.
2. Select the check boxes next to the VLAN/VXLAN traffic analysis tasks you want to view in this report.
3. Click **OK**. The page displays the **Traffic Trend** and **TopN Application** reports for the selected VLAN/VXLAN task.

Summary List (Last 1 Hour)

The **Summary List (last 1 hour)** displays inbound and outbound VLAN or VXLAN traffic volume and the rate of each VLAN/VXLAN traffic analysis task during the last hour.

Figure 52 Summary List (Last 1 Hour)



Summary list contents

- **Task Name**—Name of the VLAN/VXLAN traffic analysis task. The field is a link to reports for the associated task.
- **Traffic**—Volume of incoming and outgoing traffic for the VLAN/VXLAN traffic analysis task in the last hour.
- **Rate**—Rate of incoming and outgoing traffic for the VLAN/VXLAN traffic analysis task in the last hour.

Click **Refresh** to update the reports with the most recent data.

The **Add** button at the top of the **Summary List** provides a shortcut to the **Add VLAN/VXLAN Traffic Analysis Task** page. For more information on adding VLAN/VXLAN traffic analysis tasks, see "[Adding a VLAN/VXLAN traffic analysis task.](#)"

Detailed reports for a VLAN/VXLAN traffic analysis task

NTA provides a suite of reports for viewing VLAN or VXLAN data. VLAN/VXLAN reports are organized into the following reporting groups: traffic, application, source, destination, and session.

- Traffic reports provide overall traffic statistics.
- Application reports provide traffic statistics by application, protocol, and application category. Application reports are for Layer 4 through Layer 7 applications. The application report types follow:
 - Application reports
 - Protocol reports
 - Application category reports
- Source reports provide rate and percentage distribution of traffic by source host.
- Destination reports provide rate and percentage distribution of traffic by destination host.
- Session reports provide rate and percentage distribution of traffic for source and destination pairs.

Source, destination, and session reports allow you to access traffic reports for individual hosts and sessions.

Traffic reports

Traffic reports provide overall traffic statistics for all VLANs or VXLANs configured in a VLAN/VXLAN traffic analysis task, or for an individual VLAN or VXLAN in a task. Click the **Traffic** tab to view traffic reports.

The traffic report contains the following fields:

- **Query Traffic**—Time range for the data displayed in the traffic report.
- **Traffic Trend**—Average inbound traffic rates or outbound traffic rates for all VLANs or VXLANs in the task. This chart also provides total traffic volume, minimum average, maximum average, and average statistics in a table.
- **Flux Distribute In VLAN/VXLAN**—Average rate of inbound or outbound traffic for every VLAN or VXLAN configured in the task.
- **VLAN/VXLAN Flux Trend**—Average inbound traffic rates or outbound traffic rates for selected VLANs or VXLANs configured in the task.
- **Traffic Details**—Data collection samples that include timestamp, total volume of traffic, and traffic rate in seconds for inbound traffic or outbound traffic.

Query traffic

NTA enables you to change the filter criteria for traffic reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
 - a. Specify the following query criteria:
 - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
 - b. Click **OK**.

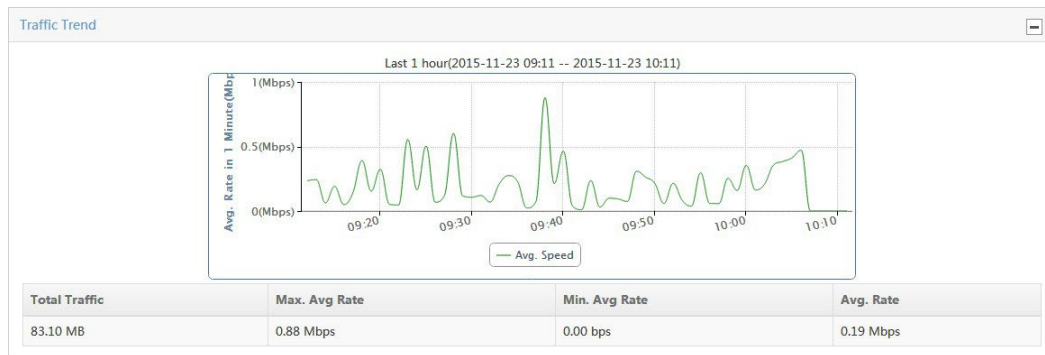
Traffic Trend

The **Traffic Trend** line chart displays average inbound or outbound traffic rates for all VLANs or VXLANs in the traffic analysis task or for a specific VLAN or VXLAN in a VLAN/VXLAN task. This chart also shows total traffic volume statistics, maximum average, minimum average, and average in a table for inbound or outbound traffic for the associated task or VLAN or VXLAN for the selected time range.

If the Baseline Analysis feature is enabled in the traffic analysis task, the traffic trend chart displays the baseline for the average traffic. For more information on configuring the Baseline Analysis feature for the VLAN/VXLAN traffic analysis task, see ["Adding a VLAN/VXLAN traffic analysis task."](#)

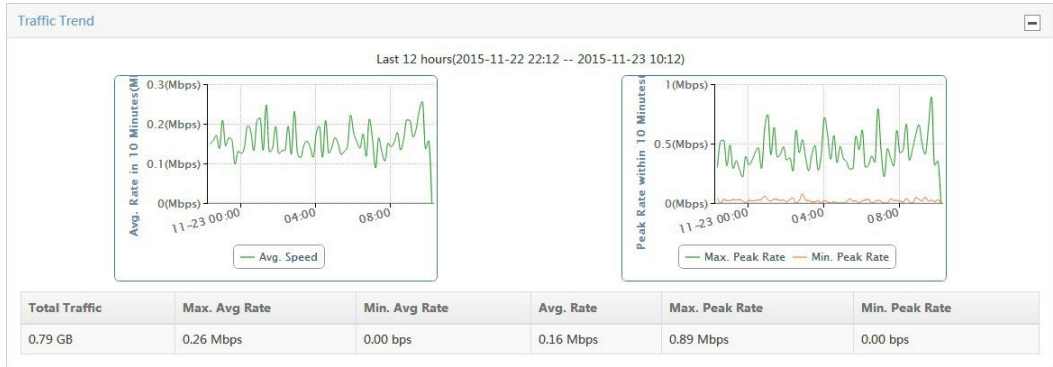
If you enabled the Peak Traffic Analysis feature and selected a time range that is a minimum of six hours earlier than the current time, NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart. For more information on enabling Peak Traffic Analysis, see ["Configuring NTA traffic analysis parameters."](#)

Figure 53 Traffic Trend



The **Peak Rate** line chart displays the minimum and maximum peak traffic rate for inbound or outbound traffic for the associated task during the selected time range.

Figure 54 Peak Rate



To view these charts for an individual VLAN or VXLAN, click a VLAN/VXLAN bar in the **VLAN/VXLAN Traffic Distribution** graph. For more information on the **VLAN/VXLAN Traffic Distribution** report, see "[VLAN/VXLAN Traffic Distribution](#)."

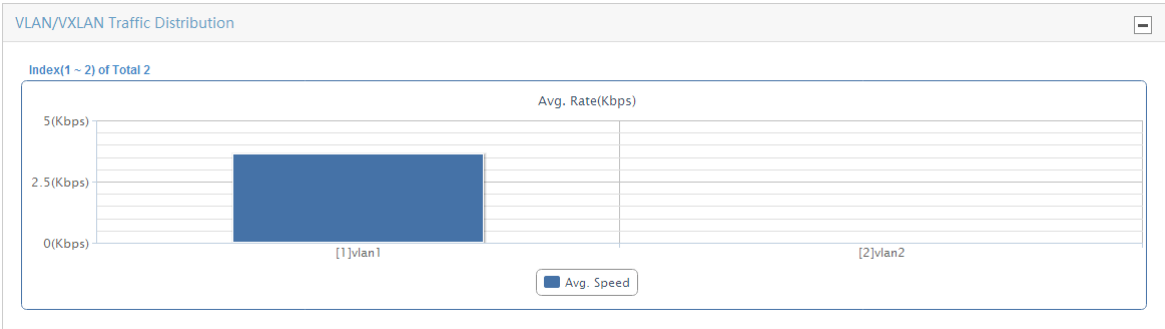
By default, the **Traffic Trend** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** in the upper right corner of the **Traffic Trend** chart.

VLAN/VXLAN Traffic Distribution

If the task you selected has multiple VLANs or VXLANs configured for it, the **VLAN/VXLAN Traffic Distribution** bar chart is displayed. This bar chart displays the average rate of inbound or outbound traffic for every VLAN or VXLAN configured in the task for the selected time range. The bars in the graph link to the reports for the selected VLAN or VXLAN.

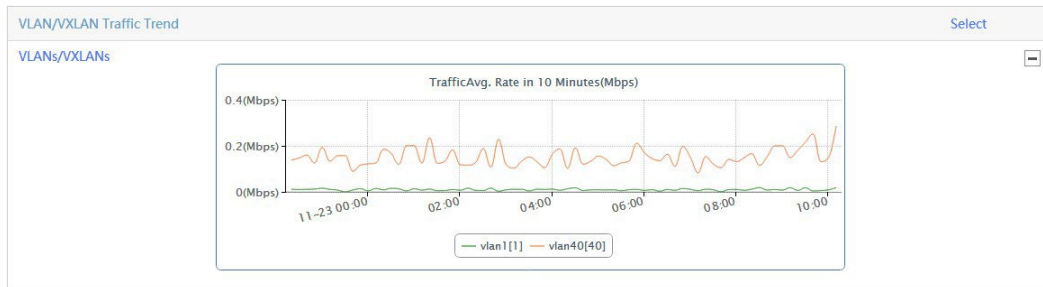
Figure 55 VLAN/VXLAN Traffic Distribution



VLAN/VXLAN Traffic Trend

The **VLAN/VXLAN Traffic Trend** line graph displays the average traffic trend for the selected VLANs or VXLANs.

Figure 56 VLAN/VXLAN Traffic Trend



No data is logged on these line charts until you specify one or more VLANs or VXLANs.

1. To select the VLANs or VXLANs, click **Select** in the upper right corner of the **VLAN/VXLAN Traffic Trend** title bar. The **Select VLANs/VXLANs** dialog box is displayed.
2. Select the check box next to each VLAN or VXLAN you want to view in this report.
3. Click **OK**. The page displays the **VLAN/VXLAN Traffic Trend** reports for the selected VLANs or VXLANs.

Traffic Details

The **Traffic Details** report provides the data collection samples for traffic statistics, based on the time range for the selected traffic analysis task or for a selected VLAN or VXLAN in a task. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic.

Figure 57 Traffic Details

Traffic Details		
Time	Traffic	Rate
2015-11-22 22:20:00	10.70 MB	0.15 Mbps
2015-11-22 22:30:00	11.26 MB	0.16 Mbps
2015-11-22 22:40:00	12.20 MB	0.17 Mbps
2015-11-22 22:50:00	9.86 MB	0.14 Mbps
2015-11-22 23:00:00	14.93 MB	0.21 Mbps
2015-11-22 23:10:00	10.34 MB	0.14 Mbps
2015-11-22 23:20:00	11.75 MB	0.16 Mbps

Application reports

Application reports collect the statistics for all VLANs or VXLANs or an individual VLAN or VXLAN in a traffic analysis task, and analyze traffic of unknown applications. After you click the **Application** tab, application reports are displayed by default.

Application reports contents

- **Query Applications**—Set the time range for the application report.
- **Application List**—Provides a list of applications for all VLANs or VXLANs in the selected traffic analysis task or for a selected VLAN or VXLAN in a task.
- **Application Traffic Trend**—Displays average inbound or outbound traffic rates for all applications for all VLANs or VXLANs in the selected traffic analysis task or for a selected VLAN or VXLAN in a task.
- **Application Traffic Trend for Individual Application**—Provides average rate of traffic for an individual application for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Application Usage List for an Individual Application**—Contains the source host list and the destination host list.

- **Source Host List**—Provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **Destination Host List**—Provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN traffic report for unknown TCP/UDP application by Port**—Displays the distribution of traffic by TCP or UDP port number for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task.
- **TopN Traffic List for Unknown TCP/UDP Application by Port**—Displays a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic observed on all VLANs or VXLANs in the selected traffic analysis task.
- **Unknown Application Traffic Information by Port**—Provides the average rate for an individual unknown application for all VLANs or VXLANs in the selected traffic analysis task.
- **TopN Traffic Details List for Unknown TCP/UDP Applications by Port**—Displays the topN source host and destination host pairs communicating through the current unknown TCP/UDP application port.
- **TopN traffic report for unknown TCP/UDP application by Source**—Provides the distribution of traffic by source for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task.
- **TopN Traffic List for Unknown TCP/UDP Application by Source**—Provides a list of the displays TopN source hosts using unknown TCP/UDP applications on all VLANs or VXLANs in the selected traffic analysis task.
- **Unknown Application Traffic Information by Source**—Provides the average traffic rate for an individual source host using unknown TCP/UDP applications for all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task.
- **TopN Traffic Details List for Unknown TCP/UDP Applications by Source**—Displays the topN destination hosts that communicate with the current source host through unknown TCP/UDP applications.
- **TopN traffic report for unknown TCP/UDP application by Destination**—Displays the distribution of traffic by destination for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task.
- **TopN Traffic List for Unknown TCP/UDP Application by Destination**—Displays topN destination hosts using unknown TCP/UDP applications on all VLANs or VXLANs in the selected traffic analysis task.
- **Unknown Application Traffic Information by Destination**—Displays the average traffic rate for an individual destination host using unknown TCP/UDP applications for all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task.
- **TopN Traffic Details List for Unknown TCP/UDP Applications by Destination**—Displays the topN source hosts that communicate with the current destination host through unknown TCP/UDP applications.

The reports for unknown TCP/UDP applications can be used only when the Unknown Application Traffic Analysis feature is enabled in the system parameter management.

Query applications

To view reports by application, you must configure the filter criteria for application reports. The application query option enables you to change the default settings for query type, application, or time range to customize the reports displayed.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.

2. Select **Application** from the **Query Type** list. The page displays the report for Layer 4 through Layer 7 applications.
3. Specify the following query criterion:

- o **Application**—To select the application you want to search for, click **Select** next to the **Application** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select the applications you want to search for, you must first query the **Application List** as follows:

- a. Specify one or more of the following query criteria in the **Query Applications** area:

- **Application**—In the **Application** field, enter a partial or complete name.
- **Pre-defined**—To search for applications that are predefined, select **Yes** in the **Pre-defined** list. To filter for applications that are user-defined, select **No** in the list. To include system or predefined and user-defined applications, select **Not limited**.

- b. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area. To display the full **Application List**, click **Query** without entering any search criteria.

- c. Click the boxes next to the applications you want to search for.

Click **OK** to add the applications to the filter. The applications you selected are displayed in the **Application** field. Click **Clear**, located next to the **Application** field, to clear all selected applications.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or,

click the **Calendar** icon  next to the input box to manually specify a start time.

- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or,

click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or

Custom. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.

4. Click **OK**.

Application List

The **Application List** displays a list of the applications observed for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the application name, a link for viewing the ports for all unknown applications, total volume of traffic for the associated application, rate of traffic, and the percentage of traffic on all VLANs or VXLANs generated by the associated application. The application name in the **Application** field is a link to reports for the selected application.

Figure 58 Application List

Application List				
Application	Unknown Applications	Traffic	Rate	Percentage
http		17.24 MB	40.17 Kbps	21.75%
snmp		15.54 MB	36.20 Kbps	19.60%
ms-sql-s		10.32 MB	24.06 Kbps	13.03%
rdp		9.42 MB	21.96 Kbps	11.89%
TCP Protocol Unknown Application	12	8.42 MB	19.63 Kbps	10.63%
microsoft-ds		3.97 MB	9.24 Kbps	5.01%
Oracle		3.70 MB	8.62 Kbps	4.67%
UDP Protocol Unknown Application	12	2.18 MB	5.08 Kbps	2.75%
kerberos		1.98 MB	4.62 Kbps	2.50%
netbios-ns		1.91 MB	4.45 Kbps	2.41%
https		1.24 MB	2.88 Kbps	1.56%
dhcpv6-server		1.02 MB	2.38 Kbps	1.29%
SSH		0.77 MB	1.79 Kbps	0.97%
Telnet		0.49 MB	1.13 Kbps	0.61%
ldap		0.47 MB	1.10 Kbps	0.60%
snmptrap		0.41 MB	0.97 Kbps	0.52%
DM		0.18 MB	0.41 Kbps	0.22%

1-17 of 17. Page 1 of 1.

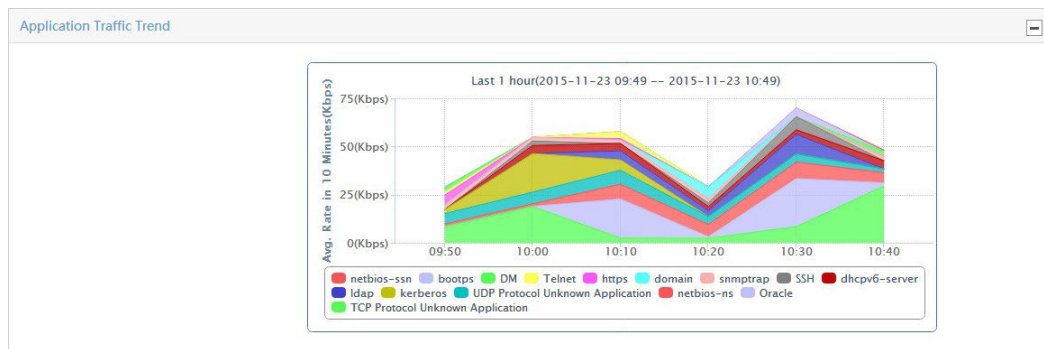
Navigation: << < 1 > >> 50

Select **8**, **15**, **50**, **100**, **200**, or **1000** from the lower right of the main pane to configure how many items per page you want to view.

Application Traffic Trend

The **Application Traffic Trend** stacked area chart displays the average inbound or outbound traffic rates for all applications observed for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. If more than one VLAN or VXLAN exists for the selected task, these statistics reflect traffic for all VLANs or VXLANs configured in a task.

Figure 59 Application Traffic Trend



Application Traffic Trend for an Individual Application

The **Application Traffic Trend** graph displays the average rate of traffic for an individual application for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task, this chart reflects traffic for all VLANs or VXLANs configured in a task.

By default, the **Application Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 60 Application Traffic Trend for an Individual Application



TopN Application Usage List for an Individual Application

The **TopN Application Usage List** displays the source host list and destination host list for an individual application for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.

- **Source Host List** provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source.
- **Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Source Host IP Address** and **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

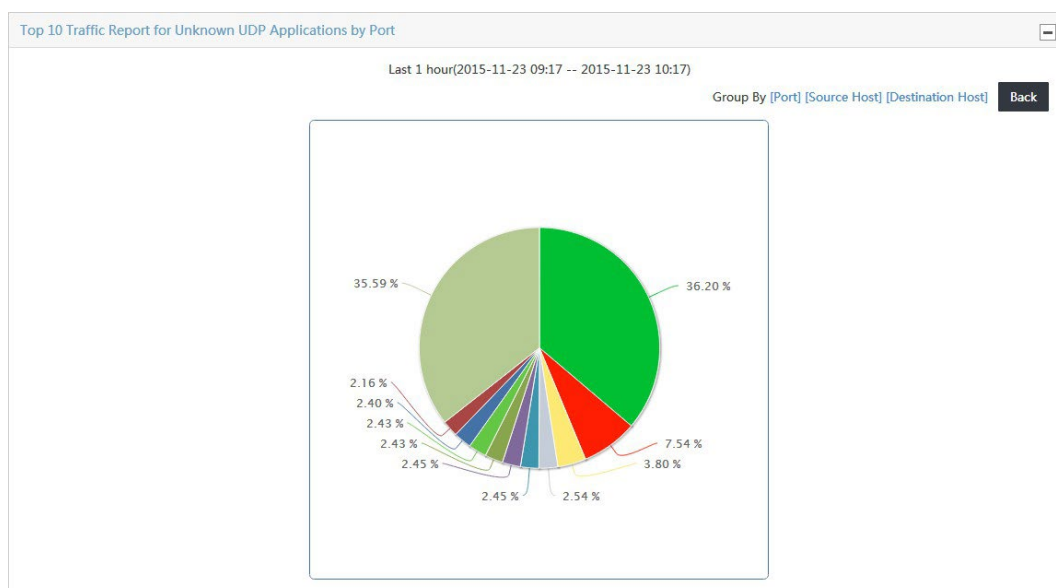
Figure 61 TopN Application Usage List for an Individual Application

Top 10 Application Usage List - http					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 192.168.20.24	6.48 MB	37.60%	 192.168.40.180	5.29 MB	30.67%
 192.168.40.180	3.28 MB	19.00%	 192.168.20.24	3.98 MB	23.09%
 192.168.20.21	3.07 MB	17.80%	 192.168.40.250	3.01 MB	17.44%
 192.168.40.140	1.02 MB	5.92%	 192.168.40.104	1.20 MB	6.94%
 192.168.1.231	0.83 MB	4.81%	 192.168.1.231	1.02 MB	5.92%
 192.168.40.104	0.77 MB	4.48%	 192.168.40.140	0.83 MB	4.81%
 192.168.30.250	0.67 MB	3.89%	 192.168.20.21	0.62 MB	3.59%
 192.168.40.250	0.62 MB	3.59%	 192.168.40.130	0.62 MB	3.57%
 192.168.40.238	0.13 MB	0.77%	 192.168.30.25	0.13 MB	0.77%
 192.168.40.125	0.13 MB	0.73%	 184.50.92.209	0.13 MB	0.73%
Other Hosts	0.24 MB	1.39%	Other Hosts	0.43 MB	2.47%

TopN Traffic Report for Unknown TCP/UDP Application by Port

The **TopN Traffic Report for Unknown TCP/UDP Application by Port** displays the distribution of traffic by TCP or UDP port number, by source host, or by destination host for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task for the selected time range. Click **Port**, **Source Host**, or **Destination Host** to change the data organization. Click **Back** to return to the main **Application** report page.

Figure 62 TopN Traffic Report for Unknown Application by Port



To analyze traffic for unknown TCP/UDP applications, click the icon [?] in the **Unknown Application** field of the **Application List** report for the application for which you want to view this report.

TopN Traffic List for Unknown TCP/UDP Application by Port

The **TopN Traffic List for Unknown TCP/UDP Application by Port** displays a list of the TopN unknown TCP or UDP applications, measured by volume and rate of traffic observed on all VLANs or VXLANs in the selected traffic analysis task for the selected time range. This list includes the TCP or UDP port number, total volume of traffic for the associated application port, rate of traffic, and the percentage of all observed traffic generated for the unknown application. The port number is a link to individual reports for the selected port. The icon [?] in the **Define Application** field is a link to add the selected port to NTA as a Layer 4 application.

Figure 63 TopN Traffic List for Unknown TCP/UDP Application by Port

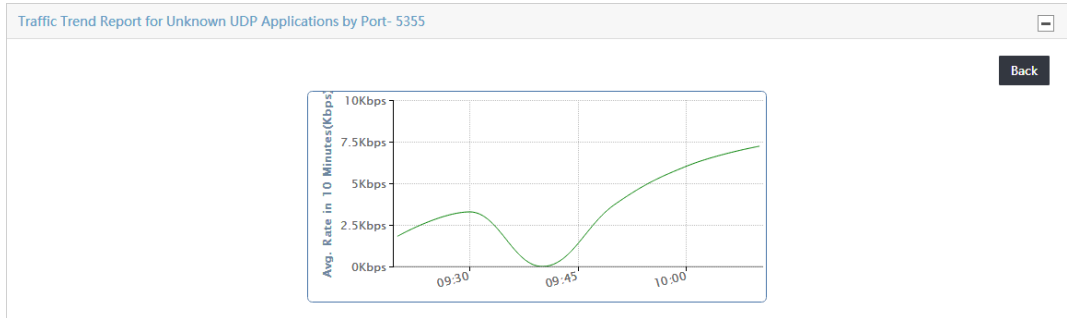
Top 10 Traffic List for Unknown UDP Applications by Port				
Port	Traffic	Rate	Define Application	Percentage
5355	1.58 MB	3.68 Kbps	[?]	36.20%
623	0.33 MB	0.77 Kbps	[?]	7.54%
3389	0.17 MB	0.39 Kbps	[?]	3.80%
55022	0.11 MB	0.26 Kbps	[?]	2.54%
902	0.11 MB	0.25 Kbps	[?]	2.45%
62372	0.11 MB	0.25 Kbps	[?]	2.45%
52747	0.11 MB	0.25 Kbps	[?]	2.43%
52414	0.11 MB	0.25 Kbps	[?]	2.43%
59864	0.10 MB	0.24 Kbps	[?]	2.40%
58258	96.68 KB	0.22 Kbps	[?]	2.16%
Others	1.55 MB	3.62 Kbps		35.59%

Traffic Trend Report for Unknown TCP/UDP Applications by Port

The **Traffic trend report for unknown TCP/UDP applications by Port** displays a line chart of the average rate for an unknown TCP/UDP port for all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task,

this chart reflects traffic for all VLANs or VXLANs configured in a task. Click **Back** to return to the **Unknown Application Traffic Information** page.

Figure 64 Traffic Trend Report for Unknown Applications by Port



To analyze traffic for an individual TCP/UDP application by port, click the **Port** link on the **TopN traffic list for unknown TCP/UDP application** list.

TopN Traffic Details List for Unknown TCP/UDP Applications by Port

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs measured by traffic volume, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source and destination host pair.

Figure 65 TopN Traffic Details for Unknown TCP/UDP Applications by Port

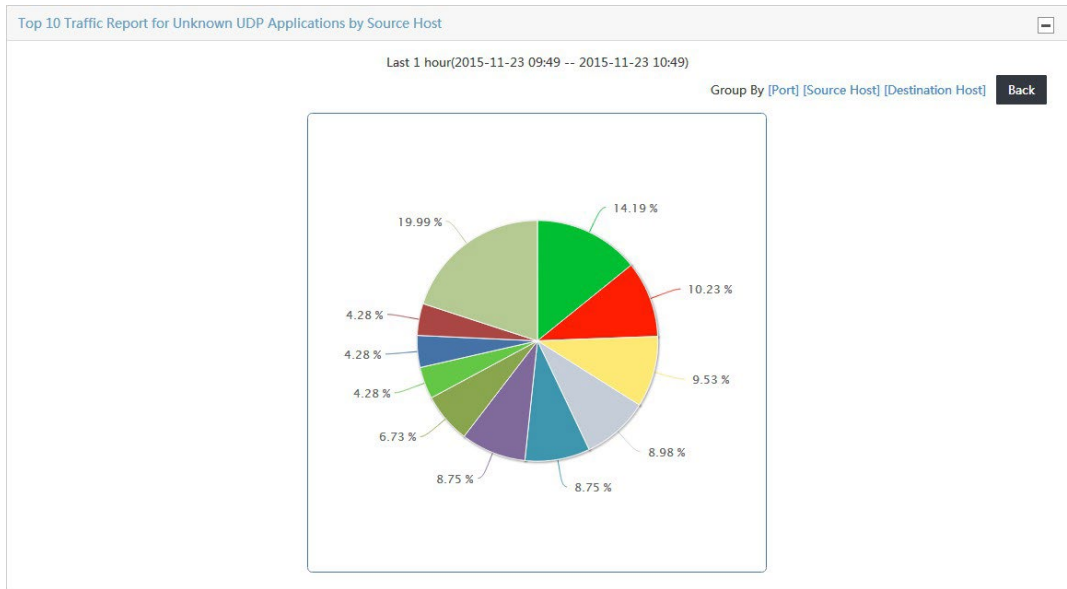
Top 10 Traffic Details List for Unknown UDP Applications by Port - 5355				
Source Host	Destination Host	Traffic	Rate	Percentage
192.168.0.153	224.0.0.252	0.27 MB	0.63 Kbps	17.03%
fe80::d976:7251:7c18:...	ff02::1:3	0.21 MB	0.49 Kbps	13.41%
fe80::9d9d:460f:8201:...	ff02::1:3	0.20 MB	0.46 Kbps	12.62%
fe80::50ca:4f7ef6f5:...	ff02::1:3	0.18 MB	0.42 Kbps	11.47%
fe80::6876:9a74:5c3e:...	ff02::1:3	0.18 MB	0.42 Kbps	11.47%
fe80::5903:4ea9:27e4:...	ff02::1:3	90.82 KB	0.21 Kbps	5.62%
192.168.40.170	224.0.0.252	87.89 KB	0.20 Kbps	5.43%
fe80::244c:6b8f:7484:...	ff02::1:3	85.94 KB	0.20 Kbps	5.31%
192.168.40.180	224.0.0.252	77.15 KB	0.18 Kbps	4.77%
192.168.3.55	224.0.0.252	73.24 KB	0.17 Kbps	4.53%

TopN Traffic Report for Unknown TCP/UDP Application by Source

The **TopN Traffic Report for Unknown TCP/UDP Application by Source** displays the distribution of traffic by source host for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task for the selected time range.

By default, the pie chart is grouped by port. Click the **Source Host** link to group the pie chart by source host. Click **Back** to return to the main **Application** report page.

Figure 66 TopN Traffic Report for Unknown TCP/UDP Application by Source



TopN Traffic List for Unknown TCP/UDP Application by Source

The **TopN Traffic List for Unknown TCP/UDP Application by Source** provides a list of the TopN source hosts using unknown TCP/UDP applications on all VLANs or VXLANs in the selected traffic analysis task for the selected time range. This list includes the source host, total volume of traffic for the associated source host, rate of traffic, and the percentage of all observed traffic generated for the unknown application. The source host is a link to individual reports for the selected source host.

Figure 67 TopN Traffic List for Unknown TCP/UDP Application by Source

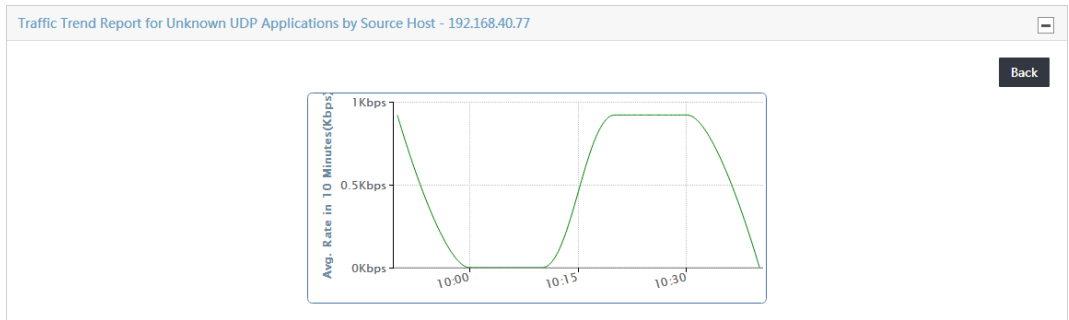
Top 10 Traffic List for Unknown UDP Applications by Source Host

Source Host	Traffic	Rate	Percentage
fe80::50ca:4f7e:f6f5:8875	0.18 MB	0.42 Kbps	21.30%
fe80::b852:50a:a58b:5380	0.17 MB	0.40 Kbps	20.40%
192.168.3.55	0.14 MB	0.33 Kbps	16.82%
fe80::2da4:a3e1:647a:6e7e	90.82 KB	0.21 Kbps	10.43%
192.168.0.154	71.29 KB	0.16 Kbps	8.18%
192.168.0.160	66.41 KB	0.15 Kbps	7.62%
192.168.0.159	66.41 KB	0.15 Kbps	7.62%
192.168.0.133	66.41 KB	0.15 Kbps	7.62%

Traffic Trend Report for Unknown TCP/UDP Applications by Source

The **Traffic trend report for unknown TCP/UDP applications by Source** line chart provides the average rate for an individual source host using unknown TCP/UDP applications for all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task, this chart reflects traffic for all VLANs or VXLANs configured in a task. Click **Back** to return to the **Unknown Application Traffic Information** page.

Figure 68 Traffic Trend Report for Unknown TCP/UDP Applications by Source Host



TopN Traffic Details List for Unknown TCP/UDP Applications by Source

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Source** displays the TopN destination hosts communicating with the current source host through unknown TCP/UDP applications, the port used by the unknown application, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source and destination host pair.

Figure 69 TopN Traffic Details List for Unknown TCP/UDP Applications by Source

Top 10 Traffic Details List for Unknown UDP Applications by Source Host - 192.168.40.77

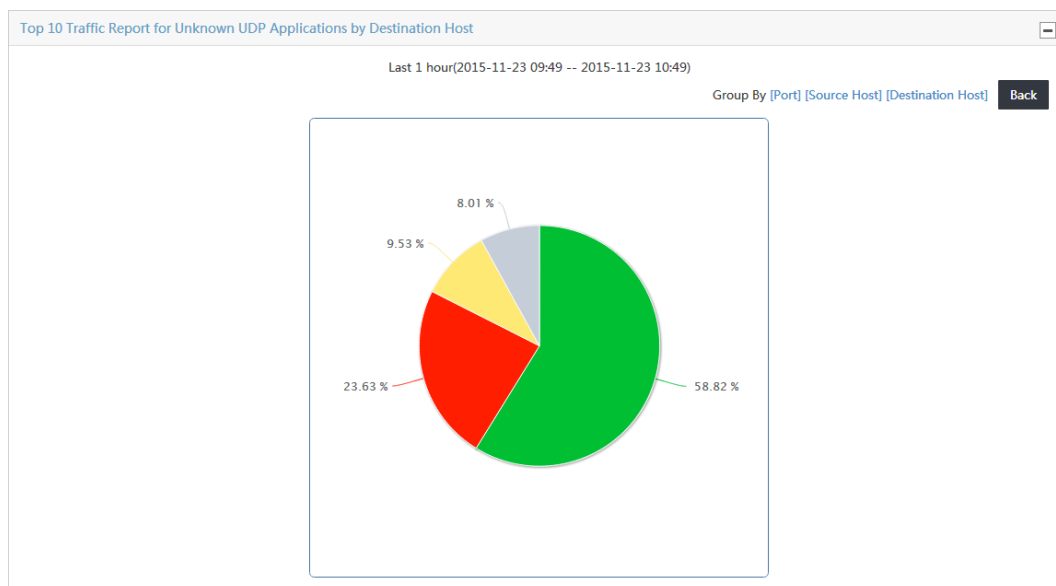
Destination Host	Port	Traffic	Rate	Percentage
172.9.0.151	623	0.20 MB	0.46 Kbps	9.53%
172.9.0.151	49169	67.38 KB	0.15 Kbps	3.18%
172.9.0.151	54192	67.38 KB	0.15 Kbps	3.18%
172.9.0.151	57483	67.38 KB	0.15 Kbps	3.18%

TopN Traffic Report for Unknown TCP/UDP Application by Destination

The **TopN Traffic Report for Unknown TCP/UDP Application by Destination** shows the distribution of traffic by destination host for all application traffic that cannot be attributed to an application for all VLANs or VXLANs in the selected traffic analysis task for the selected time range.

By default, the pie chart is grouped by port. Click the **Destination Host** link to group the pie chart. Click **Back** to return to the main **Application** report page.

Figure 70 TopN Traffic Report for Unknown TCP/UDP Application by Destination



TopN Traffic List for Unknown TCP/UDP Application by Destination

The **TopN Traffic List for Unknown TCP/UDP Application by Destination** provides a list of the TopN hosts using unknown TCP/UDP applications on all VLANs or VXLANs in the selected traffic analysis task for the selected time range. This list includes the destination host, total volume of traffic for the associated destination host, rate of traffic, and the percentage of all observed traffic generated for the unknown application. The source host is a link to individual reports for the selected source host.

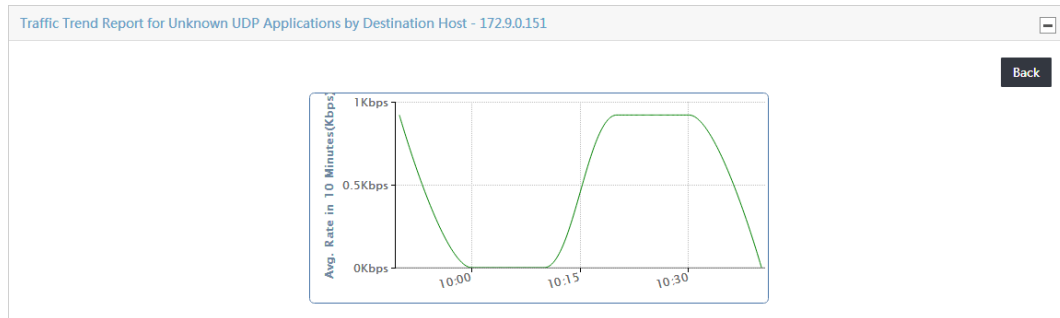
Figure 71 TopN Traffic List for Unknown TCP/UDP Application by Destination

Top 10 Traffic List for Unknown UDP Applications by Destination Host				
Destination Host	Traffic	Rate	Percentage	
ff02::1:3	1.22 MB	2.84 Kbps	58.82%	
224.0.0.252	0.49 MB	1.14 Kbps	23.63%	
172.9.0.151	0.20 MB	0.46 Kbps	9.53%	
192.168.20.24	0.17 MB	0.39 Kbps	8.01%	

TopN Traffic List for Unknown TCP/UDP Application by Destination

The **Traffic trend report for unknown TCP/UDP applications by Destination** line chart provides the average rate for an individual destination host using unknown TCP/UDP applications for all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task, this chart reflects traffic for all VLANs or VXLANs configured in a task. Click **Back** to return to the **Unknown Application Traffic Information** page.

Figure 72 TopN Traffic List for Unknown TCP/UDP Application by Destination Host



TopN Traffic Details List for Unknown TCP/UDP Applications by Destination

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Destination** displays the TopN source hosts communicating with the current destination host through unknown TCP/UDP applications, the ports used by unknown applications, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source and destination host pair.

Figure 73 TopN Traffic Details List for Unknown TCP/UDP Applications by Destination Host

Top 10 Traffic Details List for Unknown UDP Applications by Destination Host - 172.9.0.151				
Source Host	Port	Traffic	Rate	Percentage
192.168.40.77	623	0.20 MB	0.46 Kbps	9.53%
192.168.40.77	49169	67.38 KB	0.15 Kbps	3.18%
192.168.40.77	54192	67.38 KB	0.15 Kbps	3.18%
192.168.40.77	57483	67.38 KB	0.15 Kbps	3.18%

Protocol Reports

Protocol reports provide the rate and percentage distribution of traffic by protocol for all VLANs or VXLANs configured in a VLAN or VXLAN traffic analysis task or for an individual VLAN or VXLAN in a task. Click the **Application** tab to display the default application reports. From the **Query Type** list, select **Protocol** to switch to the protocol reports.

The protocol reports contain the following fields:

- **Query Protocols**—Set the time range for the protocol reports.
- **Protocol List**—Provides a list of protocols observed for all VLANs or VXLANs in the selected traffic analysis task or for a selected VLAN or VXLAN in a task.
- **Protocol Traffic Trend**—Provides average inbound or outbound traffic rates for all protocols observed for all VLANs or VXLANs in the selected traffic analysis task or for a selected VLAN or VXLAN in a task.
- **Protocol Traffic Trend for an Individual Protocol**—Provides average rate of traffic for an individual protocol for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Protocol Usage List for an Individual Protocol**—Includes the source host list and the destination host list.
 - **Source Host List**—Provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
 - **Destination Host List**—Provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.

Query protocols

To view reports by protocol, you must configure the filter criteria for protocol reports. To customize the reports displayed, the protocol query option enables you to change the default settings for query type, protocol, or time range for the graphs and tables.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.

2. Select **Protocol** from the **Query Type** list.

The page refreshes the report for protocols.

3. Click **Select** next to the **Protocol** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the applications you want to search for, you must first query the **Protocol List** as follows:

- a. Specify one or more of the following query criteria in the **Query Protocols** area:
 - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
 - **Pre-defined**—To search for protocols that are predefined, select **Yes** from the **Pre-defined** list. To filter for protocols that are user-defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.
- b. Click **Query**. The query results are displayed in the **Protocol List** below the **Query Protocols** area. To display the full **Protocol List**, click **Query** without entering any search criteria.
- c. Select the check boxes next to the protocols you want to add to the application category.
- d. Click **OK** to add the protocols to the filter. The protocols you selected are displayed in the **Protocol** field. Click **Clear**, located next to the **Protocol** field, to clear all selected protocols.
 - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the protocol report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**,

or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic for protocols.

4. Click **OK**.

Protocol List

The **Protocol List** provides a list of the protocols for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the protocol name, total volume of traffic for the associated protocol, rate of traffic and the percentage of traffic on all VLANs or VXLANs generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.

Figure 74 Protocol List

Protocol List			
Protocol	Traffic	Rate	Percentage
IGMP	0.23 MB	0.53 Kbps	0.02%
IPv6-ICMP	0.27 MB	0.62 Kbps	0.02%
ICMP	2.81 MB	6.54 Kbps	0.23%
UDP	21.47 MB	50.03 Kbps	1.75%
TCP	1.17 GB	2.78 Mbps	97.26%
Other Protocols	8.84 MB	20.59 Kbps	0.72%

1-6 of 6, Page 1 of 1.

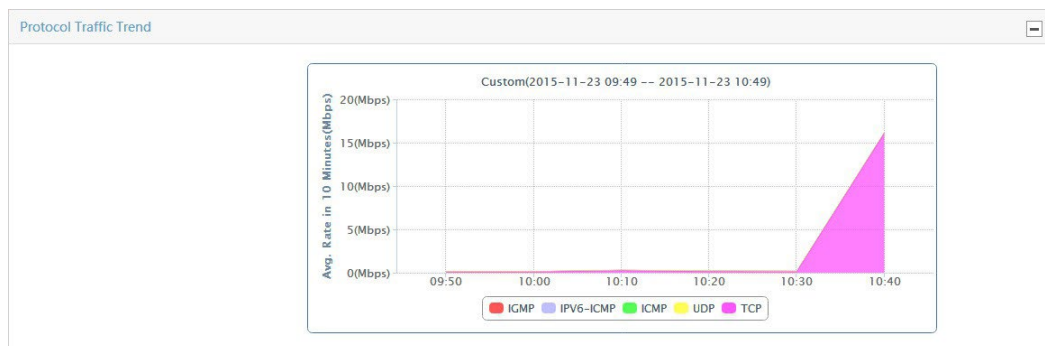
< << 1 >> > 50

Select **8**, **15**, **50**, **100**, **200**, or **1000** from the lower right of the main pane to configure how many items per page you want to view.

Protocol Traffic Trend

The **Protocol Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all protocols observed for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. If more than one VLAN or VXLAN exists for the selected task, these statistics reflect traffic for all VLANs or VXLANs configured in a task.

Figure 75 Protocol Traffic Trend



Protocol Traffic Trend for an Individual Protocol

The **Protocol Traffic Trend** graph provides average rate of traffic for an individual protocol for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task, this chart reflects traffic for all VLANs or VXLANs configured in a task.

By default, the **Protocol Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 76 Protocol Traffic Trend for an Individual Protocol



TopN Protocol Usage List for an Individual Protocol

The **TopN Protocol Usage List** includes the source host list and destination host list for an individual protocol for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.

- **Source Host List** provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source.
- **Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Source Host IP Address** and **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

Figure 77 TopN Protocol Usage List for an Individual Protocol

Top 10 Protocol Usage List - UDP					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 192.168.40.180	1.94 MB	9.05% 	 192.168.40.104	2.83 MB	13.20% 
 10.153.0.61	1.75 MB	8.15% 	 192.168.40.180	2.65 MB	12.33% 
 192.168.30.50	1.52 MB	7.10% 	 192.168.40.170	2.01 MB	9.36% 
 90.16.0.2	0.90 MB	4.20% 	 192.168.40.22	1.75 MB	8.15% 
 192.168.40.104	0.75 MB	3.50% 	 192.168.40.130	1.52 MB	7.06% 
 192.168.40.100	0.71 MB	3.32% 	 192.168.3.255	1.46 MB	6.82% 
 192.168.40.170	0.66 MB	3.06% 	 ff02::1:3	1.22 MB	5.67% 
 192.168.3.139	0.64 MB	2.98% 	 ff02::1:2	1.19 MB	5.53% 
 192.168.40.53	0.64 MB	2.97% 	 192.168.40.53	0.99 MB	4.59% 
 192.168.30.1	0.63 MB	2.95% 	 224.0.0.252	0.49 MB	2.28% 
Other Hosts	11.32 MB	52.72% 	Other Hosts	5.37 MB	25.01% 

Application category reports

Application category reports provide rate and percentage distribution of traffic by application category for all VLANs or VXLANs configured in a VLAN or VXLAN traffic analysis task or for an individual VLAN or VXLAN in a task. Click the **Application** tab to display the application reports by default. Select **Application Category** from the **Query Type** list to switch to the application category reports.

The application category reports contain the following fields:

- **Query Application Categories**—Set the time range for the application category reports.
- **Application Category List**—Provides a list of the application categories observed for all VLANs or VXLANs in the selected traffic analysis task or for a selected VLAN or VXLAN in a task.
- **Application Category Traffic Trend**—Provides average inbound or outbound traffic rates for all applications observed for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a selected task.
- **Application Category Traffic Trend for an Individual Application Category**—Provides the average rate for an individual application category for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Application Category Usage List for an Individual Application Category**—Includes the source host list and the destination host list:
 - **Source Host List**—Provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
 - **Destination Host List**—Provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.

The introduction to application category reports also applies to individual VLAN or VXLAN traffic reports in VLAN/VXLAN traffic analysis tasks.

Query application categories

To view reports by application category, you must configure the filter criteria for application category reports. NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports displayed.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application Category** from the **Query Type** list.
The page displays the report for application categories.
3. Click **Select** next to the **Application Category** field.
The **Query Application Categories** dialog box displays an empty **Application Category List**. To select the applications you want to search for, you must first query the **Application Category List** as follows:
 - a. Specify one or more of the following query criteria in the **Query Application Categories** area:
 - **Application Category**—Enter a partial or complete name for the application categories you want to search for in the **Application Category** field.
 - **Pre-defined**—To search for application categories that are predefined, select **Yes** from the **Pre-defined** list. To filter for application categories that are user-defined, select **No** from the list. To include system or predefined and user-defined application categories, select **Not limited**.
 - b. Click **Query**. The query results are displayed in the **Application Category List** below the **Query Application Categories** area. To display the full **Application Category List**, click **Query** without entering any search criteria.
 - c. Select the check boxes next to the application categories for which you want to search.

- d. Click **OK** to add the application categories to the filter. The application categories you selected are displayed in the **Application Category** field. Click **Clear** next to the **Application Category** field to clear all selected application categories.
 - **Start Time**—Enter the start time of the timer range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the timer range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
- Additionally, to set the start time and end time for the application category report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.

4. Click **OK**.

Application Category List

The **Application Category List** provides a list of the application categories observed for all VLANs or VXLANs in the selected VLAN/VXLAN traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the application category name, total volume of traffic for the associated application category, rate of traffic, and the percentage of traffic on all VLANs or VXLANs generated by the associated application category. The application category name in the **Application Category** field is a link to reports for the selected application category.

Figure 78 Application Category List

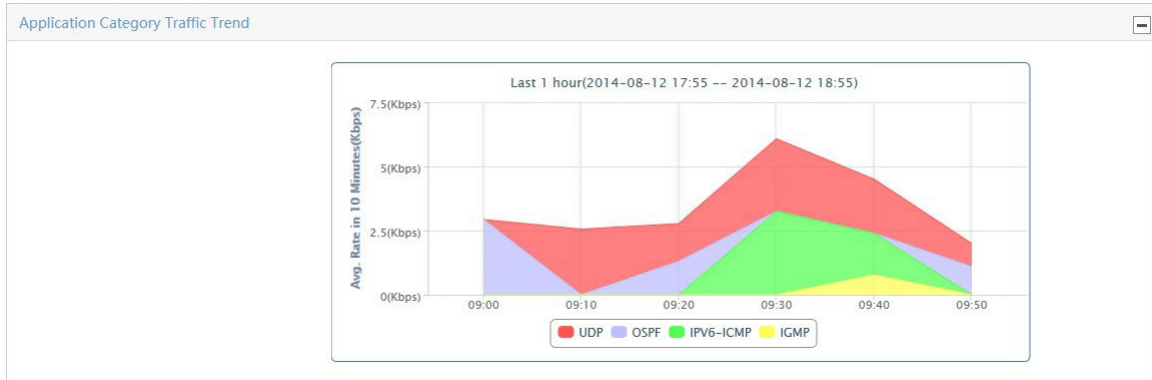
Application Category List			
Application Category ↕	Traffic ↕	Rate ↕	Percentage ↕
Enterprise Application	3.27 MB	7.61 Kbps	0.27% 
Remote Management	8.44 MB	19.68 Kbps	0.69% 
Network Management	14.91 MB	34.75 Kbps	1.21% 
Database Application	16.02 MB	37.32 Kbps	1.30% 
HTTP	18.18 MB	42.36 Kbps	1.48% 
File Service	1.12 GB	2.67 Mbps	93.43% 
Other Application Category	19.93 MB	46.43 Kbps	1.62% 
1-7 of 7, Page 1 of 1.			
« < 1 > » 50			

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

Application Category Traffic Trend

The **Application Category Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all application categories observed for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. If more than one VLAN or VXLAN exists for the selected task, these statistics reflect traffic for all VLANs or VXLANs configured in a task.

Figure 79 Application Category Traffic Trend



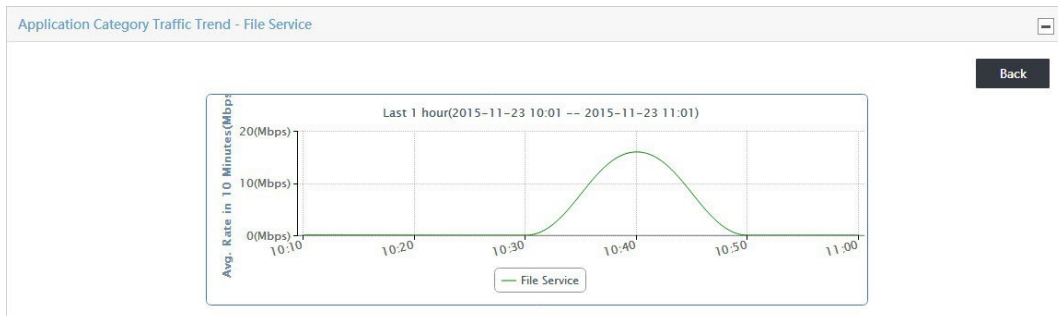
Application Category Traffic Trend for an Individual Application Category

The **Application Category Traffic Trend** graph provides the average rate for an individual application category for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task. If more than one VLAN or VXLAN exists for the selected task, this chart reflects traffic for all VLANs or VXLANs configured in a task.

By default, this graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 80 Application Category Traffic Trend Report for an Individual Application Category



TopN Application Category Usage List for an Individual Application Category

The **TopN Application Category Usage List** includes **Source Host List** and **Destination Host List** for an individual protocol for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.

- **Source Host List** provides a list of the TopN source hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source.
- **Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic observed on all VLANs or VXLANs in the selected traffic analysis task or a VLAN or VXLAN in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Source Host IP Address** and **Destination Host IP Address** is a link for initiating a host query and a link for to the results of the query.

Figure 81 TopN Application Category Usage List

Top 10 Application Category Usage List - File Service					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
192.168.40.110	0.57 GB	50.55%	10.153.3.131	0.56 GB	49.52%
10.153.3.154	0.54 GB	47.82%	192.168.40.110	0.55 GB	48.80%
10.153.3.131	14.41 MB	1.25%	10.153.3.154	12.81 MB	1.12%
192.168.40.25	1.05 MB	0.09%	192.168.40.25	3.15 MB	0.27%
192.168.3.139	0.92 MB	0.08%	192.168.3.255	1.92 MB	0.17%
192.168.40.125	0.28 MB	0.02%	10.153.0.67	0.28 MB	0.02%
192.168.3.55	0.27 MB	0.02%	192.168.40.170	0.25 MB	0.02%
90.16.0.165	0.25 MB	0.02%	192.168.0.211	0.24 MB	0.02%
192.168.1.135	0.19 MB	0.02%	192.168.40.130	0.21 MB	0.02%
99.99.99.2	0.18 MB	0.02%	192.168.40.180	0.19 MB	0.02%
Other Hosts	1.17 MB	0.10%	Other Hosts	0.24 MB	0.02%

Source reports

Source reports provide rate and percentage distribution of traffic by source host for all VLANs or VXLANs configured in a VLAN/VXLAN traffic analysis task or for an individual VLAN or VXLAN in a task. Click the **Source** tab to view traffic reports.

Source reports contain the following fields:

- **Query Sources**—Set the time range for the source host reports.
- **TopN Traffic Report for Source Host**—The pie chart displays the distribution of traffic generated by the TopN source hosts for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Traffic List for Source Host**—Provides a list of the TopN source hosts, measured by volume of traffic on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **Traffic Trend Report for Source Host**—Provides the average rate of traffic for the selected source host.
- **Traffic Details**—Provides two lists for a source host table:
 - **TopN Destination Hosts Communicating with the Source Host**
The list displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and destination hosts, and the percentage of all traffic observed for this source and destination hosts.
 - **TopN Applications Communicating with the Source Host**
The list displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

The introduction to source host reports also applies to individual VLANs or VXLANs in VLAN/VXLAN traffic analysis tasks.

Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.

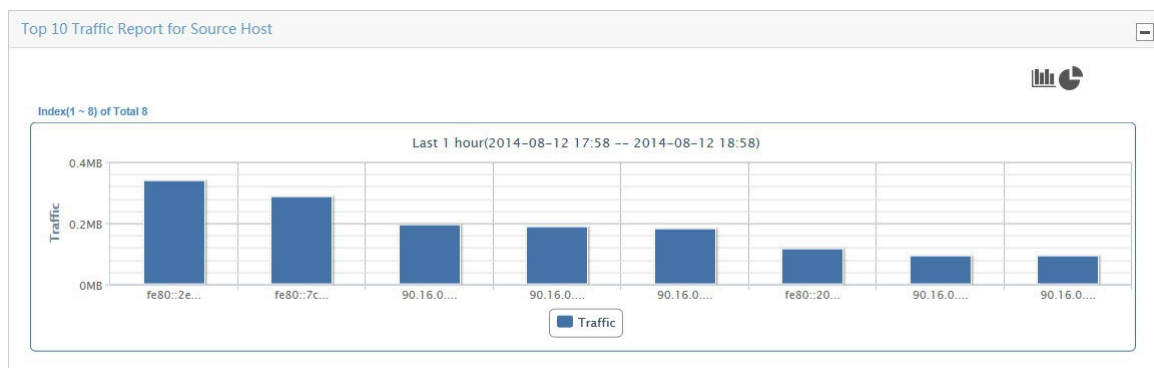
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Enter one or more of the following query criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field.
 Example of a valid IP address:
 10.153.89.10
 Example of a valid network/subnet mask in dotted decimal notation:
 10.153.89.0/255.255.255.0
 Example of a valid network/subnet mask using CIDR notation:
 10.153.89.0/24
 Example of a valid IPv6 address:
 a001:410:0:1::1
 Example of a valid IPv6 address and subnet mask using CIDR notation:
 a001:410:0:1::1/64
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
 The page displays the results of your query.

TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host** bar chart displays the TopN source hosts with the most inbound/outbound traffic for all VLANs or VXLANs in a certain period of time in a selected VLAN/VXLAN traffic analysis task. Click a bar in the chart to view the traffic analysis report of each source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound or outbound traffic of the TopN source hosts for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. The slices of the pie chart are links to traffic reports for the selected host.

Figure 82 TopN Traffic Report for Source Host



TopN Traffic List for Source Host

The **TopN Traffic List for Source Host** provides a list of the TopN source hosts measured by volume of inbound or outbound traffic observed on all VLANs or VXLANs in the selected traffic

analysis task or for a VLAN or VXLAN in a task for the selected time range. This list includes the source IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The IP address is a link to reports for the selected source.

The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the query.

Figure 83 TopN Traffic List for Source Host

Top 10 Traffic List for Source Host			Generate Chart
Source	Traffic	Percentage	
 192.168.3.139	0.55 MB	13.55%	
 192.168.0.133	0.37 MB	9.22%	
 192.168.3.55	0.37 MB	9.03%	
 192.168.0.153	0.36 MB	8.84%	
 fe80::2da4:a3e1:647a:6e7e	0.35 MB	8.66%	
 fe80::b852:50aa:58b:5380	0.35 MB	8.56%	
 192.168.0.99	0.27 MB	6.77%	
 192.168.0.157	0.22 MB	5.46%	
 192.168.0.158	0.21 MB	5.22%	
 fe80::50ca:4f7e:f6f5:8875	0.18 MB	4.47%	
Other Hosts	0.82 MB	20.21%	

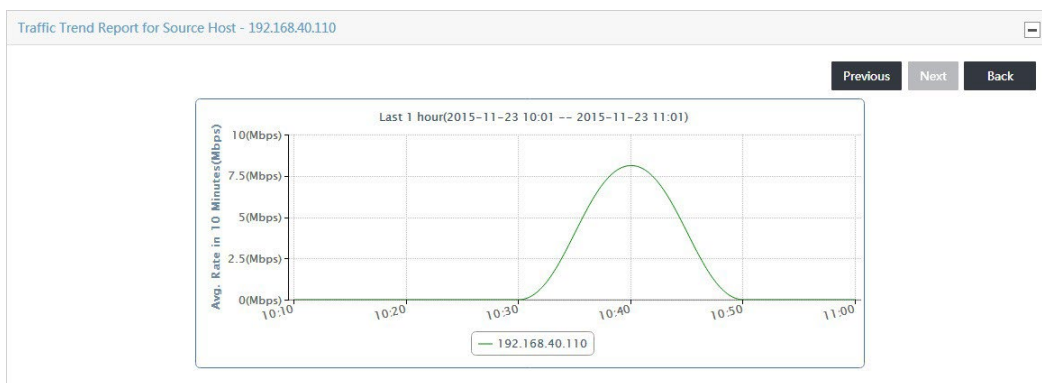
Traffic Trend Report for Source Host

The **Traffic Trend Report for Source Host** line chart provides the average rate of traffic for the selected source host. To view this line chart, click the slices of the **TopN Traffic Report for Source Host** pie chart or click the IP address of the **TopN Traffic List for Source Host**.

By default, the **Traffic Trend Report for Source Host** chart displays statistics for the last 1 hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 84 Traffic Trend Report by Source Host



Traffic Details for Source Host

The **Traffic Details For Source Host** table provides two lists:

- The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and destination hosts, and the percentage of all traffic observed for this source and destination hosts.
- The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

Figure 85 Traffic Details For Source Host

Traffic Details					
Top 10 Destination Hosts Communicating with the Source Host			Top 10 Applications Communicating with the Source Host		
Destination	Traffic	Percentage	Application Name	Traffic	Percentage
10.153.3.131	0.56 GB	97.85%	microsoft-ds	0.57 GB	99.88%
10.153.3.154	11.76 MB	2.02%	rdp	0.48 MB	0.08%
192.168.30.25	0.48 MB	0.08%	TCP Protocol Unknown Application	0.13 MB	0.02%
192.168.1.136	0.20 MB	0.03%	Unknown Protocol Application	68.36 KB	0.01%
192.168.40.130	68.36 KB	0.01%			

Destination reports

Destination reports provide rate and percentage distribution of traffic by destination host for all VLANs or VXLANs configured in a VLAN/VXLAN traffic analysis task or for an individual VLAN or VXLAN in a task. Click the **Destination** tab to view traffic reports.

Destination reports contain the following fields:

- **Query Destinations**—Set the time range for the destination host reports.
- **TopN Traffic Report for Destination Host**—Displays the distribution of traffic generated by the TopN destination hosts for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Traffic List for Source Host**—Provides a list of the TopN destination hosts measured by volume of traffic on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **Traffic Trend Report for Destination Host**—Provides the average rate of traffic for the selected destination host.
- **Traffic Details**—For a source host table, provides two lists:
 - **TopN Source Hosts Communicating with the Destination Host**
The list displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.
 - **TopN Applications Communicating with the Destination Host**
The list displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

The introduction to destination host reports also applies to individual VLANs or VXLANs in VLAN/VXLAN traffic analysis tasks.

Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Enter one or more of the following query criteria:
 - **Destination Host**—Enter the IP address or address range in the **Destination Host** field.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

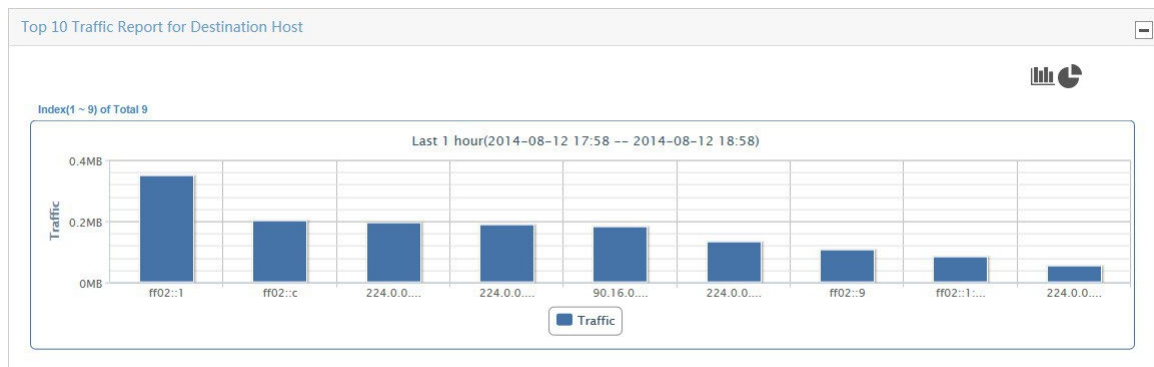
4. Click **OK**.

The page displays the results of your query.

TopN Traffic Report for Destination Host

The **TopN Traffic Report for Destination Host** pie chart displays the distribution of inbound or outbound traffic for TopN destination hosts for all VLANs or VXLANs in the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the selected destination host.

Figure 86 TopN Traffic Report for Destination Host



TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host** provides a list of the TopN destination hosts measured by volume of inbound or outbound traffic observed on all VLANs or VXLANs in the selected traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic generated by the associated destination, and the percentage of all observed traffic generated by the destination. The IP address is a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a destination host query and a link to the results of the query.

Figure 87 TopN Traffic List for Destination Host

Top 10 Traffic List for Destination Host			Generate Chart
Destination	Traffic	Percentage	
192.168.3.255	1.37 MB	32.58%	
ff02::1:3	1.04 MB	24.71%	
224.0.0.22	0.43 MB	10.23%	
ff02::1:2	0.30 MB	7.17%	
192.168.0.255	0.27 MB	6.52%	
192.168.0.211	0.26 MB	6.24%	
224.0.0.252	0.26 MB	6.15%	
ff02::1:6	0.18 MB	4.25%	
224.0.0.5	80.08 KB	1.86%	
192.168.1.239	76.17 KB	1.76%	

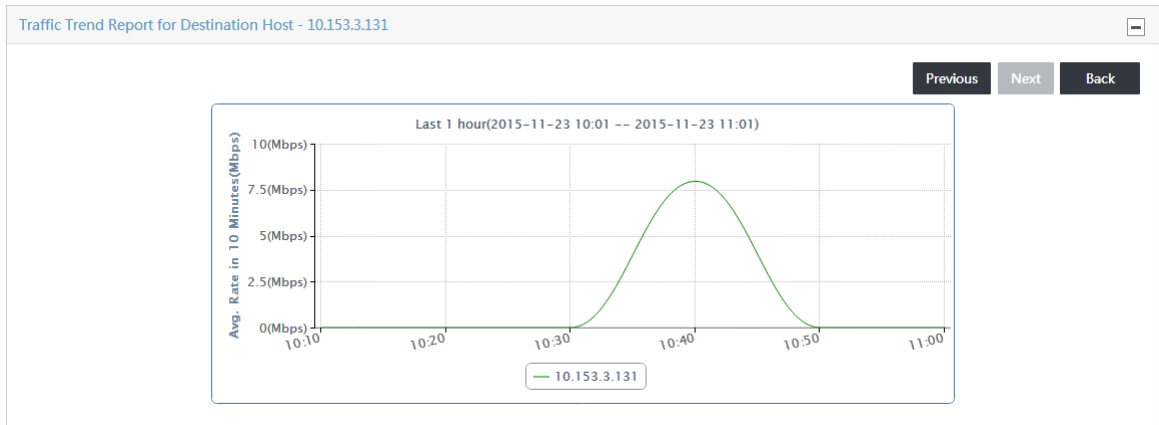
Traffic Trend Report for Destination Host

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. To view this line chart, click the slices of the **TopN Traffic Report for Destination Host** pie chart or click the IP address of the **TopN Traffic List for Destination Host**.

By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the last 1 hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 88 Traffic Trend Report for Destination Host



Traffic Details for Destination Host

The **Traffic Details For Destination Host** table provides the following lists:

- The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.
- The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

Figure 89 Traffic Details for Destination Host

Traffic Details					
Top 10 Source Hosts Communicating with the Destination Host			Top 10 Applications Communicating with the Destination Host		
Source	Traffic	Percentage	Application Name	Traffic	Percentage
 192.168.40.110	0.56 GB	100.00% 	microsoft-ds	0.56 GB	100.00% 

Session reports

A session is a unique source and destination host pair. Session reports provide rate and percentage distribution of traffic for source and destination pairs for all VLANs or VXLANs configured in a VLAN/VXLAN traffic analysis task or for an individual VLAN or VXLAN in a task. Click the **Session** tab to view traffic reports.

Session reports contain the follow fields:

- **Query Sessions**—Set the time range for the session host reports.
- **TopN Traffic Report for Session Host**—Displays the distribution of the traffic generated by the TopN session hosts for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **TopN Traffic List for Session Host**—Provides a list of the TopN session hosts measured by volume of traffic on all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task.
- **Session Host Traffic Trend Report**—Provides the average rate of traffic for the source and destination host pair.
- **TopN Applications for Session Host**—Displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

The introduction to session host reports also applies to individual VLANs or VXLANs in VLAN/VXLAN traffic analysis tasks.

Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the session report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field.
 Example of a valid IP address:
 10.153.89.10
 Example of a valid network or subnet mask in dotted decimal notation:
 10.153.89.0/255.255.255.0
 Example of a valid network or subnet mask using CIDR notation:
 10.153.89.0/24
 Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- o **Destination Host**—Enter the IP address or address range in the **Destination Host** field.
- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

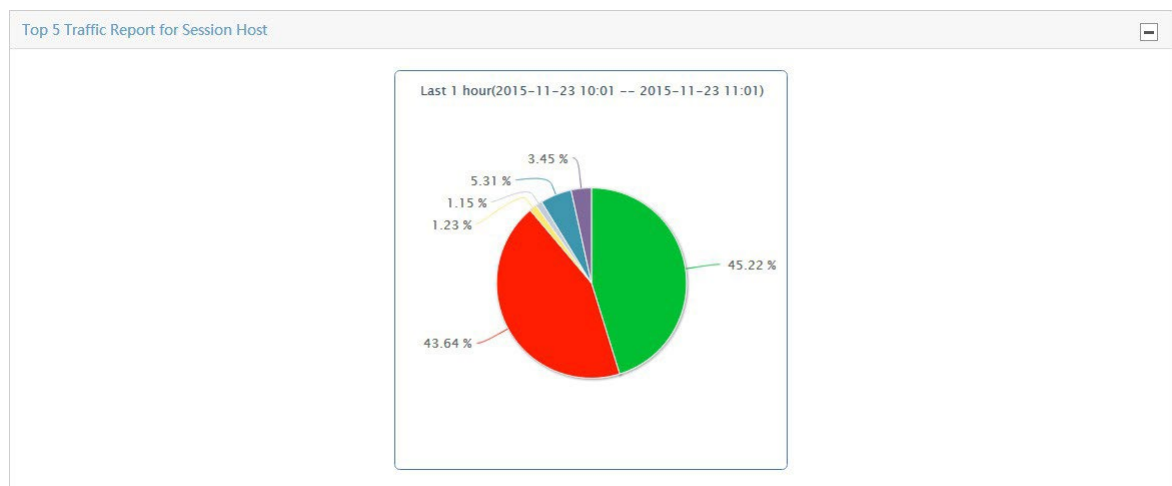
4. Click **OK**.

The page displays the results of your query.

TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host** pie chart displays the distribution of inbound or outbound traffic for TopN source and destination session pairs for all VLANs or VXLANs in the selected traffic analysis task or for a VLAN or VXLAN in a task for the selected time range. Each pie chart slice is a link to traffic reports for the selected source and destination session pair.

Figure 90 TopN Traffic Report for Session Host



TopN Traffic List for Session Host

The **TopN Traffic List for Session Host** provides a list of the TopN session source and destination pairs measured by volume of inbound or outbound traffic observed on all VLANs or VXLANs in the selected traffic analysis task for the selected time range. This list includes the source and destination IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair. The

icon  in the **Details** field is a link to reports for the selected session or source and destination pair.

The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link to the results of the query.

Figure 91 TopN Traffic List for Session Host

Top 10 Traffic List for Session Host				Generate Chart	
Source Host	Destination Host	Traffic	Percentage	Details	Topology
192.168.40.110	10.153.3.131	0.56 GB	45.22%		
10.153.3.154	192.168.40.110	0.54 GB	43.64%		
192.168.40.22	192.168.30.25	15.51 MB	1.23%		
10.153.3.131	192.168.40.110	14.46 MB	1.15%		
192.168.40.110	10.153.3.154	11.76 MB	0.94%		
172.4.8.88	192.168.40.150	9.68 MB	0.77%		
192.168.20.24	192.168.40.104	6.53 MB	0.52%		
192.168.40.25	192.168.30.250	5.57 MB	0.44%		
192.168.40.150	172.4.8.88	5.23 MB	0.42%		
192.168.40.104	192.168.20.24	4.58 MB	0.36%		
Other Hosts	Other Hosts	66.76 MB	5.31%		

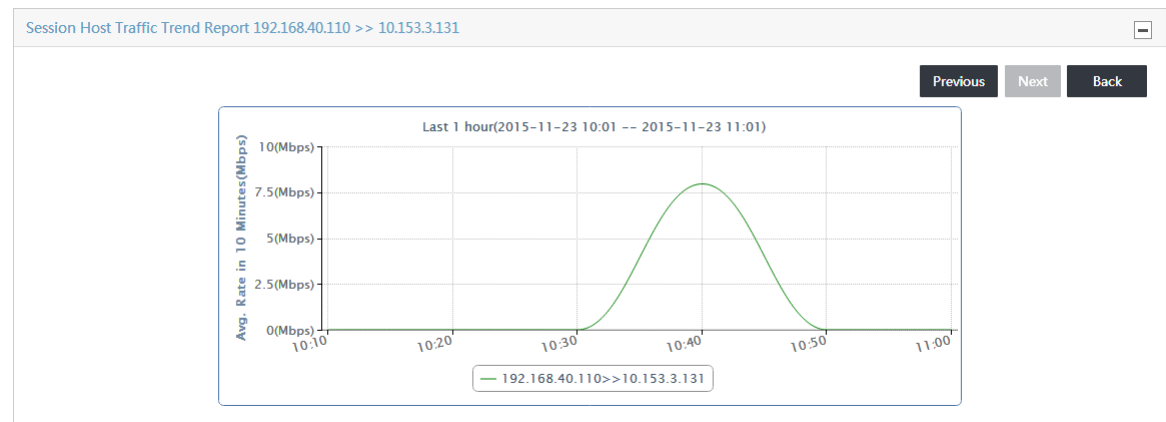
Session Host Traffic Trend Report

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. To view this line chart, click the slices of the **TopN Traffic Report for Destination Host** pie chart or click the icon in the **Details** field of the **TopN Traffic List for Destination Host**.

By default, the **Session Host Traffic Trend Report** chart displays statistics for the last 1 hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 92 Session Host Traffic Trend Report



TopN Applications for Session Host

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

Figure 93 TopN Applications for Session Host

Top 10 Applications for Session Host 192.168.40.110 >> 10.153.3.131		
Application Category	Traffic	Percentage
microsoft-ds	0.56 GB	100.00% 

Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source and destination hosts.

Probe monitoring

This chapter provides information on network flow data reporting using data gathered by probe servers, also called probes. This chapter explains how NTA analyzes network flow records from probes to report on network traffic and looks at the reporting options for probe traffic analysis. This chapter also provides a survey of the summary reports for all probe tasks a look at the more detailed reports for an individual probe traffic analysis task.

Probe traffic monitoring overview

In NTA, a probe is a probe server. A probe server is an application that runs on a dedicated server. A probe server acts as a network flow generator that transmits network flow data to the NTA server that acts as a flow collector. Probe servers receive information forwarded to it from network devices. NTA retrieves data from probe servers when the probe server is added to the NTA server as a probe. Operators use probe servers when the devices in their network cannot generate NetStream, NetFlow, or sFlow data.

After you add a probe server to an NTA server as a probe, and the probe is selected in the NTA **Server Management** page, the NTA server is ready to begin processing data from the probe. Probe traffic analysis tasks instruct NTA to begin processing probe server data based on the task configuration.

Probe traffic analysis tasks analyze network flow data by the probes you specify in probe traffic analysis tasks. NTA parses all network flow data and provide various statistical views of traffic that was received by the probes configured in a probe traffic analysis task. For example, NTA provides source and destination host information reporting by probe, displaying traffic attributed to specific source or destination hosts that were observed sending or receiving traffic from the locations on the network where probes were deployed.

In general, the NTA probe traffic analysis tasks provide traffic visibility for the locations on the network where probes have been deployed. The probe reports include traffic for all probes in all tasks, for all probes in each task, and for individual probes in a task. Probe statistics include traffic statistics and statistics by application, source host, destination host, and a session or source/destination host pair. These reports are organized into multiple layers from summarized information for all tasks to detailed reporting for specific probes configured for an individual probe traffic analysis task.

Probe traffic analysis reporting overview

After you create the first probe traffic analysis task, NTA creates a  **Probe Traffic Analysis Task** entry under the **Traffic Analysis and Audit** area on the left navigation tree.

Click **Probe Traffic Analysis Task** on the left navigation tree to view the summary report for all probe traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon >>> next to  **Probe Traffic Analysis Task**. The **Probe Traffic Analysis Task** shortcut menu displays all probe traffic analysis tasks created in NTA. Click the name of a task to view the probe traffic analysis report of the task.

The summary probe traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides summarized average rate per second reporting for all probe traffic analysis tasks summarized by task. Each bar in the graph a link to more detailed reporting for the selected task including reporting for traffic rates, application, source, destination, and session statistics. Each of these detailed report types also include several reports for the selected task including:

- **Traffic**—Reports include traffic trends that display the average rate within 1 minute and the individual data samples for the selected task.
- **Application**—Reports include a table that displays the percentage of application traffic generated by the probe in a task, and a graph that displays the average rate of application traffic for the probe in the task.
- **Source**—Reports include a pie chart the TopN source hosts and a list displaying the TopN source hosts in the selected task. The contents of the chart link to more detailed reporting for the selected host.
- **Destination**—Reports include a pie chart the TopN destination hosts and a list displaying the TopN destination hosts for the selected task. The contents of the chart link to more detailed reporting for the selected host.
- **Session**—Reports include a chart the TopN source and destination pairs and a list displaying the TopN sessions for the selected task. The contents of the chart link to more detailed reporting for the selected host.
- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—This set of line charts provides traffic summarized by probe traffic analysis task for traffic for all probes for all tasks. A second set of pie charts reveals the distribution of traffic for the TopN applications.
- **Summary List (Last 1 Hour)**—Provides traffic statistics summarized by probe traffic analysis task for all tasks.

Probe traffic analysis configuration considerations

Consider the following when adding a probe to a task:

- By default, NTA does not report on any data received by probes. Therefore, you must create a task for every probe or group of probes that you want to monitor and report on.
- You can add only one probe a single task. However, a probe can only belong to one task.
- Add only those probes whose statistics you want to view. Do not add all probes unless you want to view reporting for all probes
- When you add probes to a task, NTA displays a list of all probes that NTA knows about. This list is generated from the probes that have been added to NTA using the Probe Management feature. If the probes you want to add are not displayed on this list, and if they are not already included in another traffic analysis task, it is most likely because the probe has not been added to NTA or it has not been selected in the NTA server configuration found under Server Management. For more information on selecting probes in NTA server management, see ["Modifying an NTA server configuration."](#)
- If you do not add a probe to a task, NTA does not report on the task.

Managing probe traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA does not analyze the data that probes forward to it or that it is configured to receive. This section describes the process for adding, modifying, or removing probe traffic analysis tasks in NTA.

Viewing a traffic analysis task

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view the traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.

2. Click the **Traffic Analysis Task Management** link. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

Task list contents

- **Task Name**—Name of the task.
The contents of this field link to the **Task Details** page for the associated task.
 - **Task Description**—Description for the associated task.
 - **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **Baseline Analysis**—Displays when the Baseline Analysis feature is enabled in the NAT parameters.
The Baseline Analysis feature provides an additional layer of analysis to NTA reports by including baseline trend data when data has been collected for a minimum of one week
 - **Modify**—Contains an icon  for modifying the associated task.
 - **Delete**—Contains an icon  for deleting the associated task.
3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** located in the upper left corner of the **Traffic Analysis Task List**.
You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing probe traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. To view the details for a probe traffic analysis task, click the task name of a **Traffic Analysis Task List** with a **Task Type** of **Probe**.

Traffic analysis task details

- **Task Name**—Contains the name of the task.
- **Task Description**—Contains the description for the associated task.
- **Server**—Contains the name or IP address of the NTA server.
- **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**

- **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by the associated traffic analysis task.
 - **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
 - **Enable Automatic Anomaly Detection Based On The Baseline**—Indicates whether automatic detection of traffic anomaly based on the baseline is enabled for the task. This parameter is displayed only when baseline analysis is enabled.
 - **Baseline Threshold Setting**—Displays the baseline threshold settings. This area is displayed only when baseline analysis is enabled. The baseline threshold setting includes the following parameters:
 - **Baseline Upper/Lower Threshold**—Indicates the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Indicates under what condition the threshold is triggered. This condition has two configuration parameters, the time interval, and the number of times that the threshold must be met.
 - **Threshold**—Indicates the percentage threshold that must be met before NTA generates an alarm.
 - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
 - **Probe Information**—Lists the name, IP address, and description for the probe providing traffic for this traffic analysis task.
4. Click **Back** to return to the **Traffic Analysis Task List**.

Adding a probe traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.
The **Add Traffic Analysis Task** page is displayed.
4. To add a probe traffic analysis task, click the option next to **Probe** in the **Select Task Type** area.
5. Click **Next**.
The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field. The task name must be unique.
The name you assign to a task is the link to the task reports. Therefore, assign descriptive and meaningful names to a task that help you navigate to reports quickly and easily.
7. Enter a description for this task in the **Task Description** field.
8. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.

Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.

9. To select the operator groups that have access to the analysis and reports provided by this probe task, click **Select** next to the **Reader** field.
The **Operator Group List** dialog box is displayed.
10. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
11. To accept the operator group selection, click **OK**.
The selected operator groups are displayed in the **Reader** field.
12. To enable the Baseline Analysis feature for the reports generated by this task, select **Enable** from the **Baseline Analysis** list.
If you select **Enable**, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.
To disable the Baseline Analysis feature, select **Disable**.
If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
13. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.
NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.
14. Configure the baseline threshold settings.
 - o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - o **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
 - o **Threshold**—Specify the percentage threshold that must be met before NTA generates an alarm.
 - o **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - o **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
15. To select the probe that provides network flow data, select the option in the **Select** field next to the probe name you want to add in the **Probe Information** list.
16. To create the probe traffic analysis task, click **OK**.

After you create a probe traffic analysis task, NTA creates a  **Probe Traffic Analysis Task** entry on the left navigation tree. Click the entry to view the summary report for the probe traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon >>> next to  **Probe Traffic Analysis Task**. The **Probe Traffic Analysis Task** shortcut menu displays all probe traffic analysis tasks created in NTA. Click the name of a task to view the probe traffic analysis report of the task.

For more information on accessing and viewing probe traffic analysis reports, see "[Viewing probe traffic analysis reports](#)."

Modifying a probe traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  associated with the probe traffic analysis task you want to modify.
The **Modify Traffic Analysis Task** page is displayed.
4. Modify the name for this task in the **Task Name** field.
The task name must be unique.
5. Modify the description for this task in the **Task Description** field.
6. From the **Server** list, select the NTA NetStream, NetFlow, or sFlow collection server.
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add new operator groups that have access to the analysis and reports provided by this probe task, click **Select** next to the **Reader** field.
The **Operator Group List** dialog box is displayed.
8. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box in the upper right corner of the column label field for all boxes.
9. To accept the new additions to operator group, click **OK**.
The operator groups you selected are displayed in the **Reader** field.
10. To revoke operator group access to the results of this probe traffic analysis task, highlight the groups you want to remove in the **Reader** field.
11. Click **Delete**.
12. To confirm the deletion of the selected operator groups from the task, click **OK**.
The **Reader** list is updated to reflect the deleted operator group changes.
13. To enable the Baseline Analysis feature for the reports generated by this task, select **Enable** from the **Baseline Analysis** list.
If you select **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.
To disable the Baseline Analysis feature, select **Disable**.
If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.

14. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.
NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.
15. Configure the baseline threshold settings.
 - **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
 - **Threshold**—Specify the percentage threshold that must be met before NTA generates an alarm.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
16. To change the probe that you want to use for this task, select the option in the **Select** field next to the probe name you want to add in the **Probe Information** list.
17. To accept your modifications the probe traffic analysis task, click **OK**.

Deleting a probe traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  associated with the probe traffic analysis task you want to delete.
4. To confirm the deletion of the selected probe traffic analysis task, click **OK**.
The **Traffic Analysis Task List** is updated to reflect the removal of the deleted task.

Viewing probe traffic analysis reports

NTA provides various levels of reporting for all traffic analysis tasks. The highest level provides summarized reporting for all tasks of the same type whether the task type is interface, VLAN/VXLAN, application, probe, host, VPN, interbusiness or BGP AS. These reports are accessed by clicking the highest level entry of the left navigation tree under the **Traffic Analysis and Audit** area. To view summarized reporting for all probe tasks, click the  **Probe Traffic Analysis Task** entry of the left navigation tree.

NTA also provides detailed reporting for individual tasks. NTA groups individual tasks by type. All probe tasks can be found on the **Probe Traffic Analysis Task** menu.

To view the **Probe Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon >>> next to  **Probe Traffic Analysis Task**. The shortcut menu displays all probe traffic analysis tasks created in NTA. Click the name of a task to view the probe traffic analysis report of the task.

This section describes the reporting options available for probe traffic analysis tasks. It also describes the process for navigating to probe traffic analysis tasks, the summary reports available for probe tasks, and the reports and features available for a probe traffic analysis task.

Navigating to the probe traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. To view summary reporting for all probe tasks, click the  **Probe Traffic Analysis Task** entry in the **Traffic Analysis and Audit** area of the left navigation tree.
3. To view summary reporting for an individual task, move your mouse pointer to the shortcut menu icon >>> next to  **Probe Traffic Analysis Task**.

The **Probe Traffic Analysis Task** shortcut menu displays all probe traffic analysis tasks created in NTA. Click the name of a task to view the probe traffic analysis report of an individual task.

Summary reports for all probe tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **Probe Traffic Analysis Task** entry of the left navigation tree under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

average rate (last 1 hour)

The **Average Rate** bar graph summarizes the average rate of traffic for all probe tasks. You can access this graph by clicking the  **Probe Traffic Analysis Task** entry on the left navigation tree. The bars in the graph link to the reports for the selected probe task.

Figure 94 Average Rate (Last 1 Hour)



Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

You can access this graph by clicking the  **Probe Traffic Analysis Task** entry of the left navigation tree.

The **Traffic Trend for Selected Task** line chart displays the average traffic rate per second for the selected probe task. The **TopN Application for Selected Task** pie chart displays the distribution of traffic for the selected probe task. These charts are located in the middle of the page.

Figure 95 TopN Application by Selected Task



By default, this chart contains no data. To populate this chart with data, you must first select a probe task.

1. To select a task, click the **Select Task** link located in the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar.
2. The **Choose NTA Task** dialog box is displayed. Click the box next to the probe task whose report you want to view.
3. Click **OK**.

The page displays the **Traffic Trend and TopN Application for Selected Task** reports for the selected task.

Summary List (Last 1 Hour)

The **Summary List** provides the total volume of traffic and traffic rates summarized by probe task for the last hour.

Summary list contents

- **Task Name**—Name of the probe traffic analysis task.
The contents of this field link to reports for the associated tasks.
- **Traffic**—Total volume of traffic in the last hour for the associated probe.
- **Rate**—Rate of traffic in the last hour for the associated probe.
- **Traffic Log Audit**—Click the **Traffic Log Audit** icon  to access the **Traffic Log Audit** page.
For more information on the traffic log auditing feature, see "[Performing traffic log audits in NTA.](#)"
The **Add** button at the top of the **Summary List** is a shortcut to the **Add Probe Traffic Analysis Task** page.
For more information on adding probe traffic analysis tasks, see "[Adding a probe traffic analysis task.](#)"
Click **Refresh** to update the reports with the most recent data.

Detailed reports for a probe traffic analysis task

NTA provides a suite of reports for viewing more detailed probe data from different perspectives. Detailed reports for probes are organized into the following reporting groups:

- **Traffic reports**—Provide overall traffic statistics for the selected time range for probe tasks.
- **Application reports**—Provide rate of traffic statistics by application with details for an individual application.

- **Source reports**—Provide rate and percentage distribution of traffic by source host for the task for the selected time range.
- **Destination reports**—Provide rate and percentage distribution of traffic by destination host the task for the selected time range.
- **Session reports**—Display the rate and percentage distribution of traffic on source and destination pairs for the selected time range.

Source, destination, and session reports allow you to access more detailed data.

Traffic reports

Traffic reports for probe tasks provide statistics for the probe traffic analysis task. The **Traffic Trend** chart displays average traffic rate, and minimum average, maximum average, and average traffic rate statistics in a table for the associated task. The **Traffic Details** list provides individual data collection samples: timestamp, total volume of traffic, and traffic rate in seconds. You can filter reports by time range.

To view the reports for a probe task, click the **Traffic** tab to view traffic reports for the selected probe traffic analysis task.

Query traffic

NTA enables you to change the filter criteria for probe reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed under the **Traffic** tab.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
 - a. Specify the following query criteria:
 - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
 - b. Click **OK**.
The page displays the results of your query.
3. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. In **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**

- RTF
- XLSX
- PPTX
- HTML
- JRXML

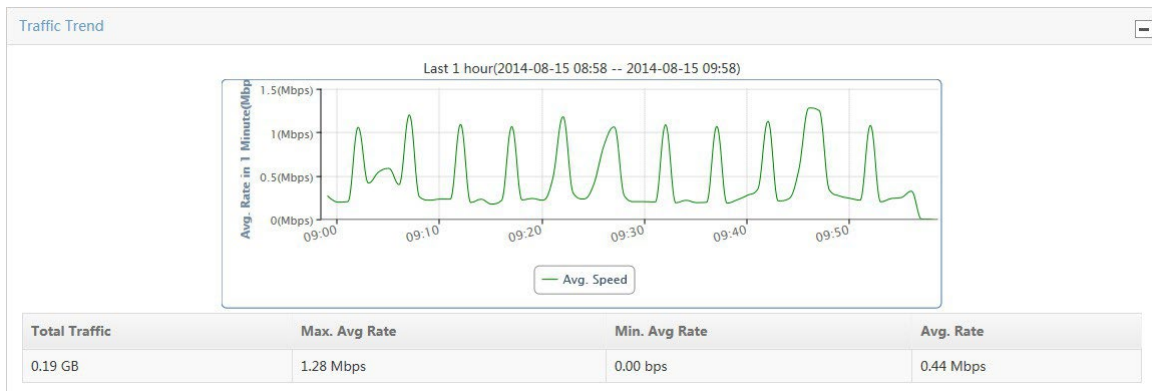
f. In **Page Range**, select the page range.

g. Click **Export**.

Traffic Trend – Average

The **Traffic Trend** line chart displays the average traffic rate for the selected time range. This chart provides total, minimum average, maximum average, and average traffic rate statistics in a table for traffic for the associated task for the selected time range.

Figure 96 Traffic Trend

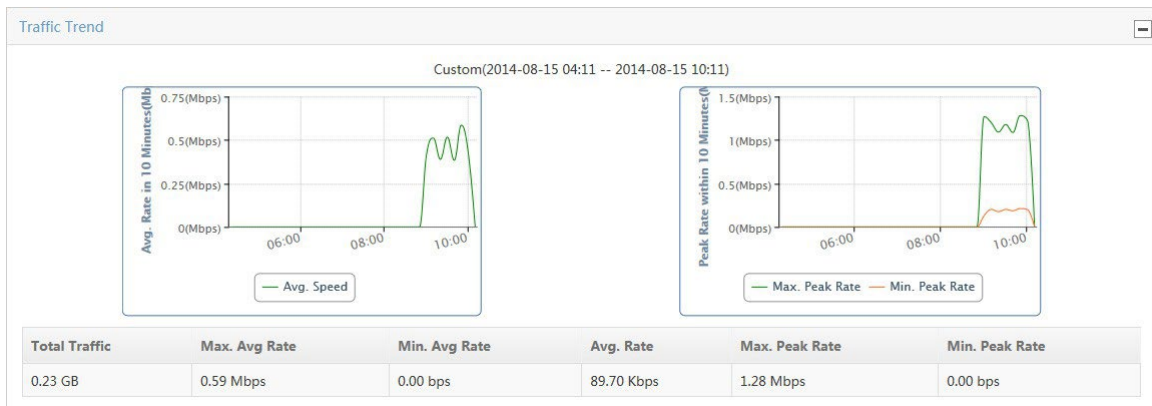


Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range. This chart contains two lines. The red line displays the maximum peak rate. The green line displays the MIN peak rate.

Figure 97 Traffic Trend – Peak Rate Report



For more information on enabling Peak Traffic Analysis, see "[Configuring NTA traffic analysis parameters.](#)"

Traffic Details

The **Traffic Details** list provides the data collection samples for traffic statistics based on the report time range. This report includes timestamp, total volume of traffic, and traffic rate in seconds.

Figure 98 Traffic Details

Traffic Details		
Time	Traffic	Rate
2014-08-15 09:13:00	1.38 MB	0.19 Mbps
2014-08-15 09:14:00	1.65 MB	0.23 Mbps
2014-08-15 09:15:00	1.25 MB	0.18 Mbps
2014-08-15 09:16:00	1.55 MB	0.22 Mbps
2014-08-15 09:17:00	7.62 MB	1.07 Mbps
2014-08-15 09:18:00	1.60 MB	0.22 Mbps
2014-08-15 09:19:00	1.71 MB	0.24 Mbps

Application reports

Application reports provide rate of traffic statistics by application, by protocol, and by application category for a task, with details for an individual application. Application reports for a probe traffic analysis task include the **Application List**, which provides a list of applications captured by the probe in the selected probe traffic analysis task. This report also provides additional reports for the selected application. The **Application Traffic Trend** stacked area chart displays average traffic rates for all applications captured by the probe in the selected traffic analysis task.

Protocol reports for a probe traffic analysis task include the **Protocol List**, which provides a list of protocols captured by the probe in the selected probe traffic analysis task. This report also links to additional reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average traffic rates for all protocols captured by the probe in the selected traffic analysis task.

Application category reports for a probe traffic analysis task include the **Application Category List**, which provides a list of the application categories captured by the probe in the selected probe traffic analysis task. This report also provides additional reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average traffic rates for all application categories captured by the probe in the selected traffic analysis task.

NTA provides a query option for filtering reports based on criteria you define. To view the reports for a probe task, click the **Application** tab to view application reports for the selected probe traffic analysis task, and set **Query Type** to **Application** as described in "[Query applications](#)."

Application reports display reports organized by the list of applications in NTA. NTA provides many system-defined applications and NTA also supports user defined applications. For more information on applications in NTA, see "[Managing applications](#)." This section describes the reports available for applications.

Query applications

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application, or time range for the graphs and tables to customize the reports listed on the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application** from the **Query Type** list.
The page displays the report for Layer 4 through Layer 7 applications.
3. Click **Select** next to the **Application** field.
The **Query Applications** dialog box displays an empty **Application List**.
To select the applications you want to search for, you must first query the **Application List** as follows:

- a. Specify one or more of the following search criteria in the **Query Applications** area of the dialog box:
 - **Application**—To search for applications, enter a partial or complete name in the **Application** field.
 - **Pre-defined**—To search for predefined applications, select **Yes** in the **Pre-defined** list. To filter for user-defined applications, select **No**.
To include system or predefined and user-defined applications, select **Not limited**.
 - b. To display the full **Application List**, click **Query** without entering any search criteria.
 - c. Click **Query**. The query results are displayed in the **Application List** below the **Query Applications** area.
 - d. Select the check boxes next to the applications you want to search.
 - e. Click **OK** to add the applications to the filter. The applications you selected are displayed in the **Application** field.
4. Click **Clear** next to the **Application** field to clear all selected applications.
- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
- Alternately, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.
5. Click **OK**.
The page displays the results of your query.
6. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
- a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.

g. Click **Export**.

Application List

The **Application List** provides a list of the applications observed for the selected probe traffic analysis task during the selected time range. This list displays the application name, a link for viewing the ports for all unknown applications, total volume of traffic for the associated application, rate of traffic, and the percentage of traffic on all probes generated by the associated application. The application name in the **Application** field is a link to reports for the selected application.

Figure 99 Application List

Application List				
Application	Unknown Applications	Traffic	Rate	Percentage
https		75.92 MB	0.18 Mbps	40.60%
TCP Protocol Unknown Application		41.93 MB	97.71 Kbps	22.43%
http		27.99 MB	65.22 Kbps	14.97%
ms-sql-s		24.88 MB	57.97 Kbps	13.31%
snmp		7.12 MB	16.58 Kbps	3.81%
UDP Protocol Unknown Application		2.45 MB	5.70 Kbps	1.31%
ldap		1.93 MB	4.49 Kbps	1.03%
kerberos		1.82 MB	4.23 Kbps	0.97%

1-8 of 23. Page 1 of 3.

Navigation: << < 1 2 3 > >> | 8

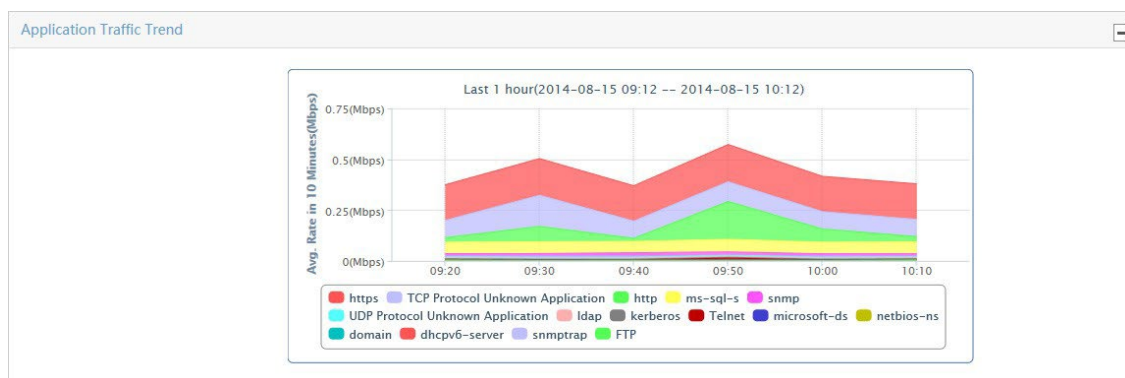
Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

To view this report for an individual application, click the name of the application. For more information about the individual application reports, see ["Individual application reports."](#)

Application Traffic Trend

The **Application Traffic Trend** stacked area chart provides average traffic for all applications observed for the selected traffic analysis task for the selected time range.

Figure 100 Application Traffic Trend



Individual application reports

NTA provides traffic trend statistics for the individual applications that were captured by the probe for a selected task. The **Traffic Trend** report displays the average rate of traffic for the selected application. The **TopN Application Usage List for Source and Destination Hosts** identifies the source and destination hosts that contributed the greatest volume of traffic for the selected application. Also included are reports for unknown TCP and UDP applications. Unknown applications are those applications for which the Layer 4 TCP or UDP port number has not been

assigned a name and is not included as an application in NTA. For more information on assigning names to TCP or UDP ports and adding them as applications to NTA, see "[Managing applications](#)."

To view individual application reports for a probe task, click the name in the **Application** field of the **Application List** report for the application for which you want to view this report.

To view unknown application reports for a probe task, click the icon  in the **Application** field of the **Application List** report for the application for which you want to view this report.

For more information about **Application List**, see "[Application List](#)."

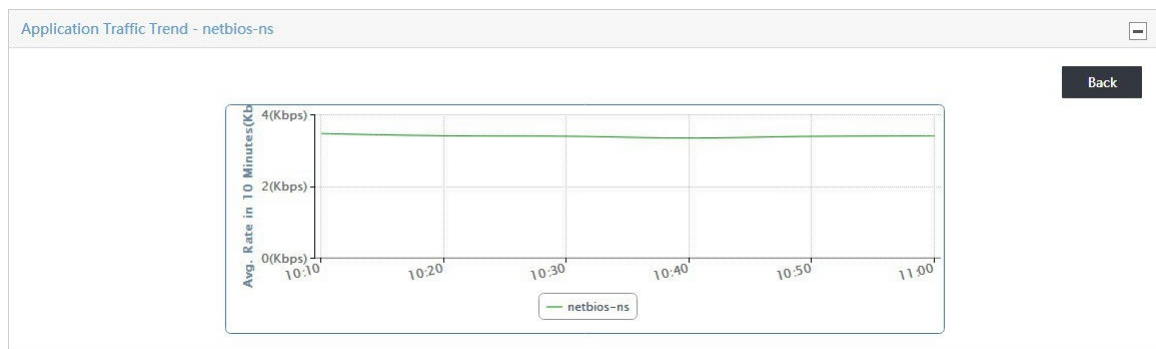
Application Traffic Trend

The **Application Traffic Trend** graph provides average rate of traffic for an individual application for the probe in the selected traffic analysis task.

By default, the **Application Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 101 Application Traffic Trend for an Individual Application



TopN Application Usage List

The **TopN Application Usage List** includes the **Source Host List** and the **Destination Host List**.

The **Source Host List** provides a list of the TopN source hosts measured by the volume of traffic in the selected probe traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

Figure 102 TopN Application Usage List

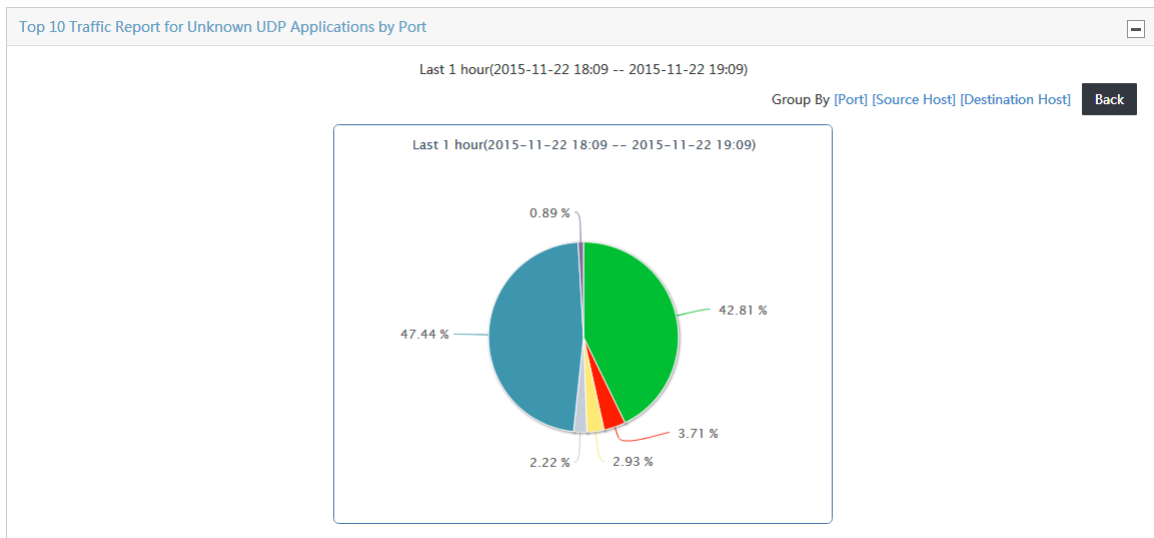
Top 10 Application Usage List - https					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
192.168.40.100	57.63 MB	75.93%	192.168.1.224	56.39 MB	74.29%
192.168.1.224	18.01 MB	23.73%	192.168.40.100	18.26 MB	24.06%
192.168.20.41	0.19 MB	0.25%	192.168.20.41	1.08 MB	1.43%
192.168.1.129	66.83 KB	0.09%	192.168.1.129	0.16 MB	0.21%
192.168.40.121	3.25 KB	0.00%	10.52.2.40	3.25 KB	0.00%

TopN traffic Report for Unknown TCP/UDP Applications by Port

The **TopN Traffic Report for Unknown TCP/UDP Applications by Port** provides the distribution of traffic by TCP or UDP port number for all application traffic that cannot be attributed to an application captured by the probe in the selected traffic analysis task for the selected time range. NTA enables you to change how the traffic is grouped. To group by port, select **Port** from the **Group By** list in the upper right corner of the **TopN Traffic Report for Unknown TCP/UDP Applications by Port** area of the page.

- To group by source host, select **Source Host** from the **Group By** list.
- To group by destination host, select **Destination Host** from the **Group By** list.

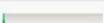
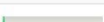
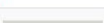
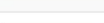
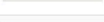
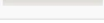
Figure 103 TopN Traffic Report for Unknown TCP/UDP Applications by Port



TopN Traffic List for Unknown TCP/UDP Applications by Port

The **TopN Traffic List for Unknown TCP/UDP Applications by Port** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the TCP or UDP port number, total volume of traffic for the associated port, rate of traffic, and the percentage of all observed traffic generated by the port. The port number is a link to individual reports for the selected port. The icon  in the **Define Application** field is a link for adding the selected port as a Layer 4 application to NTA. For more information on managing applications in NTA, see "[Managing applications](#)."

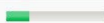
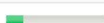
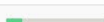
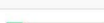
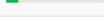
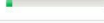
Figure 104 TopN Traffic List for Unknown TCP/UDP Applications by Port

Top 10 Traffic List for Unknown UDP Applications by Port				
Port	Traffic	Rate	Define Application	Percentage
5355	0.34 MB	0.80 Kbps		42.81% 
1900	30.63 KB	69.69 bps		3.71% 
18802	24.19 KB	55.05 bps		2.93% 
18801	18.31 KB	41.67 bps		2.22% 
55559	3.08 KB	7.01 bps		0.37% 
55648	1.01 KB	2.31 bps		0.12% 
51214	0.96 KB	2.18 bps		0.12% 
51073	0.93 KB	2.11 bps		0.11% 
56911	0.71 KB	1.62 bps		0.09% 
58890	0.68 KB	1.55 bps		0.08% 
Others	0.38 MB	0.89 Kbps		47.44% 

TopN traffic List for Unknown TCP/UDP Applications by Source Host

The **TopN Traffic List for Unknown TCP/UDP Applications by Source Host** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, rate of traffic, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host** is a link for initiating a host query and a link to the results of the query.

Figure 105 TopN Traffic List for Unknown TCP/UDP Applications by Source Host

Top 10 Traffic List for Unknown TCP Applications by Source Host				
Source Host	Traffic	Rate		Percentage
 192.168.40.222	1.25 MB	2.92 Kbps		23.07% 
 192.168.40.221	0.93 MB	2.16 Kbps		17.06% 
 192.168.40.223	0.91 MB	2.11 Kbps		16.67% 
 192.168.40.224	0.90 MB	2.11 Kbps		16.65% 
 192.168.40.205	0.69 MB	1.61 Kbps		12.70% 
 192.168.40.206	0.36 MB	0.84 Kbps		6.61% 
 192.168.40.191	0.21 MB	0.49 Kbps		3.84% 
 192.168.40.190	0.18 MB	0.43 Kbps		3.40% 

TopN Traffic List for Unknown TCP/UDP Applications by Destination Host

The **TopN Traffic List for Unknown TCP/UDP Applications by Destination Host** provides a list of the TopN unknown TCP or UDP applications, measured by volume and rate of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the destination host IP address, total volume of traffic for the associated destination, rate of traffic, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host** is a link for initiating a host query and a link to the results of the query.

Figure 106 TopN Traffic List for Unknown TCP/UDP Applications by Destination Host

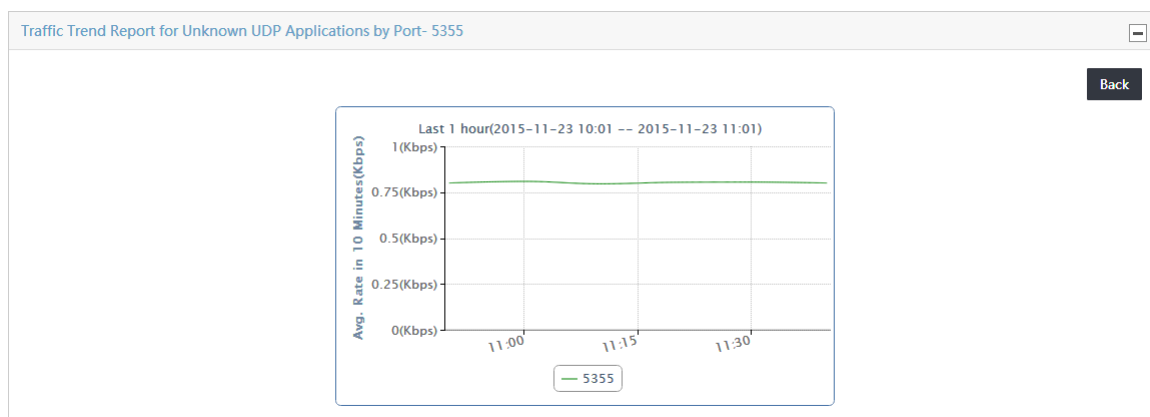
Top 10 Traffic List for Unknown TCP Applications by Destination Host				
Destination Host	Traffic	Rate	Percentage	
192.168.40.222	1.10 MB	2.56 Kbps	20.23%	
192.168.40.221	1.00 MB	2.32 Kbps	18.31%	
192.168.40.224	0.95 MB	2.21 Kbps	17.49%	
192.168.40.223	0.95 MB	2.21 Kbps	17.42%	
192.168.40.206	0.69 MB	1.61 Kbps	12.70%	
192.168.40.205	0.36 MB	0.84 Kbps	6.61%	
192.168.40.190	0.21 MB	0.49 Kbps	3.84%	
192.168.40.191	0.18 MB	0.43 Kbps	3.40%	

Traffic Trend Report for Unknown TCP/UDP Applications by Port

To view this report for a probe task, click the link in the **Port** field of the **TopN Traffic List for Unknown TCP/UDP Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **Traffic Trend** graph provides the average rate for an individual unknown application captured by the probe in the selected traffic analysis task.

Figure 107 Traffic Trend Report for Unknown TCP/UDP Applications by Port



TopN Traffic Details for Unknown TCP/UDP Applications by Port

To view this report for a probe task, click the link in the **Port** field of the **TopN Traffic List for Unknown TCP/UDP Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **TopN Traffic Details for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source host.

Figure 108 TopN Traffic Details for Unknown Applications by Port

Top 10 Traffic Details List for Unknown UDP Applications by Port - 5355

Source Host	Destination Host	Traffic	Rate	Percentage
fe80::d976:7251:7c18:...	ff02::1:3	50.26 KB	0.11 Kbps	14.23% 
fe80::2da4:a3e1:647a:...	ff02::1:3	43.41 KB	98.78 bps	12.29% 
192.168.40.180	224.0.0.252	39.17 KB	89.14 bps	11.09% 
192.168.0.153	224.0.0.252	29.90 KB	68.04 bps	8.46% 
fe80::8144:1c13:1f00:...	ff02::1:3	18.21 KB	41.43 bps	5.15% 
fe80::b852:50aa:58b:5...	ff02::1:3	16.56 KB	37.69 bps	4.69% 
fe80::4972:3255:cd7b:...	ff02::1:3	16.13 KB	36.70 bps	4.57% 
fe80::d8a6:2313:a73a:...	ff02::1:3	15.24 KB	34.68 bps	4.31% 
fe80::244c:6b8f:7484:...	ff02::1:3	14.86 KB	33.82 bps	4.21% 
192.168.0.158	224.0.0.252	11.65 KB	26.51 bps	3.30% 
Others	Others	97.88 KB	0.22 Kbps	27.71% 

Protocol reports

Protocol reports display traffic rate trend reports organized by the list of predefined and user-defined protocols in NTA. Protocol reports for a probe traffic analysis task include the **Protocol List**, which provides a list of protocols captured by the probe in the selected probe traffic analysis task. This report also provides drill-down capabilities for additional reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart displays average traffic rates for all protocols captured by the probe in the selected traffic analysis task. Protocol reports also include traffic lists and trend reports for individual protocols.

As with all report types for a probe task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a probe task, click the **Application** tab to view application reports for the selected probe traffic analysis task, and set **Query Type** to **Protocol** as described in "Query protocols." For more information on protocols in NTA, see "Managing protocols." This section describes the reports available for protocols.

Query protocols

To view reports by protocol, you must configure the filter criteria for application reports. You can change the default settings for query type, protocol, or time range for the graphs and tables to customize the reports displayed on the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Protocol** from the **Query Type** list. The page displays the report for protocols.
3. Click **Select** next to the **Protocol** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the protocol you want to search for, you must first query the **Protocol List** as follows:

- a. Specify one or more of the following search criteria in the **Query Protocols** area of the dialog box:
 - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
 - **Pre-defined**—To search for protocols that are predefined, select **Yes** in the **Pre-defined** list.

To filter for protocols that are user-defined, select **No**.

To include system or predefined and user-defined protocols, select **Not limited**.

- b. To display the full **Protocol List**, click **Query** without entering any search criteria.
- c. Click **Query**. The query results are displayed in the **Protocol List** below the **Query Protocols** area.
- d. Select the check boxes next to the protocols for which you want to search.
- e. Click **OK** to add the protocols to the filter. The protocols you selected are displayed in the **Protocol** field.

Click **Clear** next to the **Protocol** field to clear all selected protocols.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the protocol report, click the icon  in the upper right corner of the protocol report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for protocols.

4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. Select the page range in **Page Range**.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. Select the page range in **Page Range**.
 - g. Click **Export**.

Protocol List

The **Protocol List** provides a list of the protocols captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the protocol name, total volume of traffic for the associated protocol, rate of traffic, and the percentage of traffic on the probe generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.

Figure 109 Protocol List

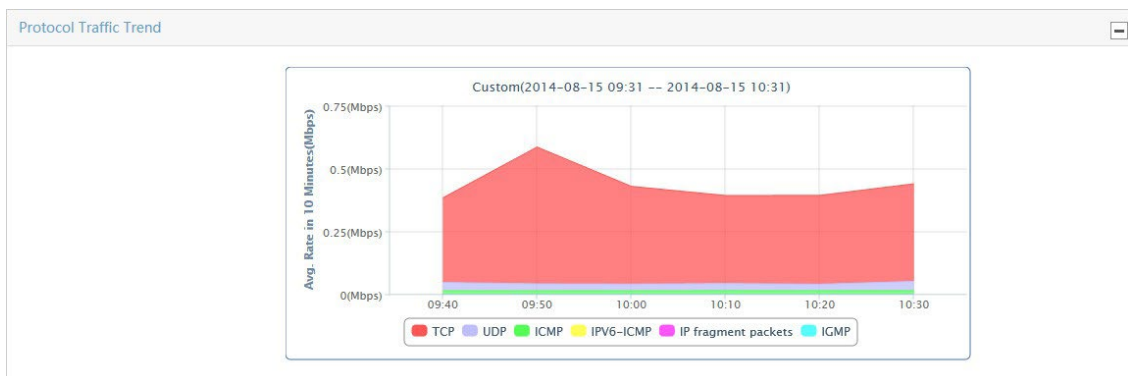
Protocol	Traffic	Rate	Percentage
TCP	0.16 GB	0.39 Mbps	90.02%
UDP	12.86 MB	29.96 Kbps	6.85%
ICMP	5.75 MB	13.40 Kbps	3.06%
IPv6-ICMP	98.36 KB	0.22 Kbps	0.05%
IP fragment packets	30.01 KB	68.29 bps	0.02%
IGMP	0.23 KB	0.53 bps	0.00%

1-6 of 6. Page 1 of 1.

Protocol traffic trend

The **Protocol Traffic Trend** stacked area chart displays average traffic rates for all protocols captured by the probe in the selected traffic analysis task for the selected time range.

Figure 110 Protocol Traffic Trend



Individual protocol reports

NTA provides traffic trend statistics for the individual protocols that were captured by the probe for a selected task. Individual protocol reports include the **Protocol Traffic Trend** report that displays the average rate of traffic for the selected protocol. Individual protocol reports also include the **TopN Protocol Usage List** source and destination hosts list that identifies which source and destination hosts contributed the greatest volume of traffic for the selected protocol.

To view individual protocol reports for a probe task, click the name in the **Protocol** field of the **Protocol List** report for the protocol for which you want to view this report. For more information about **Protocol List**, see "[Protocol List](#)."

Protocol traffic trend

The **Protocol Traffic Trend** graph provides the average rate for an individual protocol captured by the probe in the selected traffic analysis task.

By default, the **Protocol Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 111 Traffic Trend Report for an Individual Protocol



TopN protocol usage list

The **TopN Protocol Usage List** includes **Source Host List** and the **Destination Host List**.

The **TopN Protocol Usage List – Source Host List** displays a list of the TopN source hosts, measured by volume of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **TopN Protocol Usage List – Destination Host List** displays a list of the TopN destination hosts, measured by volume of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

Figure 112 TopN Protocol Usage List

Top 10 Protocol Usage List - TCP					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 192.168.40.100	59.69 MB	35.40% 	 192.168.1.224	56.38 MB	33.43% 
 192.168.40.205	21.02 MB	12.47% 	 192.168.40.100	19.86 MB	11.78% 
 192.168.1.224	18.01 MB	10.68% 	 192.168.40.208	15.32 MB	9.09% 
 192.168.40.207	12.36 MB	7.33% 	 192.168.40.205	11.03 MB	6.54% 
 192.168.40.208	9.18 MB	5.45% 	 192.168.20.41	8.76 MB	5.19% 
 192.168.40.222	8.31 MB	4.93% 	 192.168.40.222	7.29 MB	4.32% 
 192.168.40.221	6.25 MB	3.71% 	 192.168.30.108	7.03 MB	4.17% 
 192.168.40.224	6.19 MB	3.67% 	 192.168.40.221	6.64 MB	3.94% 
 192.168.40.223	6.10 MB	3.62% 	 192.168.40.207	6.53 MB	3.87% 
 192.168.20.41	5.65 MB	3.35% 	 192.168.40.224	6.46 MB	3.83% 
Other Hosts	15.86 MB	9.41% 	Other Hosts	23.33 MB	13.83% 

Application category reports

Application category reports display traffic rate trend reports organized by the NTA application categories. Application category reports for a probe traffic analysis task include the **Application Category List**, which provides a list of the application categories captured by the probe in the selected probe traffic analysis task. This list includes total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic captured by the probe

generated by the associated application category. This report also provides access to additional reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average traffic rates for all applications captured by the probe in the selected traffic analysis task. Application category reports also include traffic lists and trend reports for the individual application categories.

As with all report types for a probe task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a probe task, click the **Application** tab to view application reports for the selected probe traffic analysis task, and set **Query Type** to **Application Category** as described in "[Query application categories](#)."

NTA provides system-defined application categories and supports user-defined application categories. For more information on application categories in NTA, see "[Managing application categories](#)." This section describes the reports available for application categories.

Query application categories

To view reports by application category, you must configure the filter criteria for application category reports.

NTA enables you to change the filter criteria for application category reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application Category** from the **Query Type** list. The page displays the report for application categories.
3. Click **Select** next to the **Application Category** field.

The **Query Application Categories** dialog box displays an empty **Application Category List**.

To select the application categories you want to search for, you must first query the **Application Category List** as follows:

- a. In the **Query Application Categories** area, specify one or more of the following search criteria:
 - **Application Category**—Enter a partial or complete name for the application categories for which you want to search.
 - **Pre-defined**—To search for application categories that are predefined, select **Yes** in the **Pre-defined** list.
To filter for application categories that are user-defined, select **No**.
To include system or predefined and user-defined application categories, select **Not limited**.
- b. Click **Query**.
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
To display the full **Application Category List**, click **Query** without entering any search criteria.
- c. Select the check boxes next to the application categories for which you want to search.
- d. Click **OK** to add the application categories to the filter.

The application categories are displayed in the **Application Category** field.

Click **Clear** next to the **Application Category** field to clear all selected application categories.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.

- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time. Additionally, to set the start time and end time for the application category report, click the icon  in the upper right corner of the application category report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

- a. To print this report, click the **Print** icon  on the toolbar.
- b. Select the page range from **Page Range**.
- c. To export the data, click **Export**.
- d. To export this report, click the **Export** icon  on the toolbar.
- e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
- f. Select the desired page rang from **Page Range**.
- g. Click **Export**.

Application Category List

The **Application Category List** provides a list of the application categories captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the application category name, total volume of traffic for the associated application category, rate of traffic, and the percentage of traffic on the probe generated by the associated application category. The application category name in the **Application Category** field is a link to reports for the selected application category.

Figure 113 Application Category List

Application Category ↕	Traffic ↕	Rate ↕	Percentage ↕
HTTP	0.10 GB	0.24 Mbps	55.08%
Database Application	24.50 MB	57.10 Kbps	13.06%
Network Management	8.64 MB	20.13 Kbps	4.60%
Enterprise Application	3.80 MB	8.86 Kbps	2.03%
File Service	1.24 MB	2.89 Kbps	0.66%
Remote Management	0.77 MB	1.80 Kbps	0.41%
P2P	0.53 KB	1.22 bps	0.00%
Other Application Category	45.34 MB	0.11 Mbps	24.16%

1-8 of 8. Page 1 of 1.

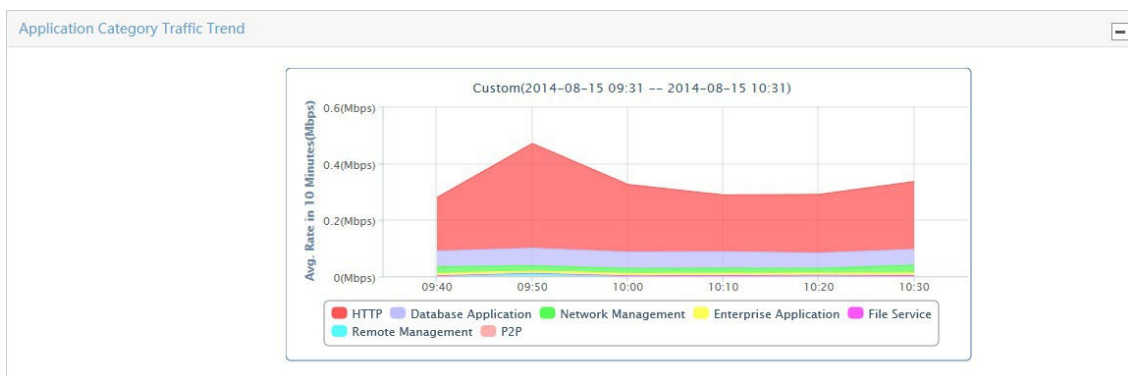
« < 1 > » 8 ▾

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

Application Category Traffic Trend

The **Application Category Traffic Trend** stacked area chart provides average traffic rates for all application categories captured by the probe in the selected traffic analysis task for the selected time range.

Figure 114 Application Category Traffic Trend



Individual application category reports

NTA provides traffic trend statistics for the individual application categories that are captured by the probe for a selected task. Individual application category reports include the **Application Category Traffic Trend** report and the **TopN Application Category Usage List**.

To view application category reports for a probe task, click the name in the **Application Category** field of the **Application Category List** report for the application category for which you want to view this report. For more information about **Application Category List**, see "[Application Category List](#)."

Application Category Traffic Trend

The **Application Category Traffic Trend** graph displays the average rate for an individual application category captured by the probe in the selected traffic analysis task. By default, this graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

Figure 115 Traffic Trend Report for an Individual Application Category



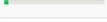
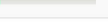
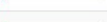
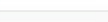
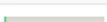
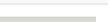
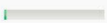
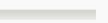
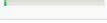
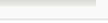
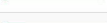
TopN Application Category Usage List

The **TopN Application Category Usage List** includes the **Source Host List** and the **Destination Host List**.

The **TopN Application Category Usage List – Source Host List** provides a list of the TopN source hosts measured by volume of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic captured by the probe in the selected probe traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

Figure 116 TopN Application Usage List

Top 10 Application Category Usage List - File Service					
Source Host List			Destination Host List		
Source Host IP Address	Traffic	Percentage	Destination Host IP Address	Traffic	Percentage
 192.168.3.139	0.80 MB	49.58% 	 192.168.3.255	1.29 MB	80.00% 
 192.168.40.180	0.14 MB	8.79% 	 192.168.40.255	0.12 MB	7.47% 
 192.168.0.153	69.87 KB	4.24% 	 192.168.40.248	73.97 KB	4.49% 
 192.168.0.132	68.19 KB	4.14% 	 192.168.0.255	47.66 KB	2.89% 
 192.168.3.55	42.82 KB	2.60% 	 169.254.255.255	44.10 KB	2.68% 
 192.168.0.99	42.25 KB	2.56% 	 192.168.1.255	26.06 KB	1.58% 
 192.168.0.157	36.63 KB	2.22% 	 192.168.2.255	4.29 KB	0.26% 
 192.168.0.160	36.54 KB	2.22% 	 1.1.3.255	4.18 KB	0.25% 
 192.168.0.158	36.54 KB	2.22% 	 192.168.43.255	3.89 KB	0.24% 
 192.168.0.133	36.00 KB	2.18% 	 172.8.255.255	2.44 KB	0.15% 
Other Hosts	0.31 MB	19.25% 			

Source reports

Source reports include the **TopN Traffic Report for Source Host** chart that provides the distribution of traffic for the TopN source hosts for the selected traffic analysis task. This report also contains a link to traffic reports for the selected source host. Source reports also include the **TopN Traffic List for Source Host**, which provides a list of the TopN source hosts measured by volume of traffic for

the selected task. This report also contains a link to reports for the selected source host. The query icon  next to the source IP address is a link for initiating a host query and a link to the results of the query. NTA also provides a query option for filtering reports based on criteria you define.

To view the source reports for a probe task, click the **Source** tab.

Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed under the **Source** tab.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following search criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
 Example of a valid IP address:
 10.153.89.10
 Example of a valid network/subnet mask in dotted decimal notation:
 10.153.89.0/255.255.255.0
 Example of a valid network or subnet mask using CIDR notation:
 10.153.89.0/24
 Example of a valid IPv6 address entry:
 a001:410:0:1::1
 Example of a valid IPv6 address and subnet mask using CIDR notation:
 a001:410:0:1::1/64
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
 The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. Select the page range in **Page Range**.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**

- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

f. Select the page range in **Page Range**.

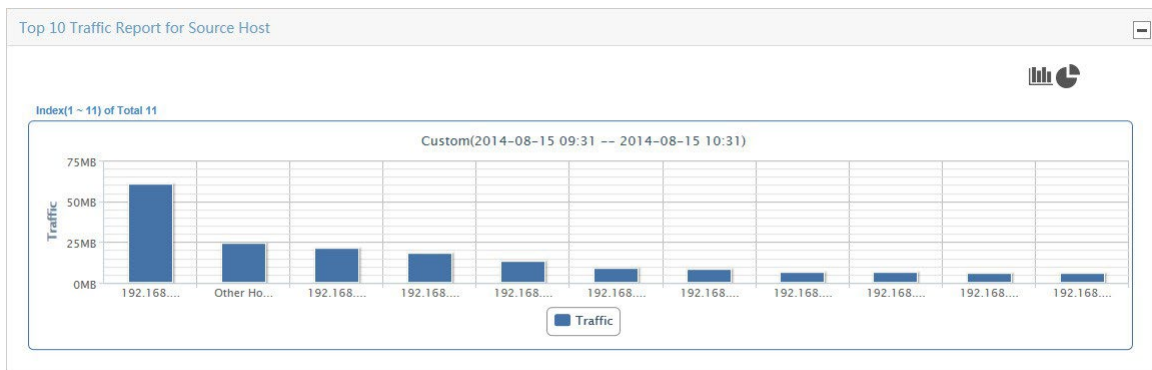
g. Click **Export**.

TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host** bar chart displays the TopN source hosts with the most inbound/outbound traffic in a certain period of time in a selected probe traffic analysis task. Click a bar in the chart to view the traffic analysis report of each source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the traffic distribution of the TopN source hosts in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected source host.

Figure 117 TopN Traffic Report for Source Host



TopN Traffic List for Source Host

The **TopN Traffic List for Source Host** provides a list of the TopN source hosts measured by volume of traffic for the selected probe traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The IP address is a link to reports for the selected source host. The probe query icon  next to the source IP address is a link for initiating a host query and a link to the results of the query.

Figure 118 TopN Traffic List for Source Host

Top 10 Traffic List for Source Host			Generate Chart
Source	Traffic	Percentage	
192.168.3.139	0.80 MB	16.59%	
192.168.40.180	0.31 MB	6.38%	
192.168.0.153	0.22 MB	4.48%	
fe80::d976:7251:7c18:a2a9	0.19 MB	3.86%	
192.168.0.132	0.18 MB	3.83%	
0.0.0.0	0.18 MB	3.81%	
fe80::9d9d:460f:8201:39c7	0.18 MB	3.73%	
fe80::2da4:a3e1:647a:6e7e	0.14 MB	2.82%	
fe80::5903:4ea9:27e4:6033	0.11 MB	2.31%	
192.168.0.154	101.43 KB	2.06%	
Other Hosts	2.41 MB	50.13%	

Traffic Trend Report for Source Host

To view this report for a probe task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Trend Report for Source Host** line chart displays the average rate of traffic for the selected source host. By default, the **Traffic Trend Report for Source Host** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.
- To return to the main **Source** host report page, click **Back**.

Figure 119 Traffic Trend Report by Source Host



Traffic details

To view this report for a probe task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Details** for a source host table provides the following lists:

- The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between the source and destination hosts, and the percentage of all traffic observed for the source and destination hosts.

- The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

Figure 120 Traffic Details

Traffic Details					
Top 10 Destination Hosts Communicating with the Source Host			Top 10 Applications Communicating with the Source Host		
Destination	Traffic	Percentage	Application Name	Traffic	Percentage
 192.168.1.224	56.38 MB	93.33% 	https	57.79 MB	95.66% 
 10.153.0.61	1.77 MB	2.93% 	kerberos	0.92 MB	1.53% 
 192.168.20.41	1.33 MB	2.20% 	ldap	0.85 MB	1.41% 
 192.168.1.138	0.71 MB	1.17% 	TCP Protocol Unknown Application	0.72 MB	1.20% 
 192.168.1.129	0.10 MB	0.17% 	domain	89.72 KB	0.15% 
 10.72.66.36	89.72 KB	0.15% 	UDP Protocol Unknown Application	28.16 KB	0.05% 
 172.8.8.1	28.16 KB	0.05% 	http	5.68 KB	0.01% 
			ICMP Protocol Application	3.10 KB	0.01% 

Destination reports

The **TopN Traffic Report for Destination Host** chart provides the distribution of traffic for the TopN destination hosts for the selected traffic analysis task. This report also contains a link to traffic reports for the selected destination host.

The **TopN Traffic List for Destination Host** provides a list of the TopN destination hosts measured by volume of traffic for the selected task. This report contains a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and a link to the results of the query. NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a probe task, click the **Destination** tab to view traffic reports for the selected probe traffic analysis task.

Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for the destination host or time range to customize the charts and lists displayed on the **Destination** tab.

1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the destination report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:

- o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

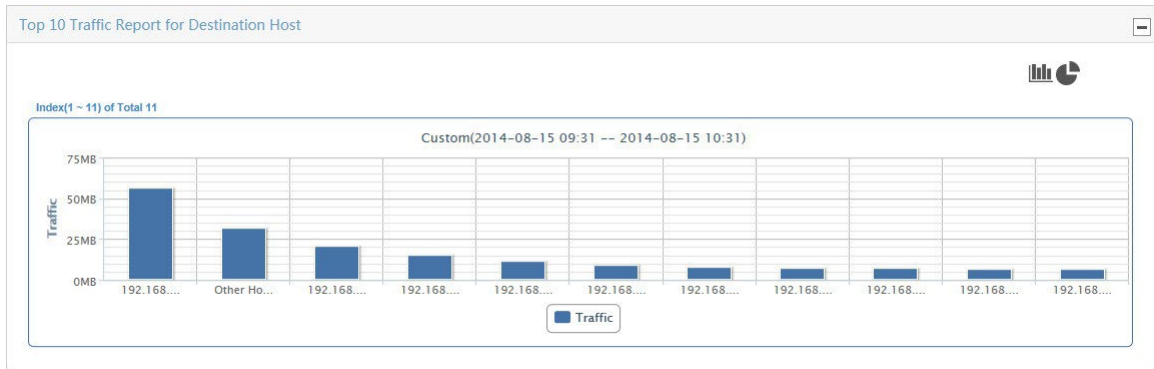
- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
- a. To print this report, click the **Print** icon  on the toolbar.
 - b. Select the page range from **Page Range**.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. Select the page range from **Page Range**.
 - g. Click **Export**.

TopN Traffic Report for Destination Host

The **TopN Traffic Report for Destination Host** bar chart displays the TopN destination hosts with the most inbound/outbound traffic in a certain period of time in a selected probe traffic analysis task. Click the bars in the chart to view the traffic analysis report of each destination host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the traffic distribution of the TopN destination hosts in the selected traffic analysis task for the selected time range.

Figure 121 TopN Traffic Report for Destination Host



TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host** provides a list of the TopN destination hosts measured by volume of traffic for the selected probe traffic analysis task for the selected time range. This list includes the destination host IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The IP address is a link to reports for the selected destination. The host query icon next to the destination IP address is a link for initiating a host query and a link to the results of the query.

Figure 122 TopN Traffic List for Destination Host

Top 10 Traffic List for Destination Host			Generate Chart
Destination	Traffic	Percentage	
192.168.3.255	1.21 MB	25.90%	
ff02::1:3	0.94 MB	20.01%	
ff02::1:2	0.72 MB	15.30%	
224.0.0.252	0.71 MB	15.13%	
224.0.0.22	0.21 MB	4.45%	
255.255.255.255	0.18 MB	3.86%	
192.168.40.255	0.12 MB	2.64%	
192.168.40.248	0.11 MB	2.33%	
ff02::1:ff3e:6099	76.59 KB	1.60%	
ff02::1:ff5:8875	76.59 KB	1.60%	
Other Hosts	0.34 MB	7.18%	

Traffic Trend Report for Destination Host

To view this report for a probe task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.
- To return to the main **Destination** host report page, click **Back**.

Figure 123 Traffic Trend Report for Destination Host



Traffic details

To view this report for a probe task, click the bar of the bar chart on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Details** for a destination host table provides two lists. The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the source hosts, and the percentage of all traffic observed for this destination host and the source hosts.

The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

Figure 124 Traffic details

Traffic Details					
Top 10 Source Hosts Communicating with the Destination Host			Top 10 Applications Communicating with the Destination Host		
Source	Traffic	Percentage	Application Name	Traffic	Percentage
192.168.40.180	98.25 KB	87.87%	UDP Protocol Unknown Application	40.75 KB	36.45%
192.168.40.77	12.47 KB	11.15%	ftp-data	36.32 KB	32.48%
192.168.40.186	0.78 KB	0.70%	FTP	34.42 KB	30.78%
192.168.30.100	0.32 KB	0.28%	snmptrap	0.32 KB	0.28%

Session reports

A session is a unique source and destination pair. Session reports include the **TopN Traffic Report for Session Host** chart that provides the distribution of traffic for the TopN session pairs for the selected traffic analysis task for the selected time range. This report also contains a link to traffic reports for the selected host. Session reports also include the **TopN Traffic List for Session Host** that provides a list of the TopN session pairs measured by volume of traffic observed for the selected probe traffic analysis task. This report also contains a link to reports for the selected session host.

The host query icon next to the **Session** IP address is a link for initiating a probe query and a link to the results of the query. As with all report types for a probe task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a probe task, click the **Session** tab to view traffic reports for the selected probe traffic analysis task.

Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination pair information, or change the time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
 Example of a valid IP address:
 10.153.89.10
 Example of a valid network/subnet mask in dotted decimal notation:
 10.153.89.0/255.255.255.0
 Example of a valid network/subnet mask using CIDR notation:
 10.153.89.0/24
 Example of a valid IPv6 address:
 a001:410:0:1::1
 Example of a valid IPv6 address and subnet mask using CIDR notation:
 a001:410:0:1::1/64
 - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
 The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. Select the page range from **Page Range**.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. Select the export file format from the **File Format** list. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**

– JRXML

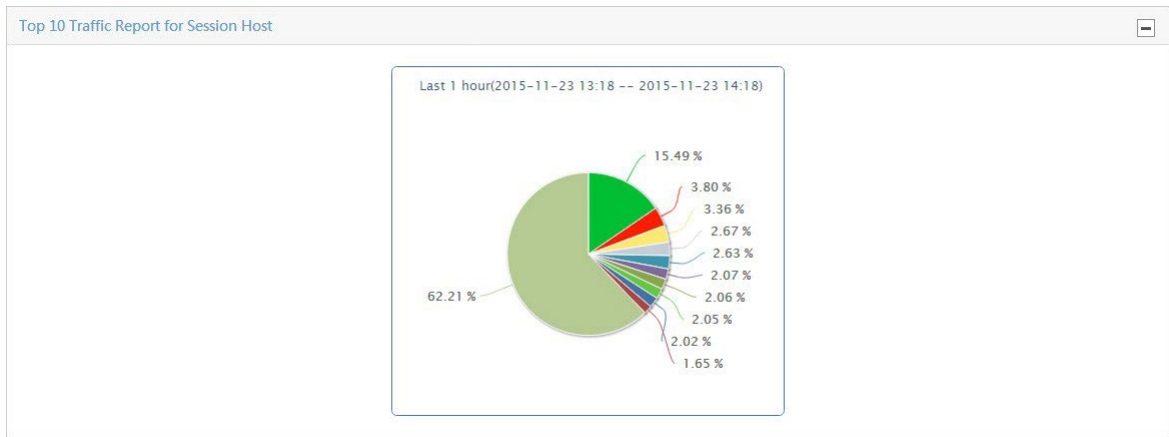
f. Select the page range from **Page Range**.

g. Click **Export**.

TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host** chart displays the distribution of traffic for TopN session source and destination pairs for the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the selected source and destination session pair.

Figure 125 TopN Traffic Report for Session Host



TopN Traffic List for Session Host

The **TopN Traffic List for Session Host** provides a list of the TopN session source and destination pairs measured by volume of traffic observed for the selected probe traffic analysis task for the selected time range. This list includes the source and destination IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair. The icon  in the **Details** field is a link to reports for the selected session or source and destination pair. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link to the results of the query.

Figure 126 TopN Traffic List for Session Host

Top 10 Traffic List for Session Host					Generate Chart
Source Host	Destination Host	Traffic	Percentage	Details	Topology
192.168.3.139	192.168.3.255	0.73 MB	15.49%		
0.0.0.0	255.255.255.255	0.18 MB	3.80%		
fe80::d976:7251:7c18:a2a9	ff02::1:3	0.16 MB	3.36%		
192.168.40.180	224.0.0.252	0.13 MB	2.67%		
fe80::2da4:a3e1:647a:6e7e	ff02::1:3	0.12 MB	2.63%		
fe80::5903:4ea9:27e4:6033	ff02::1:3	99.54 KB	2.07%		
fe80::9d9d:460f:8201:39c7	ff02::1:3	98.75 KB	2.06%		
192.168.40.180	192.168.40.248	98.25 KB	2.05%		
192.168.0.153	224.0.0.252	96.74 KB	2.02%		
192.168.40.170	224.0.0.252	79.15 KB	1.65%		
Other Hosts	Other Hosts	2.91 MB	62.21%		

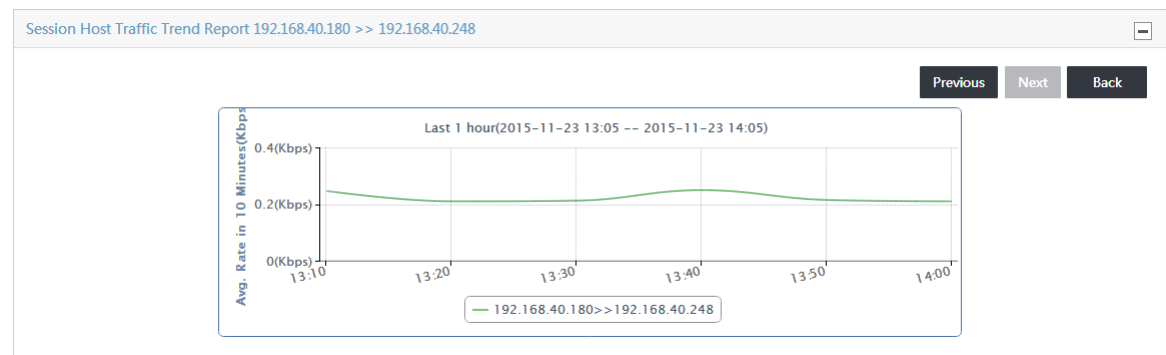
Session Host Traffic Trend Report

To view this report for a probe task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Host Traffic Trend Report** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.
- To return to the main **Session** report page, click **Back**.

Figure 127 Session Host Traffic Trend Report

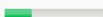


TopN Applications for Session Host

To view this report for a probe task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

Figure 128 TopN Applications for Session Host

Top 10 Applications for Session Host 192.168.40.180 >> 192.168.40.248		
Application Category	Traffic	Percentage
ftp-data	36.32 KB	36.97% 
FTP	34.42 KB	35.03% 
UDP Protocol Unknown Application	27.51 KB	28.00% 

Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source and destination hosts.

Application monitoring

This chapter describes application monitoring in NTA. It provides an overview of the application traffic analysis tasks and the reports they generate, and describes considerations when adding applications to a task. The chapter also explains how to manage the application traffic analysis tasks and view their reports.

Application traffic analysis overview

Application traffic analysis tasks analyze network flow data by examining the application data in network flow records. NTA parses network flow data and provides various statistical views of network traffic generated by the applications configured in an application traffic analysis task. For example, NTA provides source and destination host traffic rate information, which shows the rate of traffic attributed to specific source or destination hosts that were observed sending or receiving application traffic for the applications specified in a task. Session reports display the source and destination host pairs that are observed sending or receiving traffic for the specified application. Because analyses based on hosts are not tied to a specific data source, such as an interface, device, or probe, these reports enable you to view application traffic rates for all areas of the network that generate network flow records.

The NTA application traffic analysis tasks provide traffic statistics for the applications configured in every application traffic analysis task. In general, the application traffic reports include rate of traffic for all applications in all tasks and for the applications in a task. Application statistics provide per-second traffic rate for each application in a task. Also, they provide distribution of application traffic generated by source host, destination host, or by a session or source/destination host pair. These reports are organized into multiple layers from summarized information for tasks to detailed reporting for specific applications configured for an individual application traffic analysis task.

This chapter looks at the report structure for application traffic analyses, configuration issues around traffic analysis tasks and the reports they generate. It describes the process for managing application traffic analysis tasks, including instructions for adding, modifying, and deleting tasks from NTA. This chapter provides a survey of the summary reports for all application tasks and also looks at the more granular reports for an individual application traffic analysis task.

Application traffic analysis reporting overview

After you create the first application traffic analysis task, NTA creates an  **Application Traffic Analysis Task** entry under the **Traffic Analysis and Audit** area on the left navigation tree.

Click  **Application Traffic Analysis Task** on the left navigation tree to view the summary report for all application traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **Application Traffic Analysis Task**. The **Application Traffic Analysis Task** shortcut menu displays all application traffic analysis tasks created in NTA. Click the name link for a task to view the application traffic analysis report of the task.

The summary application traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides summarized average traffic rate per second reporting for all applications specified in all application traffic analysis tasks summarized by task for the last hour. Each bar in the graph is a link to more detailed reporting for the selected task. This includes reporting for traffic rates, source, destination, and session statistics. Each of these detailed categories include several reports:
 - **Traffic**—Reports found under the **Traffic** tab for application reporting include traffic trends that display the average rate per second attributed to the applications in the selected task and the data samples for the applications in the selected task.

- **Source**—Reports found under the **Source** tab for application reporting include a pie chart showing the percentage of traffic generated by the TopN source hosts. Also included is a tabular list showing volume and percentage of traffic generated for each of the TopN source hosts that generated traffic for the selected application.
- **Destination**—Reports found under the **Destination** tab for application reporting include a pie chart showing the percentage of traffic generated by the TopN destination hosts. Also included is a tabular report showing volume and percentage of traffic generated for each of the TopN destination hosts that generated traffic for the selected application.
- **Session**—Reports found under the **Session** tab for application reporting include a pie chart showing the percentage of traffic generated by the TopN source and destination host pairs. Also included is a tabular report showing volume and percentage of traffic generated for each of the TopN source and destination host pairs that generated traffic for the selected application.
- **Traffic Trend for Selected Task (Last 1 Hour)**—This line chart provides the per second average traffic rate summarized by application traffic analysis task for the application tasks you select.
- **Summary List (Last 1 Hour)**—This list provides the per second traffic rate and the total volume of traffic summarized by the application traffic analysis task. This list enables you to navigate to more detailed application reporting for the selected task.

Application traffic analysis configuration considerations

You must consider several things when adding applications to a task—the most important of which is determining the applications that belong to each task. Consider the following:

- By default, NTA does not monitor any applications. Therefore, you must create a task for every application or group of applications on which you want to monitor and report.
- You must anticipate the locations on your network where you are certain to capture application data. You must enable network flow data for the devices and the interfaces on them for those locations on your network where you know the application for which you want to monitor traffic can be captured. Then, you must add these devices and probes to NTA using the Device Management and Probe Management features in NTA. NTA then summarizes application data for all devices and probes on which it observes the application traffic.
- NTA provides summarized application reporting based on the way you group applications into tasks. Consider how you want to summarize, access, and view application data. Then, structure your tasks around it. For example, create an application task called NetMgmt and add all applications used that support the network management function for your environment. NTA summarizes all traffic observed for all applications into the group **NetMgmt** and attribute traffic in the reports to the task name you have configured.
- When you add applications to a task, NTA presents a list of all applications that NTA knows about. This list is generated from the applications that came predefined in NTA and to which user-defined applications have been added. If this list does not contain the applications you want to add, it is most likely because the application has not been added to NTA. For more information on adding applications to NTA, see "[Modifying an NTA server configuration](#)."

Managing application traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA does not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need. This section describes the process for managing application traffic analysis tasks in NTA. It also describes the process for adding, modifying, or removing application traffic analysis tasks in NTA.

Viewing a traffic analysis task

NTA displays all tasks in the **Traffic Analysis Task List**. From this list, you can view, add, modify, and delete all tasks including application traffic analysis tasks.

To view the NTA traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

Task list contents

- **Task Name**—Contains the name of the task. The contents of this field link to the **Traffic Analysis Task Details** page for the associated task.
 - **Task Description**—Contains the description for the associated task.
 - **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **Baseline Analysis**—This parameter is displayed when the Baseline Analysis feature is enabled in NTA parameters. The Baseline Analysis feature provides an additional layer of analysis to reports provided by NTA by including baseline trend data when data has been collected for a minimum of one week.
 - **Modify**—Contains an icon  for modifying the associated task.
 - **Delete**—Contains an icon  for deleting the associated task.
3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** located in the upper left corner of the **Traffic Analysis Task List**.

You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing application traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. In the **Task Name** field of the **Traffic Analysis Task List** whose **Task Type** is **Application**, click the contents to view the details for an individual task.

Traffic analysis task details

- **Task Name**—Contains the name of the task.
- **Task Description**—Contains the description for the associated task.
- **Server**—Contains the name or IP address of the NTA server.

- **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
- **Reader**—Identifies the groups in INC that have been granted access to read the reports generated by the associated task.
- **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA server, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
- **Enable Automatic Anomaly Detection Based On The Baseline**—Indicates whether automatic detection of abnormal traffic based on the baseline is enabled for the task. This parameter is displayed only when baseline analysis is enabled.
- **Baseline Threshold Setting**—Displays parameters of the baseline threshold setting. This area is displayed only when baseline analysis is enabled. The baseline threshold setting includes the following parameters:
 - **Baseline Upper/Lower Threshold**—Indicates the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - **Trigger**—Indicates under what condition the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be met.
 - **Threshold**—Indicates the traffic percentage threshold that must be met before NTA generates an alarm.
 - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
- **Application List**—Identifies all applications configured for reporting in the associated application traffic analysis task.
- **Threshold Alarm**—Specifies whether the Threshold Alarm feature is enabled for the task.
- **Threshold Alarm Settings**—Displays threshold alarm settings. If you enabled the Threshold Alarm feature, the page shows the **Threshold Alarm Settings** configuration parameters. The parameters include:
 - **Trigger**—Specifies the condition under which the threshold alarm is triggered. The condition has two configuration parameters, the time interval and the number of times that the threshold must be exceeded.
 - **Threshold**—Specifies the traffic threshold. When the alarm trigger condition is met, a threshold alarm is generated.
 - **Severity**—Specifies the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specifies the time interval in which a triggered alarm is not sent again.
- **Interface Information**—Identifies all interfaces configured for reporting in the associated application traffic analysis task.

- o **Probe Information**—Identifies all probes configured for reporting in the associated application traffic analysis task.
- 4. Click **Back** to return to the **Traffic Analysis Task List**.

Adding an application traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.

The **Add Traffic Analysis Task** page opens.
4. Next to **Application** on the **Select Task Type** area, click the option to add an application traffic analysis task.
5. Click **Next**.

The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.

The task name must be unique. The name you assign to a task is the link to the task reports. Therefore, assign descriptive and useful names to a task that helps you navigate to reports quickly and easily.
7. Enter a description for this task in the **Task Description** field.
8. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.

Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
9. Next to the **Reader** field, click **Select** to select the operator groups that have access to the analysis and reports provided by this application task.

The **Operator Group List** dialog box opens.

 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.
 - b. In the upper left corner of the column label field for all boxes, select the check box to select all operator groups.
 - c. Click **OK** to accept your operator group selection.

The operator groups you selected are displayed in the **Reader** field.
10. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; otherwise, select **Disable** to disable the Baseline Analysis feature.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
11. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.

NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.

12. Configure the baseline threshold settings.

- o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
- o **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
- o **Threshold**—Specify the traffic percentage threshold that must be met before NTA generates an alarm.
- o **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- o **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

13. To add applications to the task, click **Select** next to the **Application List** field.

The **Query Applications** dialog box displays an empty **Application List** in the lower portion of the dialog box.

14. To select applications to add to your task, you must first query the **Application List** as follows:

- a. **Application**—In the **Application** field, enter a partial or complete name for the applications for which you want to search.
- b. **Pre-defined**—Do one of the following:
 - From the **Pre-defined** list, select **Yes** to search for applications that are predefined.
 - From the list, select **No** to filter for applications that are user-defined.
 - Select **Not limited** to include system or predefined and user-defined applications.
- c. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area. To display the full **Application List**, click **Query** without entering any search criteria.
- d. Select the check boxes next to the applications you want to add to the application traffic analysis task. If the application you want to add does not exist, add it to NTA. For more information on adding applications to NTA, see "[Managing applications](#)."
- e. Click **OK** to add the applications to the application traffic analysis task you want to create. The applications you selected are displayed in the **Application List**.

You can add one or more applications to an application traffic analysis task. However, you must add at least one and no more than 50 applications per task.

For information about organizing application into tasks, see "[Application traffic analysis configuration considerations](#)."

15. From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure, and select **Disable** if you do not want to generate alarms.

If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.

16. Configure the threshold alarm settings.

- **Trigger**—Configure the condition under which the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
 - **Threshold**—Specify the threshold value or amount of the traffic that must be exceeded before NTA generates an alarm.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
17. Above the **Interface Information** list, click **Select** to select one or more interfaces that provide network flow data.
- The **Add Interface** page opens.
- To add interfaces, you can obtain them automatically or configure them manually.
- a. To add interfaces automatically to the task, click the **Obtain Automatically** tab at the top of the **Add Interface** page.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.
 - b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.
 - c. Click **OK** to accept your interface selection.

When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.
 - d. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.

The page will update to display the configuration options for manually adding an interface to a traffic analysis task.
 - e. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.
 - f. In the **Interface Alias** field, enter the alias for the interface.

Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.
 - g. From the **Device** list, select the device to which the interface belongs.

For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.

For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- h. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.

You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.

- i. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.
- j. Under the **View Management** area on the left navigation tree, click **Device View**.

The **Device List – All** is displayed. This list displays all devices in INC.

- k. Locate the device for which you want to view interface details.
- l. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.

The **Device Details** page opens.

- m. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.

The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.

- n. In the **Max. Speed** field, enter the maximum speed of the interface.
- o. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.

 IMPORTANT:

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

- p. Click **OK** to add the interface manually.

- 18. Next to the **Probe Name** field, select the check box for each probe that provides network flow data.

- 19. Click **OK** to create the application traffic analysis task.

After you create an application traffic analysis task, NTA creates an entry called  **Application Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the application traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon >>> next to  **Application Traffic Analysis Task**. The **Application Traffic Analysis Task** shortcut menu displays all application traffic analysis tasks created in NTA. Click the name of a task to view the application traffic analysis report of the task.

For more information about accessing and viewing application traffic analysis reports, see "[Viewing application traffic analysis reports](#)."

Modifying an application traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  for the task you want to modify.
The **Modify Traffic Analysis Task** page opens.
4. In the **Task Name** field, modify the name for this task.
The task name must be unique.
5. In the **Task Description** field, modify the description for this task.
6. From the **Server** list, select a new NTA, NetStream, NetFlow, or sFlow collection server.
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add new operator groups that have access to the analysis and reports provided by this application task, click **Select** next to the **Reader** field.
The **Operator Group List** dialog box opens.
 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
 - b. Click **OK** to accept your operator group selection.
The operator groups you selected are displayed in the **Reader** field.
 - c. In the **Reader** field, highlight the groups you want to remove to revoke operator group access to the results of this traffic analysis task.
 - d. Click **Delete**.
 - e. Click **OK** to confirm the deletion of the selected operator groups from the task.
The **Reader** list is updated to reflect the deleted operator group changes.
8. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; otherwise, select **Disable** to disable the Baseline Analysis feature.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
9. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.

NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.
10. Configure the baseline threshold settings.
 - o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.

- **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
- **Threshold**—Specify the traffic percentage threshold that must be met before NTA generates an alarm.
- **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

11. To add more applications to the task, click **Select** next to the **Application List** field. However, you must have at least one application and no more than 50 applications configured for each task.

For information about organizing application into tasks, see "[Application traffic analysis configuration considerations](#)."

The **Query Applications** dialog box displays an empty **Application List** in the lower portion of the dialog box.

To select applications to add to your task, you must first query the **Application List** as follows:

12. In the **Query Applications** area of the dialog box, specify one or more of the following search criteria:
- a. **Application**—In the **Application** field, enter a partial or complete name for the applications for which you want to search.
 - b. **Pre-defined**—Do one of the following:
 - From the **Pre-defined** list, select **Yes** to search for applications that are predefined.
 - From the list, select **No** to filter for applications that are user-defined.
 - Select **Not limited** to include system or predefined and user-defined applications.
 - c. To display the full **Application List**, click **Query** without entering any search criteria.

If the application you want to add does not exist in the **Application List**, add it as a user-defined application. For more information on adding applications to NTA, see "[Managing applications](#)."
 - d. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area. If the application you want to add does not exist, add it to NTA. For more information on adding applications to NTA, see "[Managing applications](#)."
 - e. Select the check boxes next to the applications you want to add to the application traffic analysis task.
 - f. Click **OK** to add the applications to the application traffic analysis task you want to create.

The applications you selected are displayed in the **Application List**.
 - g. To delete an application from the list, highlight the applications you want to delete.
 - h. Click **Delete** next to the **Application List** field.
 - i. Click **OK** to confirm the deletion of the selected applications.

13. From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure, and select **Disable** if you do not want to generate alarms.

If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.

14. Configure the threshold alarm settings.

- **Trigger**—Configure the condition under which the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
- **Threshold**—Specify the threshold value or amount of the traffic that must be exceeded before NTA generates an alarm.
- **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

15. Above the **Interface Information** list, click **Select** to select one or more interfaces that provide network flow data.

The **Add Interface** page opens.

To add interfaces, you can obtain them automatically or configure them manually.

- a. To add interfaces automatically to the task, click the **Obtain Automatically** tab at the top of the **Add Interface** page.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.
- c. Click **OK** to accept your interface selection.
- When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.
- d. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.
- The page will update to display the configuration options for manually adding an interface to a traffic analysis task.
- e. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.

- f. In the **Interface Alias** field, enter the alias for the interface.
Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.
- g. From the **Device** list, select the device to which the interface belongs.
For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.
For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."
The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.
- h. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.
You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.
- i. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.
- j. Under the **View Management** area on the left navigation tree, click **Device View**.
The **Device List – All** is displayed. This list displays all devices in INC.
- k. Locate the device for which you want to view interface details.
- l. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.
The **Device Details** page opens.
- m. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.
The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.
- n. In the **Max. Speed** field, enter the maximum speed of the interface.
- o. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.

 IMPORTANT:

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

- p. Click **OK** to add the interface manually.
16. To delete the interface, click the **Delete** icon  for the interface you want to delete.
17. To modify the interface name and interface speed, click the **Modify** icon  for the interface you want to modify.
This field contains a link to the **Modify Interface Configuration** page for the associated interface.
18. Next to the **Probe Name** field, select the check box for each probe that provides network flow data.
Leave the check box unselected if you do not want to analyze the network flow data for that probe.
19. Click **OK** to accept your modifications to the application traffic analysis task.

Deleting an application traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the task you want to delete.
4. Click **OK** to confirm the deletion of the selected application traffic analysis task.
The **Traffic Analysis Task List** reflects the deletion of the selected task.

Viewing application traffic analysis reports

NTA provides several levels of reporting for all application tasks:

- Summarized reports for all tasks
- Detailed reports for an individual task
- More detailed reports for an application within a task

All reports can be accessed by clicking the highest level entry of the left navigation tree under the **Traffic Analysis and Audit** area. To view summarized reporting for all application tasks, click the  **Application Traffic Analysis Task** entry of the left navigation tree.

NTA also provides more detailed reporting for individual application traffic analysis task. NTA groups individual tasks by type. All application tasks can be found on the **Application Traffic Analysis Task** menu.

To view the **Application Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to  **Application Traffic Analysis Task**. The shortcut menu displays all application traffic analysis tasks created in NTA. Click the name of a task to view the application traffic analysis report of the task.

This section describes the reporting options available for application traffic analysis tasks. It also describes the process for navigating to application traffic analysis tasks, the summary reports available for application tasks, and the reports and features available for a traffic analysis task.

Navigating to the application traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Under the **Traffic Analysis and Audit** area of the left navigation tree, click the  **Application Traffic Analysis Task** entry under the **Traffic Analysis and Audit** area of the left navigation tree.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to  **Application Traffic Analysis Task**.
The **Application Traffic Analysis Task** menu displays all application traffic analysis tasks created in NTA. Click the name of a task to view the application traffic analysis report of the task.

Summary reports for all application tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **Application Traffic Analysis Task** entry of the left navigation tree

under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

Average Rate (Last 1 Hour)

The **Average Rate** bar graph summarizes traffic rates for all applications in every application traffic analysis task, grouped by application traffic analysis task. You can access this graph by clicking the  **Application Traffic Analysis Task** entry of the left navigation tree. The bars in the graph link to the reports for the selected task.

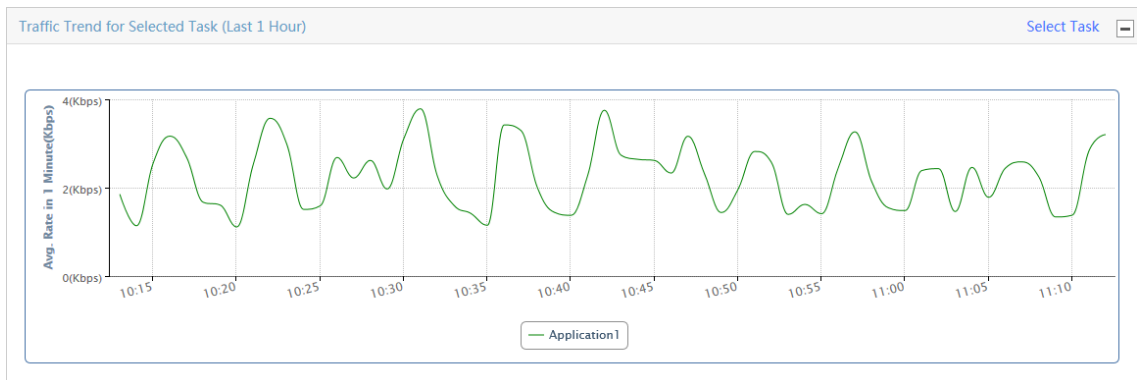
Figure 129 Application Task Average Rate (Last 1 Hour)



Traffic Trend For Selected Task (Last 1 Hour)

The **Traffic Trend for Selected Task** line chart provides traffic trend rates for the selected application traffic analysis tasks for the last hour. You can access this chart by clicking the  **Application Traffic Analysis Task** entry of the left navigation tree.

Figure 130 Traffic Trend for Selected Task



All application tasks are graphed on this line chart until you specify a task.

1. In the upper right corner of the **Traffic Trend for Selected Task** title bar, click the **Select Task** link to select the task.
The **Choose NTA Task** dialog box opens.
2. Select the check box next to the application task for which you want to view this report.
3. Click **OK**.
The page will update to display an updated line chart for the selected application task.

Summary List (Last 1 Hour)

The **Summary List** provides traffic rates and total volume of traffic statistics summarized by application task.

1. On the left navigation tree, click the  **Application Traffic** entry icon to access the list.
Summary list contents

- **Task Name**—Contains the name of the application traffic analysis task. The contents of this field link to reports for the associated task.
 - **Traffic**—Provides the total volume of traffic observed for all applications configured for the associated application task for the last hour.
 - **Rate**—Provides the rate traffic for all applications configured for the associated task for the last hour.
2. At the top of the **Summary List**, click **Add** for a shortcut to the **Add Application Traffic Analysis Task** page.
For more information on adding application traffic analysis tasks, see ["Adding an application traffic analysis task."](#)
 3. Click **Refresh** to update the reports with the most recent data.

Detailed reports for an application traffic analysis task

NTA provides a suite of reports for viewing application data from different perspectives. Reports for applications are organized into four reporting groups: traffic, source, destination, and session.

- Traffic reports for application tasks provide overall traffic statistics and the data samples collected for the specified time period.
- Source reports provide distribution of traffic for the TopN source hosts for all applications in a task and a total traffic volume and percentage of application traffic for the TopN hosts.
- Destination reports provide distribution of traffic for the TopN destination hosts for all applications in a task as well a total traffic volume and percentage of application traffic for the TopN destination hosts.
- Session reports provide distribution of traffic for the TopN session pairs for all applications in a task as well a total traffic volume and percentage of application traffic for session pairs in a task.

Source, destination, and session reports provide detailed capabilities to traffic reports for an individual host/session pair.

Traffic reports

Traffic reports for an application traffic analysis task include the **Traffic Trend** line chart that provides average per second traffic rates for all applications in the selected traffic analysis task for the selected time range. This report also summarizes total traffic along with the average, minimum average and maximum average rate for all applications in the selected task.

The traffic reports include the **Traffic Details** list that provides the data collection samples that includes timestamp, total volume of traffic, and traffic rate in seconds for all applications in the selected task for the selected time range. You can filter reports by time range.

To view the reports for an application task, click the **Traffic** tab to view traffic reports for the selected application traffic analysis task.

Query traffic

NTA enables you to change the filter criteria for traffic reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed under the **Traffic** tab.

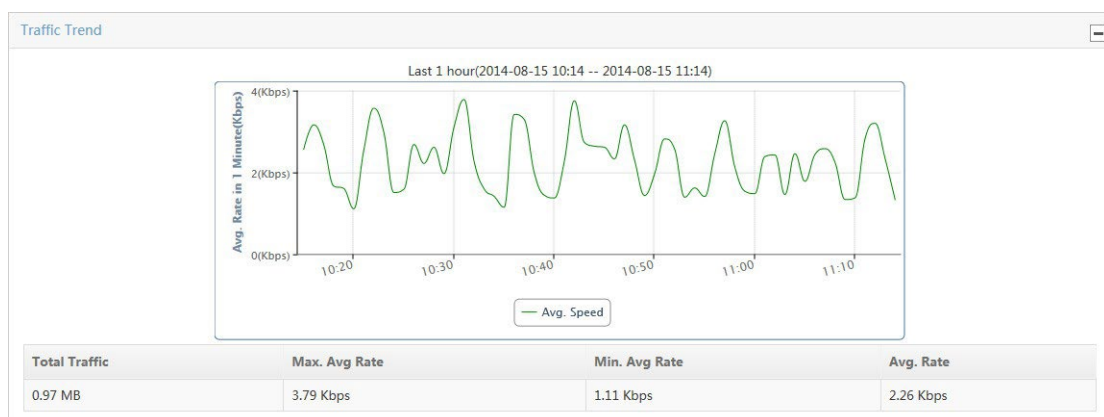
1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify the following query criteria:

- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
 5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
 - f. From **Page Range**, select the page range.
 - g. Click **Export**.

Traffic Trend – Average

The **Traffic Trend** line chart displays the average per second traffic rate for all applications in the selected traffic analysis task. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for all applications in the associated task. If more than one application exists for the selected task, these statistics reflect traffic for all applications configured in a task.

Figure 131 Traffic Trend Report



The **Trend** chart displays statistics for the previous hour.

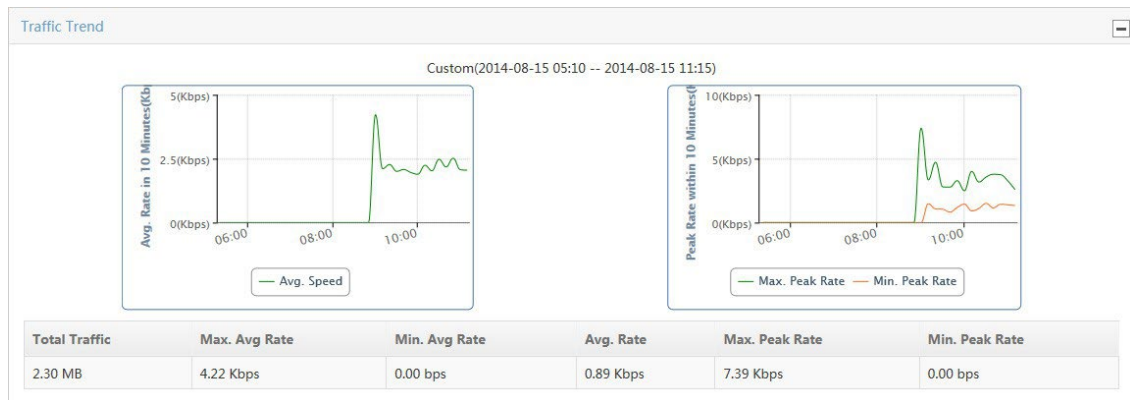
- To view data for an earlier period, click **Previous** located in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** located in the upper right corner of the **Traffic Trend** chart.

Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range. This chart contains two lines. The red line displays the maximum peak rate. The green line displays the minimum peak rate.

Figure 132 Traffic Trend – Peak Rate Report



- In the upper right corner of the **Traffic Trend** chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the **Traffic Trend** chart, click **Next** to view data for a later period.

For more information on enabling Peak Traffic Analysis, see "[Configuring NTA traffic analysis parameters.](#)"

Traffic Details

The **Traffic Details** list provides the data collection samples for traffic statistics for all applications in the task based on the report time range. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic for the selected time range.

Figure 133 Traffic Details

Traffic Details		
Time	Traffic	Rate
2014-08-15 10:17:00	19.68 KB	2.69 Kbps
2014-08-15 10:18:00	12.22 KB	1.67 Kbps
2014-08-15 10:19:00	11.80 KB	1.61 Kbps
2014-08-15 10:20:00	8.14 KB	1.11 Kbps
2014-08-15 10:21:00	18.63 KB	2.54 Kbps
2014-08-15 10:22:00	26.17 KB	3.57 Kbps
2014-08-15 10:23:00	21.83 KB	2.98 Kbps

Source reports

Source reports include the **TopN Traffic Report for Source Host** pie chart, which displays the distribution of traffic for the TopN source hosts for all applications in the selected traffic analysis task for the selected time range. This report also contains a link to traffic reports for the selected host.

Source reports also include the **TopN Traffic List for Source Host**, which provides a list of the TopN source hosts measured by volume of traffic observed on all applications in the selected application traffic analysis task for the selected time range. This report also contains a link to reports for the selected source host.

The host query icon  next to the source IP address is a link for initiating a host query and the results of the host query. As with all report types for an application task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an application task, click the **Source** tab to view traffic reports for the selected application traffic analysis task.

Query source hosts

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed under the **Source** tab.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/6
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

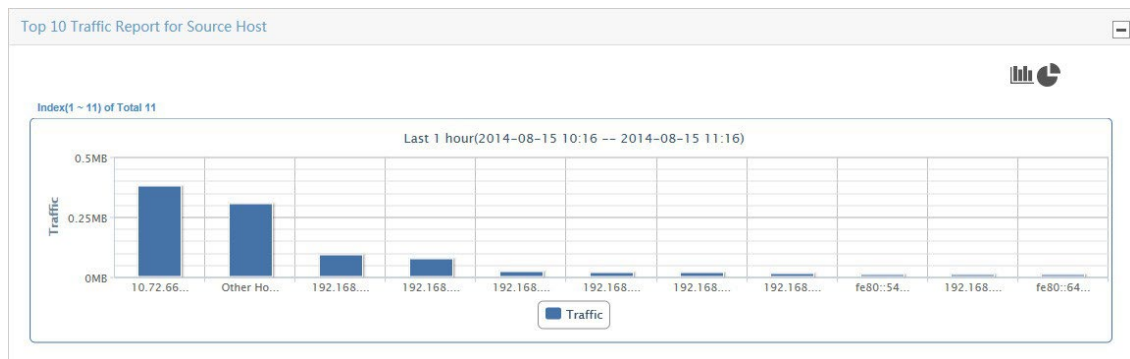
- a. To print this report, click the **Print** icon  on the toolbar.
- b. From **Page Range**, select the page range.
- c. To export the data, click **Export**.
- d. To export this report, click the **Export** icon  on the toolbar.
- e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
- f. From **Page Range**, select the page range.
- g. Click **Export**.

TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host** bar chart displays the TopN source hosts with the most inbound/outbound application traffic in a certain period of time in a selected application traffic analysis task. Click a bar in the chart to view the traffic analysis report of each source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the traffic distribution of the TopN source hosts for all applications in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

Figure 134 TopN Traffic Report for Source Host



TopN Traffic List for Source Host

The **TopN Traffic List for Source Host** provides a list of the TopN source hosts measured by volume of traffic observed for all applications in the selected application traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source host, and the percentage of all observed traffic generated by the source host.

The IP address is a link to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the host query.

Figure 135 TopN Traffic List for Source Host

Top 10 Traffic List for Source Host			Generate Chart
Source	Traffic	Percentage	
10.72.66.36	0.38 MB	39.71%	
192.168.40.100	94.85 KB	9.72%	
192.168.40.207	77.86 KB	7.97%	
192.168.100.2	23.71 KB	2.43%	
192.168.40.23	19.55 KB	2.00%	
192.168.40.175	18.40 KB	1.88%	
192.168.40.190	12.44 KB	1.27%	
fe80::546f:1ccd:907d:a9f0	10.66 KB	1.09%	
192.168.100.237	10.16 KB	1.04%	
fe80::641b:6318:79e3:567	9.81 KB	1.01%	
Other Hosts	0.30 MB	31.87%	

Source Host Traffic Trend Report

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Source Host Traffic Trend Report** line chart provides the average rate of traffic for the selected source host. By default, the **Source Host Traffic Trend Report** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Source** host report page, click **Back**.

Figure 136 Source Host Traffic Trend Report



TopN Destination Hosts Communicating with Source Host

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP address, the volume of traffic sent and received between this source host and the destination, and the percentage of all traffic observed for this source host.

Figure 137 TopN Destination Hosts Communicating with Source Host

Traffic Details		
Top 10 Destination Hosts Communicating with the Source Host		
Destination	Traffic	Percentage
 192.168.40.100	0.14 MB	36.07% 
 192.168.40.175	0.10 MB	26.92% 
 192.168.40.211	29.33 KB	7.56% 
 192.168.40.40	28.60 KB	7.38% 
 192.168.40.170	28.49 KB	7.35% 
 192.168.40.24	14.36 KB	3.70% 
 192.168.40.150	11.43 KB	2.95% 
 192.168.40.151	6.66 KB	1.72% 
 192.168.40.23	5.82 KB	1.50% 
 192.168.40.248	5.73 KB	1.48% 
Other Hosts	13.08 KB	3.37% 

Destination reports

Destination reports include the **TopN Traffic Report for Destination Host** pie chart, which displays the distribution of inbound traffic observed for the TopN destination hosts for all applications in the selected traffic analysis task for the selected time range. This report also contains a link to traffic reports for the selected host.

Destination reports also include the **TopN Traffic List for Destination Host**, which provides a list of the TopN destination hosts measured by volume of traffic observed on all applications in the selected application traffic analysis task for the selected time range. This report also contains a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and the results of the host query.

As with all report types for an application task, NTA provides a query option for filtering reports based on criteria you define.

To view the reports for an application task, click the **Destination** tab to view traffic reports for the selected application traffic analysis task.

Query destination hosts

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed under the **Destination** tab.

1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the destination report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
 - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

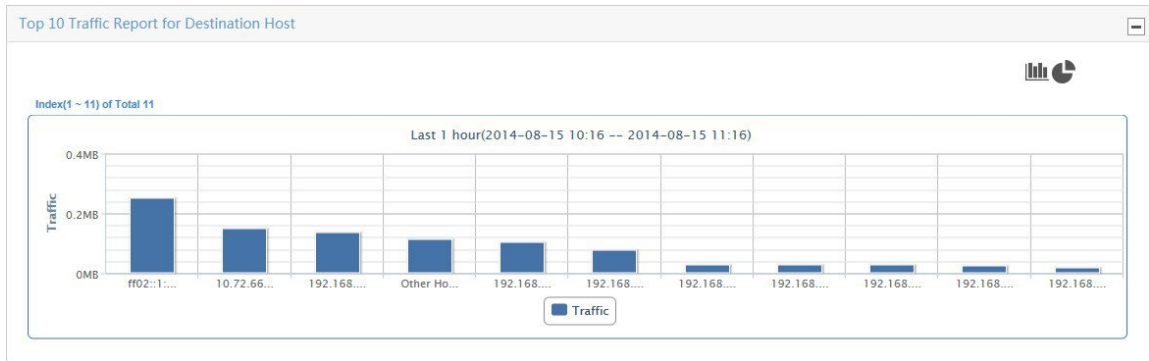
- a. To print this report, click the **Print** icon  on the toolbar.
- b. From **Page Range**, select the page range.
- c. To export the data, click **Export**.
- d. To export this report, click the **Export** icon  on the toolbar.
- e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**
 - **CSV**
 - **DOCX**
 - **RTF**
 - **XLSX**
 - **PPTX**
 - **HTML**
 - **JRXML**
- f. From **Page Range**, select the page range.
- g. Click **Export**.

TopN Traffic Report by Destination Host

The **TopN Traffic Report for Destination Host** bar chart displays the TopN destination hosts with the most inbound/outbound application traffic in a certain period of time in a selected application traffic analysis task. Click a bar for a destination host in the bar chart to view the traffic analysis report of the destination host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the traffic distribution of TopN destination hosts for all applications in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

Figure 138 TopN Traffic Report for Destination Host



TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host** provides a list of the TopN destination hosts measured by volume of traffic observed for all applications in the selected application traffic analysis task for the selected time range. This list includes the host IP address, total volume of traffic generated by the associated destination host, and the percentage of all observed traffic generated by the destination host.

The IP address is a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and a link to the results of the host query.

Figure 139 TopN Traffic List for Destination Host

Top 10 Traffic List for Destination Host			Generate Chart
Destination	Traffic	Percentage	
 ff02::1:2	0.25 MB	26.39%	
 10.72.66.36	0.15 MB	15.48%	
 192.168.40.100	0.14 MB	14.38%	
 192.168.40.175	0.10 MB	10.69%	
 192.168.40.215	77.61 KB	7.95%	
 192.168.40.211	29.33 KB	3.00%	
 192.168.40.40	28.60 KB	2.93%	
 192.168.40.170	28.49 KB	2.92%	
 192.168.100.2	23.83 KB	2.44%	
 192.168.100.1	18.28 KB	1.87%	
Other Hosts	0.11 MB	11.94%	

Destination Host Traffic Trend Report

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Destination Host Traffic Trend Report** line chart provides the average rate of traffic for the selected destination host. By default, the **Destination Host Traffic Trend Report** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Destination** host report page, click **Back**.

Figure 140 Destination Host Traffic Trend Report



TopN Source Hosts Communicating with the Destination Host

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.

Figure 141 TopN Source Hosts Communicating with the Destination Host

Traffic Details

Top 10 Source Hosts Communicating with the Destination Host

Source	Traffic	Percentage
fe80::546f1ccd:907d:a9f0	10.66 KB	4.14%
fe80::641b:6318:79e3:567	9.81 KB	3.81%
fe80::b187:f96a:3a4d:2923	9.66 KB	3.75%
fe80::a918:20a6:ba9a:93b8	9.66 KB	3.75%
fe80::98ef:93c4:1cca:5063	9.66 KB	3.75%
fe80::2053:a8b:2cb5:f99	9.66 KB	3.75%
fe80::c4a1:25dd:67c4:a66e	9.51 KB	3.69%
fe80::4c3d:eff6:549:dd96	9.08 KB	3.53%
fe80::684c:49f0:6122:3fd0	9.05 KB	3.51%
fe80::e090:79fd:8b63:99d5	8.63 KB	3.35%
Other Hosts	0.16 MB	62.98%

Session reports

Session reports include the **TopN Traffic Report for Session Host** pie chart, which shows the distribution of traffic for the TopN session hosts for all applications in the selected traffic analysis task for the selected time period. This report also contains a link to traffic reports for the selected host.

Session reports also include the **TopN Traffic List for Session Host**, which provides a list of the TopN session hosts measured by volume of traffic observed for all applications in the selected application traffic analysis task for the selected time period. This report also contains a link to reports for the selected session host.

The host query icon  next to **Session** IP address is a link for initiating a host query and the results of the host query. As with all report types for an application task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for an application task, click the **Session** tab to view traffic reports for the selected application traffic analysis task.

Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify the following query criteria:
 - o **Source Host**—Enter the IP address or address range in the **Source Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
Example of a valid IP address:
10.153.89.10
Example of a valid network/subnet mask in dotted decimal notation:
10.153.89.0/255.255.255.0
Example of a valid network/subnet mask using CIDR notation:
10.153.89.0/24
Example of a valid IPv6 address:
a001:410:0:1::1
Example of a valid IPv6 address and subnet mask using CIDR notation:
a001:410:0:1::1/64
 - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
 - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
 - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
 - a. To print this report, click the **Print** icon  on the toolbar.
 - b. From **Page Range**, select the page range.
 - c. To export the data, click **Export**.
 - d. To export this report, click the **Export** icon  on the toolbar.
 - e. From the **File Format** list, select the export file format. Options are:
 - **PDF**
 - **XLS**

- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

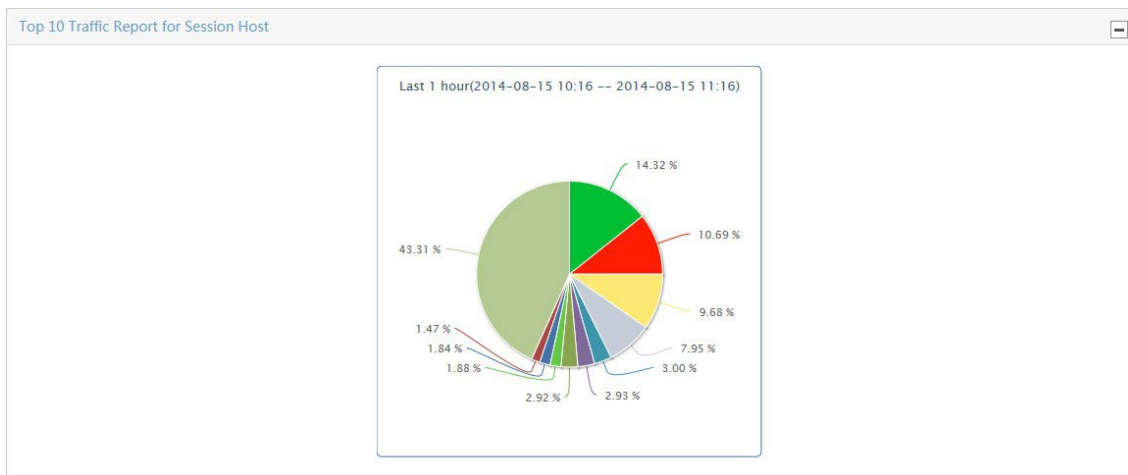
f. From **Page Range**, select the page range.

g. Click **Export**.

TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host** pie chart displays the distribution of inbound traffic for TopN source and destination session pairs for all applications in the selected traffic analysis task for the selected time period. Each pie chart slice is a link to traffic reports for the select source and destination session pair.

Figure 142 TopN Traffic Report for Session Host



TopN Traffic List for Session Host

The **TopN Traffic List for Session Host** provides a list of the TopN source and destination session pairs measured by volume of traffic observed for all applications in the selected application traffic analysis task for the selected time range. This list includes the source and destination host IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair.

The icon  in the **Details** field is a link for viewing reports for the selected session or source/destination pair. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link to the results of the host query.

Figure 143 TopN Traffic List for Session Host

Top 10 Traffic List for Session Host					Generate Chart
Source Host	Destination Host	Traffic	Percentage	Details	Topology
192.168.3.139	192.168.3.255	1.46 MB	33.60%		
fe80::50ca:4f7e:f6f5:8875	ff02::1:3	0.36 MB	8.31%		
192.168.3.55	224.0.0.252	0.36 MB	8.20%		
fe80::ec30:383c:c5bc:5cec	ff02::1:2	0.32 MB	7.39%		
192.168.3.55	192.168.3.255	0.27 MB	6.30%		
fe80::5486:1eb4:4ff9:9a7	ff02::1:3	0.25 MB	5.78%		
fe80::99c3:e650:f53a:b3e3	ff02::1:2	0.17 MB	3.89%		
fe80::2da4:a3e1:647a:e7e	ff02::1:3	0.17 MB	3.85%		
fe80::80e3:d8e9:5b5b:dfc	ff02::1:2	0.15 MB	3.48%		
fe80::51ad:acdd:8319:470	ff02::1:2	0.15 MB	3.41%		
Other Hosts	Other Hosts	0.69 MB	15.77%		

Session Traffic Trend Report

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **Session Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Traffic Trend Report** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Session** report page, click **Back**.

Figure 144 Session Traffic Trend Report



Session Traffic List

To view this report for an application task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon on the **TopN Traffic List for Session Host**.

The **Session Traffic List** displays the data samples for the selected source and destination pair. This list displays the date and timestamp for the data collection, the total volume of traffic observed for the session pair and the rate of traffic for the collection interval.

Figure 145 Session Traffic List

Session Traffic List 10.72.66.36 >> 192.168.40.100		
Time	Traffic	Rate
2014-08-15 10:20:00	20.36 KB	0.28 Kbps
2014-08-15 10:30:00	24.35 KB	0.33 Kbps
2014-08-15 10:40:00	25.93 KB	0.35 Kbps
2014-08-15 10:50:00	22.15 KB	0.30 Kbps
2014-08-15 11:00:00	21.24 KB	0.29 Kbps
2014-08-15 11:10:00	25.81 KB	0.35 Kbps

Session host topology

To view the topology between the source host and the destination host, click the **Topology** icon  on the **TopN Traffic List for Session Host**.

Host monitoring

This chapter describes host monitoring in NTA, including how NTA analyzes network flow records to report on network traffic from a host perspective. It provides an overview of how NTA looks at network flow data from the viewpoint of hosts; how it reviews the report structure for host traffic reports; and how it manages configuration issues around host analysis tasks and the reports they generate. This chapter describes the process for adding host traffic analysis tasks, and adding, modifying, and deleting host tasks in NTA. It surveys the summary reports for all host tasks. Finally, it looks at the more detailed reports for an individual host traffic analysis task.

Host traffic analysis overview

Host traffic analysis tasks analyze network flow data by the IP addresses of hosts configured in a host traffic analysis task. NTA parses all network flow data and provides various statistical views of traffic that was observed for the hosts configured in a host traffic analysis task. For example, NTA provides application information reporting for a given host or set of hosts. NTA displays the rate of application traffic attributed to the specified hosts observed sending or receiving application traffic. Because analyses based on hosts are not tied to a specific interface, device, or probe network flow data sources, host reports provide visibility for all areas of the network that generate network flow records.

The NTA host traffic analysis tasks provide traffic statistics for all hosts configured in the host traffic analysis tasks. In general, the host traffic reports include rate of traffic for all hosts in all configured host traffic analysis tasks and for the hosts in a task. Host statistics include per-second traffic rate for each host; for application traffic observed for the configured host; and for distribution of host traffic generated by source host, destination host, or by a session or source/destination host pair. These reports are organized into multiple layers from summarized information for tasks to detailed reporting for specific hosts configured for a host traffic analysis task.

Host traffic analysis reporting overview

After you create the first host traffic analysis task, NTA creates an entry called  **Host Traffic Analysis Task** under the **Traffic Analysis and Audit** area on the left navigation tree.

Click **Host Traffic Analysis Task** on the left navigation tree to view the summary report for all host traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to  **Host Traffic Analysis Task**. The **Host Traffic Analysis Task** shortcut menu displays all host traffic analysis tasks created in NTA. Click the name of a task to view the host traffic analysis report of the task.

The summary host traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides summarized average rate per second reporting for all hosts specified in all host traffic analysis tasks summarized by task name. Each bar in the graph is a link to more detailed reporting for the selected task, including reporting for traffic rates, application, source, destination, and session statistics. Each of these detailed report types also include several reports:
 - **Traffic**—Reports found under the **Traffic** tab for host reporting include traffic trends that display the average rate per second attributed to the hosts in the selected task and the data samples for the selected host task.
 - **Application**—Reports found under the **Application** tab for host reporting include a tabular report showing volume, rate and percentage of application traffic summarized for all hosts in the task and a graph showing average rate of traffic by application for all hosts.

- **Source**—Reports found under the **Source** tab for host reporting include inbound and outbound reports.
 - **Inbound report**—Includes a pie chart showing the percentage of traffic sent from the TopN source hosts to the hosts configured in the selected task. It also includes a tabular list showing volume and percentage of traffic generated for each of the TopN source hosts that generated traffic to the hosts that configured in the selected task.
 - **Outbound report**—Includes a pie chart showing the percentage of traffic sent from the hosts configured in the selected task to any other hosts. It also includes a tabular list showing volume and percentage of traffic generated for each of the TopN source hosts that configured in the selected task.

The contents of the inbound and outbound pie chart link to more detailed reporting for the selected host.

- **Destination**—Reports found under the **Destination** tab for host reporting include inbound and outbound reports. The contents of the inbound and outbound pie chart link to more detailed reporting for the selected host.
 - **Inbound report**—Includes a pie chart showing the percentage of traffic sent to the hosts configured in the selected task by any other hosts. Also included is a tabular report showing volume and percentage of traffic sent to each of the TopN destination hosts that configured in the selected task by any other hosts.
 - **Outbound report**—Includes a pie chart showing the percentage of traffic sent to the TopN destination hosts by the hosts configured in the task. Also included is a tabular report showing volume and percentage of traffic sent to each of the TopN destination hosts by the hosts that configured in the selected task.

The contents of the inbound and outbound pie chart link to more detailed reporting for the selected host.

- **Session**—Reports found under the **Session** tab for host reporting include inbound and outbound reports. The contents of the pie chart link to more detailed reporting for the selected sessions.
 - **Inbound report**—Includes a pie chart, which displays the percentage of traffic generated by the TopN source/destination pairs with the destination hosts configured in the selected task, and a table, which displays the volume and percentage of traffic generated for each of the TopN source/destination pairs with the destination hosts configured in the selected task.
 - **Outbound report**—Includes a pie chart, which displays the percentage of traffic generated by the TopN source/destination pairs with source hosts configured in the selected task, and a table, which displays the volume and percentage of traffic generated for each of the TopN source/destination pairs with source hosts configured in the selected task.

The contents of the pie chart link to more detailed reporting for the selected sessions.

- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—This area has two charts:
 - A line chart that provides per second average traffic rate summarized by host traffic analysis task for the host tasks you select.
 - A pie chart that provides distribution statistics for application traffic for all hosts in the task.
- **Summary List (Last 1 Hour)**—This list provides per second traffic rate summarized by host traffic analysis task. This list provides navigation to more detailed host reporting for the selected task.

Host traffic analysis configuration considerations

This section explains configuration considerations and how to maximize the NTA host reporting features. You must consider several things when adding hosts to a task —the most important of which is how you select the hosts that belong to each task. Additional considerations follow:

- By default, NTA does not monitor any hosts. You must create a task for every host or group of hosts on which you want to monitor and report.
- You must enable network flow data on the devices and for the interfaces on them for those locations on your network where you know host traffic for can be captured. Then, you must add these devices and probes to NTA using the features described in "[Device management](#)" and "[Probe management](#)." NTA then summarizes application data for all devices and probes on which it observes the application traffic.
- NTA provides summarized host reporting based on the way you have grouped hosts into tasks. Consider how you want to summarize, access, and view host data. Then, structure your tasks around it. For example, create a host task called **NetMgmtHosts** and add all hosts used in your environment that support network management. NTA summarizes all traffic observed for all hosts into the group **NetMgmtHosts** and attribute traffic in the reports to the task name you have configured.

Managing host traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until you create a task, NTA does not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need. This section describes the process for adding, modifying, or removing host traffic analysis tasks in NTA.

Viewing a traffic analysis task

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view the NTA traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

Task list contents

- **Task Name**—Contains the name of the task. The contents of this field link to the **Traffic Analysis Task Details** page for the associated task.
- **Task Description**—Contains the **description** for the associated task.
- **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**

- **Baseline Analysis**—This parameter is displayed when the Baseline Analysis feature is enabled in the NAT parameters. The Baseline Analysis feature provides an additional layer of analysis to reports provided by NTA by including baseline trend data when data has been collected for a minimum of one week.
 - **Modify**—Contains an icon  for modifying the associated task.
 - **Delete**—Contains an icon  for deleting the associated task.
3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** in the upper left corner of the **Traffic Analysis Task List**.
- You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

Viewing host traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. In the **Task Name** field of the **Traffic Analysis Task List** whose **Task Type** is **Host**, click the contents to view the details for an individual task.
Traffic analysis task details page
 - **Task Name**—Contains the name of the task.
 - **Task Description**—Contains the description for the associated task.
 - **Server**—Contains the name or IP address of the NTA server.
 - **Task Type**—Options are:
 - **Interface**
 - **VLAN/VXLAN**
 - **Probe**
 - **Application**
 - **Host**
 - **VPN**
 - **Inter-Business**
 - **BGP AS**
 - **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by the associated traffic analysis task.
 - **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled on the NTA server. For more information about configuration options for the NTA server, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
 - **Enable Automatic Anomaly Detection Based On The Baseline**—Indicates whether automatic detection of traffic anomaly based on the baseline is enabled for the task. This parameter is displayed only when baseline analysis is enabled.
 - **Baseline Threshold Setting**—Displays parameters of the baseline threshold setting. This area is displayed only when baseline analysis is enabled. The baseline threshold setting includes the following parameters:
 - **Baseline Upper/Lower Threshold**—Indicates the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.

- **Trigger**—Indicates under what condition the threshold is triggered. This condition has two configuration parameters, the time interval, and the number of times that the threshold must be met.
 - **In Threshold**—Indicates the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
 - **Out Threshold**—Indicates the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
 - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
- **IP Stat. Direction**—Identifies whether the specified IP addresses are included. **Include** indicates that IP addresses in the **Host IP List** are included. **Exclude** indicates that the IP addresses in the **Host IP List** are excluded.
 - **Host IP List**—Contains the IP address for all hosts configured for this traffic analysis task.
 - **Application List**—Identifies all applications configured for the associated traffic analysis task.
 - **Threshold Alarm**—Indicates whether the Threshold Alarm feature is enabled for the task.
 - **Threshold Alarm Settings**—Displays parameters for the threshold alarm setting. If you enabled the Threshold Alarm feature, the page shows the **Threshold Alarm Settings** configuration parameters. The parameters include:
 - **Direction**—Indicates the direction you want to apply the threshold, **In**, **Out** or **In/Out**.
 - **Trigger**—Indicates under what conditions the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
 - **In Threshold**—Indicates the threshold value or amount of the inbound traffic that must be exceeded before NTA generates an alarm. This field is displayed only when **Direction** is set to **In** or **In/Out**.
 - **Out Threshold**—Indicates the threshold value or amount of the outbound traffic that must be exceeded before NTA generates an alarm. This field is displayed only when **Direction** is set to **Out** or **In/Out**.
 - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
 - **Interface Information**—Identifies all interfaces configured for reporting in the associated application traffic analysis task.
 - **Probe Information**—Identifies all probes configured for reporting in the associated application traffic analysis task.
4. Click **Back** to return to the **Traffic Analysis Task List**.

Adding a host traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.
The **Add Traffic Analysis Task** page is displayed.

4. To add a host traffic analysis task, click the option next to **Host** on the **Select Task Type** area.
5. Click **Next**.

The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.

The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. Enter a description for this task in the **Task Description** field.
8. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.

Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
9. Next to the **Reader** field, click **Select** to select the operator groups that have access to the analysis and reports provided by this host task.

The **Operator Group List** dialog box opens.

 - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.
 - b. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
 - c. Click **OK** to accept your operator group selection. The selected operator groups are displayed in the **Reader** field.
10. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; select **Disable** to disable the Baseline Analysis feature.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week of collection. Statistics are adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
11. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.

NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.
12. Configure the baseline threshold settings.
 - o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
 - o **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
 - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
 - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.

- **In Threshold**—Specify the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
 - **Out Threshold**—Specify the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
 - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
 - **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
- 13.** To include traffic from one or more hosts or address ranges, select **Include** from the **IP Stat. Direction** list.
- To exclude traffic from one or more hosts or address ranges, select **Exclude**. The default setting is **Include**.
- You can add one or more hosts or address ranges to a task. However, you must have at least one host defined and no more than 50 host entries defined for each task.
- For information about organizing application into tasks, see "[Host traffic analysis configuration considerations](#)."
- You can configure a host traffic analysis task to include or exclude traffic for one or more hosts defined by IP address. You can enter a range of IP addresses to be included or excluded in the analysis. Or, you can enter a combination of IP host addresses and IP address ranges to be included or excluded in the analysis. No two addresses or address ranges entered in the **Host IP** field can overlap.
- 14.** In the **Host IP** field, enter the IP address for a single host using dotted decimal notation.
- Example of a valid IP address:
- ```
10.153.89.10
```
- Example of a valid network/subnet mask in dotted decimal notation:
- ```
10.153.89.0/255.255.255.0
```
- Example of a valid network/subnet mask using CIDR notation:
- ```
10.153.89.0/24
```
- Example of a valid IPv6 address:
- ```
a001:410:0:1::1
```
- Example of a valid IPv6 address and subnet mask using CIDR notation:
- ```
a001:410:0:1::1/64
```
- 15.** Next to the **Host IP** field, click **Add**.
- The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.
- You also configure host analysis tasks to include applications. You can have more than one application configured for a host traffic analysis tasks. Traffic data for the selected applications is included in report processing and presentation. You must have at least one application and no more than 50 applications configured for a host traffic analysis task.
- 16.** Next to the **Application List** field, click **Select** to add applications to the task.
- The **Query Applications** dialog box displays an empty **Application List**.
- To select applications to add to your task, you must first query the **Application List** as follows:
- a.** Specify one or more of the following search criteria in the **Query Applications** area of the dialog box:
    - **Application**—In the **Application** field, enter a partial or complete name for the applications for which you want to search.
    - **Pre-defined**—To search for predefined applications, select **Yes** from the **Pre-defined** list.

To filter for applications that are user-defined, select **No** from the list.

To include system or predefined and user-defined applications, select **Not limited**.

If the application you want to add does not exist, add it to NTA. For information on adding applications to NTA, see "[Managing applications](#)."

**b. Click **Query**.**

The query results are displayed in the **Application List** below the **Query Applications** area.

To display the full **Application List**, click **Query** without entering any search criteria.

**c. Check the boxes next to the applications to add to the host traffic analysis task.**

**d. Click **OK** to add the applications to the host traffic analysis task you want to create.**

The applications you selected are displayed in the **Application List**.

- 17. From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure, and select **Disable** if you do not want to generate alarms.**

If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.

- 18. Configure the threshold alarm settings.**

- **Direction**—Specify the direction of traffic monitoring. Options are **In**, **Out**, and **In/Out**.
- **Trigger**—Configure the condition under which the threshold is triggered. The condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
  - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
  - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
- **In Threshold**—Specify the threshold value or amount of the inbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
- **Out Threshold**—Specify the threshold value or amount of the outbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
- **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

- 19. Above the **Interface Information** list, click **Select** to select one or more interfaces that provide network flow data.**

The **Add Interface** page opens.

To add interfaces, you can obtain them automatically or configure them manually.

- a. To add interfaces automatically to the task, click the **Obtain Automatically** tab at the top of the **Add Interface** page.**

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.

- c. Click **OK** to accept your interface selection.

When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.

- d. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.

The page will update to display the configuration options for manually adding an interface to a traffic analysis task.

- e. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.

- f. In the **Interface Alias** field, enter the alias for the interface.

Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.

- g. From the **Device** list, select the device to which the interface belongs.

For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.

For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- h. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.

You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.

- i. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.

- j. Under the **View Management** area on the left navigation tree, click **Device View**.

The **Device List – All** is displayed. This list displays all devices in INC.

- k. Locate the device for which you want to view interface details.

- l. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.

The **Device Details** page opens.

- m. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.

The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.

- n. In the **Max. Speed** field, enter the maximum speed of the interface.

- o. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.

---

 **IMPORTANT:**

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

---

- p. Click **OK** to add the interface manually.
20. Next to the **Probe Name** field, select the check box for each probe that provides network flow data.
21. Click **OK** to create the host traffic analysis task.

After you create a host traffic analysis task, NTA creates an entry called  **Host Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the host traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to  **Host Traffic Analysis Task**. The **Host Traffic Analysis Task** shortcut menu displays all host traffic analysis tasks created in NTA. Click the name of a task to view the host traffic analysis report of the task.

For information about accessing and viewing host traffic analysis reports, see "[Viewing host traffic analysis reports](#)."

## Modifying a host traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  associated with the host traffic analysis task you want to modify.
4. In the **Task Name** field, modify the name for this task.  
The task name must be unique.
5. In the **Task Description** field, modify the description for this task.
6. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.  
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add new operator groups that have access to the analysis and reports provided by this host task, click **Select** next to the **Reader** field.  
The **Operator Group List** dialog box opens.
  - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.  
To select all operator groups, select the check box located in the upper left corner of the column label field for all boxes.
  - b. Click **OK** to accept your operator group selection.  
The operator groups you selected are displayed in the **Reader** field.
  - c. To revoke operator group access to the results of this traffic analysis task, highlight the groups you want to remove.
  - d. Click **Delete**.
  - e. Click **OK** to confirm the deletion of the selected operator groups from the task.  
The **Reader** list is updated to reflect the deleted operator group changes.

8. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; to disable the Baseline Analysis feature, select **Disable**.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially the baseline trendline shows statistics based on the first week's collection and is adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.

9. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.

NTA automatically detects and generates alarms for traffic anomaly according to the traffic baseline.

10. Configure the baseline threshold settings.

- **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
- **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
  - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
  - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
- **In Threshold**—Specify the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
- **Out Threshold**—Specify the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
- **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

11. From the **IP Stat**, select **Include** to include traffic from one or more hosts or address ranges; to exclude traffic from one or more hosts or address ranges, select **Exclude**. The default setting is **Include**.

You can configure a host traffic analysis task to include or exclude traffic for one or more hosts defined by IP address. You can enter a range of IP addresses to be included or exclude in the analysis. Or, enter a combination of IP host addresses and IP address ranges to be included or exclude in the analysis. No two addresses or address ranges entered in the **Host IP** field can overlap. You must configure at least one host address or address range and no more than fifty host entries for a task.

For information about organizing application into tasks, see "[Host traffic analysis configuration considerations](#)."

12. Add IP address entries in the **Host IP** field.

- a. To enter the IP address for a single host, enter the IP address using dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- b. Next to the **Host IP** field, click **Add**.

The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.

- c. To remove one or more hosts from the task, highlight the hosts and/or address ranges you want to remove.
- d. Next to the **Host IP List** field, click **Delete**.
- e. Click **OK** to confirm the deletion of the selected hosts or addresses ranges.

The **Host IP List** is updated to reflect the host or address range deletions.

Configure host analysis tasks to include applications. Traffic data for the selected applications is included in report processing and presentation.

Configure more than one application per task but you must configure at least one application and no more than fifty applications configured for a host traffic analysis task.

13. Next to the **Application List** field, click **Select** to add applications to the task.

The **Query Applications** dialog box displays an empty **Application List**.

To select applications to add to your task, you must first query the **Application List** as follows:

14. In the **Query Applications** area of the dialog box, specify one or more of the following search criteria:

- a. **Application**—Enter a partial or complete name for the applications you want to search for in the **Application** field.

- b. **Pre-defined**—To search for applications that are predefined, select **Yes** from the **Pre-defined** list.

To filter for applications that are user-defined, select **No** from the list.

To include system or predefined and user-defined applications, select **Not limited**.

- c. To display the full **Application List**, click **Query** without entering any search criteria.

If the application you want to add does not exist, add it to NTA. For information on adding applications to NTA, see "[Managing applications](#)."

- d. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.

- e. Select the check boxes next to the applications you want to add to the application traffic analysis task.

- f. Click **OK** to add the applications to the traffic analysis task you want to create.

The applications you selected are displayed in the **Application List**.

- g. To remove one or more applications from the task, highlight the applications you want to remove.

- h. Next to the **Application List** field, click **Delete**.

- i. Click **OK** to confirm the deletion of the selected applications.

The **Application List** reflects the deletions.

15. From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this task and the thresholds you configure, and select **Disable** if you do not want to generate alarms.

If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.

16. Configure the threshold alarm settings.
  - o **Direction**—Specify the direction of traffic monitoring. Options are **In**, **Out**, and **In/Out**.
  - o **Trigger**—Configure the condition under which the threshold is triggered. This option has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
    - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
    - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
  - o **In Threshold**—Specify the threshold value or amount of inbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
  - o **Out Threshold**—Specify the threshold value or amount of outbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
  - o **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
  - o **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
17. Above the **Interface Information** list, click **Select** to select one or more interfaces that provide network flow data.

The **Add Interface** page opens.

To add interfaces, you can obtain them automatically or configure them manually.

- a. To add interfaces automatically to the task, click the **Obtain Automatically** tab at the top of the **Add Interface** page.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

For the interfaces of a device to be displayed on this list, you must first add the device to NTA using the Device Management feature. Then, you must select the device in the NTA server configuration under **Server Management**.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

The device you want to add must also be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.

- b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.
- c. Click **OK** to accept your interface selection.

When you add the selected interfaces successfully to the task, they are displayed in the **Interface Information** list.



- d. At the top of the **Add Interface** page, click the **Configure Manually** tab to add interfaces manually to an application traffic analysis task.  
The page will update to display the configuration options for manually adding an interface to a traffic analysis task.
- e. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.
- f. In the **Interface Alias** field, enter the alias for the interface.  
Assigning a descriptive and meaningful alias to an interface will help you navigate quickly and easily to reports.
- g. From the **Device** list, select the device to which the interface belongs.  
For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration under **Server Management**.  
For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."  
The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.
- h. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.  
You can view the interface index for any interface on a device managed by INC by navigating to the **Interface Details** page of a device from its **Device Details** page.
- i. Click the **Resource** tab to navigate to the **Interface Details** page for an individual device.
- j. Under the **View Management** area on the left navigation tree, click **Device View**.  
The **Device List – All** is displayed. This list displays all devices in INC.
- k. Locate the device for which you want to view interface details.
- l. Click the link in the **Device Label** column in the **Device List – All** for the device for which you want to view interface details.  
The **Device Details** page opens.
- m. In the **Interfaces** field of the **Device Details** page for the selected device, click the **Interface List** link.  
The **Interface List** is displayed. See the **Interface Index** field for the value that NTA accepts as the interface index in the **Interface Index** field.
- n. In the **Max. Speed** field, enter the maximum speed of the interface.
- o. In the list next to the **Max. Speed** field, select the unit of measure for the interface speed.



#### IMPORTANT:

Assigning an incorrect interface maximum speed and unit of measure to an interface results in incorrect statistical analysis and reporting of metrics. Verify that the maximum interface speed and unit of measure you enter are correct.

- p. Click **OK** to add the interface manually.
18. To delete the interface, click the **Delete** icon  for the interface you want to delete.
19. To modify the interface name and interface speed, click the **Modify** icon  for the interface you want to modify.



This field contains a link to the **Modify Interface Configuration** page for the associated interface.

20. Next to the **Probe Name** field, select the check box for each probe that provides network flow data.

Leave the check box unselected if you do not want to analysis the network flow data for the associated probe.

21. Click **OK** to accept your modifications to the host traffic analysis task.

## Deleting a host traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the task you want to delete.
4. Click **OK** to confirm the deletion of the selected host traffic analysis task.  
The **Traffic Analysis Task List** reflects the deletion of the selected task.

## Viewing host traffic analysis reports

NTA provides the following levels of reporting for all host tasks:

Summarized reports for all tasks

Detailed reports for an individual task

More detailed reports for a host within a task.

All reports can be accessed by clicking the highest level branch of the left navigation tree under the **Traffic Analysis and Audit** area.

To view summarized reporting for all host tasks, click the  **Host Traffic Analysis Task** entry in the left navigation tree.

NTA also provides more detailed reporting for individual tasks, including reports for every host configured in a host traffic analysis task. NTA groups individual tasks by type. All host tasks can be found on the **Host Traffic Analysis Task** menu.

To view the **Host Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to  **Host Traffic Analysis Task**. The shortcut menu displays all host traffic analysis tasks created in NTA. Click the name of a task to view the host traffic analysis report of the task.

This section describes the reporting options available for host traffic analysis tasks. It also describes the process for navigating to host traffic analysis tasks, the summary reports available for host tasks, and the reports and features available for a host traffic analysis task.

## Navigating to the host traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Under the **Traffic Analysis and Audit** area of the left navigation tree, click the  **Host Traffic Analysis Task** entry to view summary reporting for all host tasks.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to  **Host Traffic Analysis Task**.

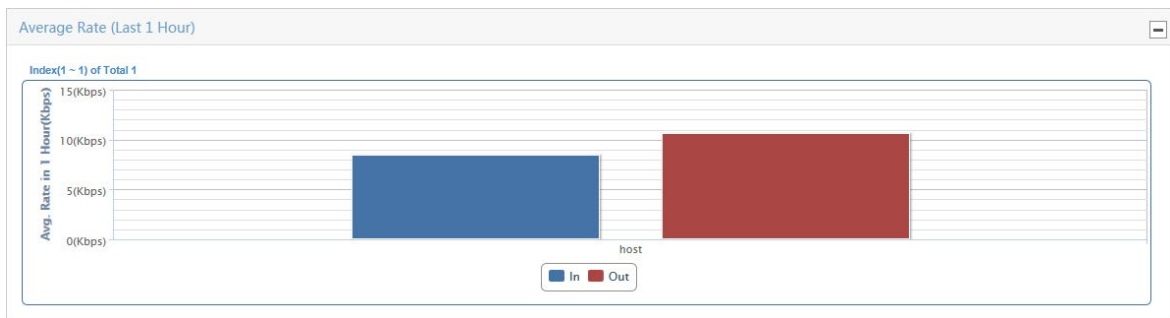
The **Host Traffic Analysis Task** menu displays all host traffic analysis tasks created in NTA. Click the name of a task to view the host traffic analysis report of the task.

## Summary reports for all host tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **Host Traffic Analysis Task** entry of the left navigation tree under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports.

The **Average Rate** bar graph summarizes the average inbound and outbound traffic rates for all hosts in every host traffic analysis task, grouped by host traffic analysis task for the last hour. You can access this graph by clicking the  **Host Traffic Analysis Task** entry of the left navigation tree. The bars are linked to allow you to navigate to the reports for the selected task.

**Figure 146 Average Rate (Last 1 Hour)**



### Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

The **Traffic Trend and TopN Application for Selected Task** includes a line chart and a pie chart. The line chart provides traffic trend rates for inbound or outbound traffic for the selected host traffic analysis tasks for the last hour. The pie chart displays the distribution of inbound or outbound TopN applications traffic for the selected host traffic analysis tasks for the last hour. You can access this chart by clicking the  **Host Traffic Analysis Task** entry of the left navigation tree.

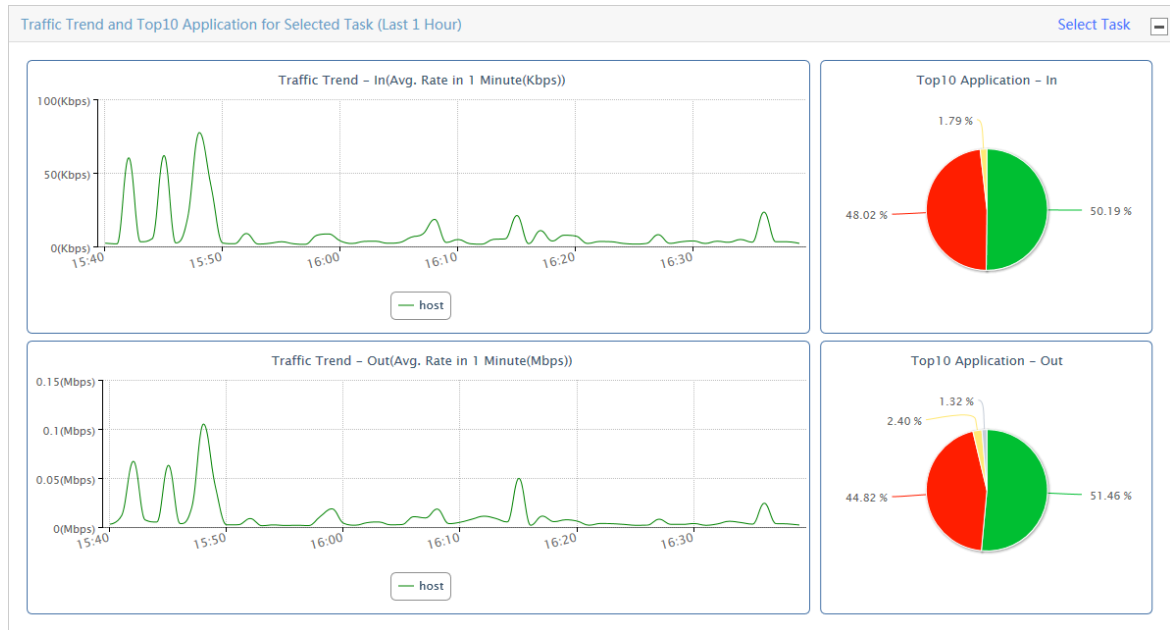
The **Traffic Trend – In** line chart provides traffic trend rates for inbound traffic for the selected host traffic analysis tasks for the last hour.

The **Traffic Trend – Out** line chart provides traffic trend rates for outbound traffic for the selected host traffic analysis tasks for the last hour.

The **TopN Application – In** pie chart displays the distribution of inbound TopN applications traffic for the selected host traffic analysis tasks for the last hour.

The **TopN Application – Out** pie chart displays the distribution of outbound TopN applications traffic for the selected host traffic analysis tasks for the last hour.

**Figure 147 Traffic Trend and TopN Application for Selected Task**



1. To select the task, click **Select Task** in the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar.  
The **Choose NTA Task** dialog box opens.
2. Select the check box next to the host task for which you want to use for this report.
3. Click **OK**.

The page displays an updated line chart for the selected host task.

### Summary list (last 1 hour)

The **Summary List** provides traffic rates statistics summarized by host task.

#### Summary list contents

- **Task Name**—Contains the name of the host traffic analysis task. The contents of this field link to reports for the associated task.
- **Total Rate**—Provides the combined inbound and outbound rate for the associated task.
- **In Rate**—Provides the rate traffic for all hosts configured for the associated task for the last hour.
- **Out Rate**—Provides the rate traffic for all hosts configured for the associated task for the last hour.

The **Add** button located at the top of the **Summary List** provides a shortcut to the **Add Host Traffic Analysis Task** page.

For more information about adding host traffic analysis tasks, see "[Adding a host traffic analysis task](#)."

Click **Refresh** to update the reports with the most recent data.

## Detailed reports for a host traffic analysis task

NTA provides a suite of reports for viewing host data from different perspectives. Reports for hosts are organized into the following reporting groups:

- **Traffic reports**—Provide overall traffic statistics and the data samples collected for the specified time period.

- **Application reports**—Provide rate of traffic statistics by application with detailed information for an individual application.
- **Source reports**—Provide distribution of traffic for the TopN source hosts as well a total traffic volume and percentage of host traffic for the TopN hosts.
- **Destination reports**—Provide distribution of traffic for the TopN destination hosts as well a total traffic volume and percentage of host traffic for the TopN destination hosts.
- **Session reports**—Provide distribution of traffic for the TopN session pairs for all hosts in a task as well a total traffic volume and percentage of host traffic for session pairs in a task.

Source, destination, and session reports enable you to get detailed information about traffic reports for an individual host/session pair.

## Traffic reports

Traffic reports for a host traffic analysis task include the **Traffic Trend** line chart that provides average per second traffic rates for all hosts in the selected traffic analysis task for the selected time range. This report also summarizes total traffic and the average, minimum, and maximum rate for all hosts in the selected task. The traffic reports include the **Traffic Details** list that provides the data collection samples that includes timestamp, total volume of traffic, and traffic rate in seconds for all hosts in the selected task for the selected range. NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a host traffic analysis task, click the **Traffic** tab to view traffic reports for the selected host traffic analysis task.

### Query traffic

NTA enables you to change the filter criteria for traffic reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed under the **Traffic** tab.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify the following query criteria:
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:

- PDF
- XLS
- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

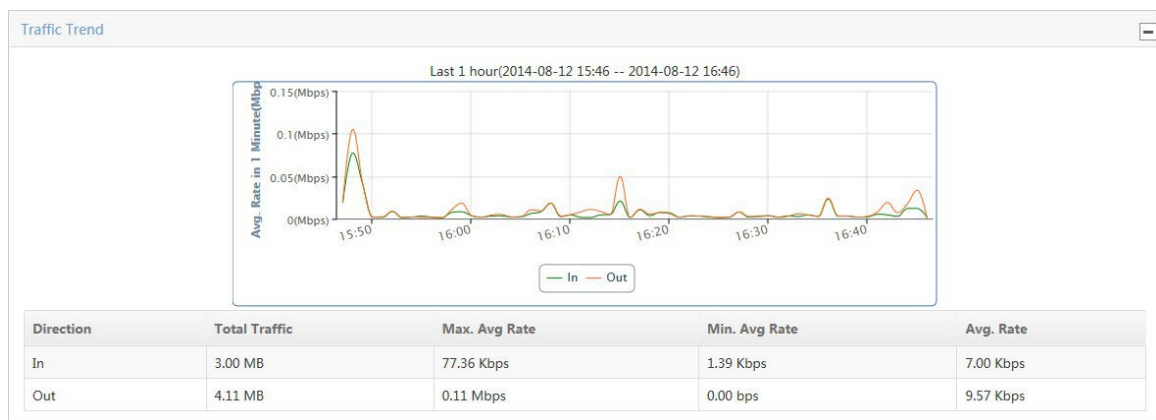
f. From **Page Range**, select the page range.

g. Click **Export**.

### Traffic Trend – Average

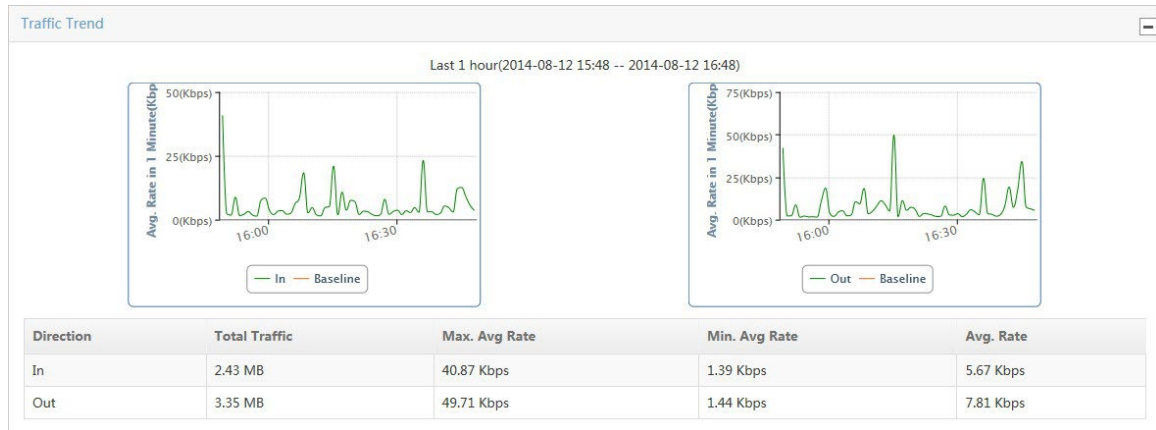
The **Traffic Trend** combination line and area chart provides average per second traffic rate for all hosts in the selected traffic analysis task for the selected time range. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for all hosts in the associated task. If more than one host exists for the selected task, these statistics reflect traffic for all hosts configured in a task.

**Figure 148 Traffic Trend Report**



If the Baseline Analysis feature is enabled for the selected traffic analysis task, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. The green line is the baseline and the red area is the average traffic rate. For more information about configuring the Baseline Analysis feature for the host traffic analysis task, see "[Configuring NTA traffic analysis parameters](#)."

**Figure 149 Traffic Trend Report**

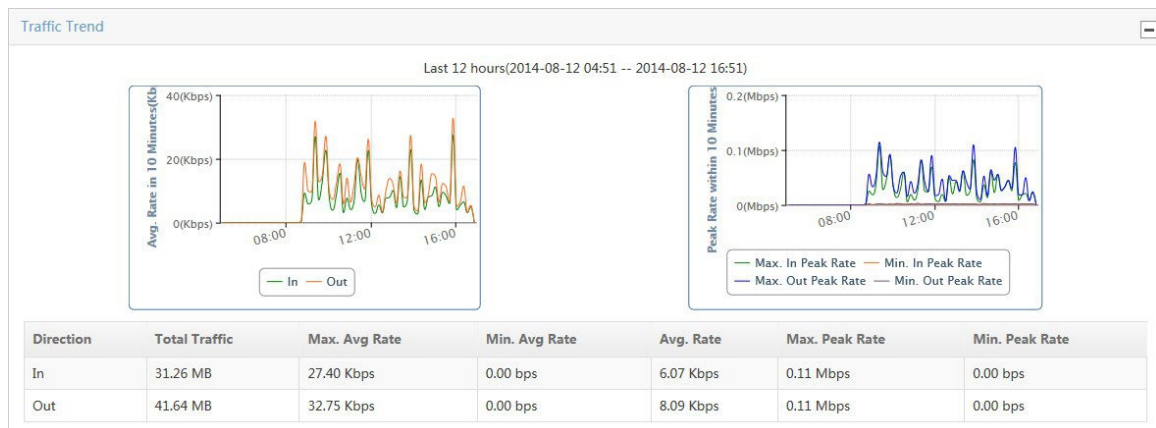


### Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range for both inbound and outbound traffic. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

**Figure 150 Traffic Trend – Peak Rate Report**



If the Baseline Analysis feature is enabled for the selected traffic analysis task, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. NTA shows the **Max./Min. In Peak Rate** chart and the **Max./Min. Out Peak Rate** chart under the **Traffic Trend** chart. For more information about configuring the Baseline Analysis feature for the host traffic analysis task, see ["Configuring NTA traffic analysis parameters."](#)

**Figure 151 Traffic Trend – Peak Rate Report**



For more information about enabling peak traffic analysis, see "[Configuring NTA traffic analysis parameters.](#)"

### Traffic details

The **Traffic Details** list provides the data collection samples for traffic statistics for all hosts in the task for the selected time range. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic for the selected time range.

**Figure 152 Traffic Details**

Figure 152 displays the Traffic Details report, showing traffic analysis data for In and Out directions. The report includes two tables.

The **Traffic - In** table shows the following data:

| Time                | Traffic | Rate       |
|---------------------|---------|------------|
| 2014-08-12 09:00:00 | 0.42 MB | 5.84 Kbps  |
| 2014-08-12 09:10:00 | 0.48 MB | 6.75 Kbps  |
| 2014-08-12 09:20:00 | 1.94 MB | 27.10 Kbps |
| 2014-08-12 09:30:00 | 0.51 MB | 7.13 Kbps  |
| 2014-08-12 09:40:00 | 0.92 MB | 12.90 Kbps |
| 2014-08-12 09:50:00 | 1.62 MB | 22.68 Kbps |
| 2014-08-12 10:00:00 | 0.54 MB | 7.62 Kbps  |

The **Traffic - Out** table shows the following data:

| Time                | Traffic | Rate       |
|---------------------|---------|------------|
| 2014-08-12 09:00:00 | 0.71 MB | 9.97 Kbps  |
| 2014-08-12 09:10:00 | 0.68 MB | 9.56 Kbps  |
| 2014-08-12 09:20:00 | 2.28 MB | 31.85 Kbps |
| 2014-08-12 09:30:00 | 0.92 MB | 12.89 Kbps |
| 2014-08-12 09:40:00 | 1.07 MB | 14.93 Kbps |
| 2014-08-12 09:50:00 | 1.94 MB | 27.15 Kbps |
| 2014-08-12 10:00:00 | 0.70 MB | 9.73 Kbps  |

## Application reports

Application reports provide rate of traffic statistics by application, by protocol, and by application category for all hosts in a task, with detailed information about an individual application. Application reports for a host traffic analysis task include the **Application List**, which provides a list of applications observed for all hosts in the selected host traffic analysis task. This list includes total volume of traffic for the associated application, rate of traffic, and the percentage of all observed traffic observed on all hosts generated by the associated application. This report also enables you to provide detailed reports for the selected application. The **Application Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all applications observed for all hosts in the selected traffic analysis task.



Protocol reports for a host traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all hosts in the selected host traffic analysis task. This list includes total volume of traffic for the associated protocol, rate of traffic, and the percentage of all observed traffic observed on all hosts generated by the associated protocol. This report also enables you to provide detailed reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all protocols observed for all hosts in the selected traffic analysis task.

Application category reports for a host traffic analysis task include the **Application Category List**, which provides a list of the application categories observed for all hosts in the selected host traffic analysis task. This list includes total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic observed on all hosts generated by the associated application category. This report also enables you to provide detailed reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all applications observed for all hosts in the selected traffic analysis task.

As with all report types for a host task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a host traffic analysis task, click the **Application** tab to view application reports for the selected host traffic analysis task, and set **Query Type** to **Application** as described in "Query applications."

Application reports display reports organized by the list of applications in NTA. NTA provides many system-defined applications and NTA also supports user defined applications. For more information on applications in NTA, see "Managing applications." This section describes the reports available for applications.

### Query applications

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of the application report, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the **Query Criteria** to expand the query criteria area.

2. Select **Application** from the **Query Type** list.

The page will display the report for Layer 4 through Layer 7 applications.

3. Click **Select** next to the **Application** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select the application for which you want to search, you must first query the **Application List** as follows:

- a. In the **Query Applications** area of the dialog box, specify one or more of the following search criteria:
  - **Application**—Enter a partial or complete name for the applications you want to search for in the **Application** field.
  - **Pre-defined**—From the **Pre-defined** list, select **Yes** to search for applications that are predefined; from the list, select **No** to filter for applications that are user-defined; finally, to include system or predefined and user-defined applications, select **Not limited**.
- b. To display the full **Application List**, click **Query** without entering any search criteria.
- c. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.
- d. Click check the boxes next to the applications for which you want to search.
- e. Click **OK** to add the applications to the filter.

The applications you selected are displayed in the **Application** field.



- f. Next to the **Application** field, click **Clear** to clear all selected applications.
  - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.

4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
    - **HTML**
    - **JRXML**
  - f. From **Page Range**, select the page range.
  - g. Click **Export**.

### Application list

The **Application List** provides a list of the applications observed for all hosts in the selected host traffic analysis task for the selected time range. This list includes the application name, an icon  for viewing the ports for all unknown applications, total volume of traffic for the associated application, rate of traffic, and the percentage of traffic on all hosts generated by the associated application. The application name in the **Application** field is a link to reports for the selected application.

**Figure 153 Application List**

| Application List                 |                      |            |           |             |           |
|----------------------------------|----------------------|------------|-----------|-------------|-----------|
| Application                      | Unknown Applications | In Traffic | In Speed  | Out Traffic | Out Speed |
| snmptrap                         |                      | 0.00 B     | 0.00 bps  | 0.98 MB     | 1.15 Kbps |
| syslog                           |                      | 0.00 B     | 0.00 bps  | 59.08 KB    | 67.22 bps |
| Telnet                           |                      | 4.27 MB    | 4.98 Kbps | 5.48 MB     | 6.39 Kbps |
| snmp                             |                      | 3.54 MB    | 4.12 Kbps | 3.81 MB     | 4.43 Kbps |
| UDP Protocol Unknown Application |                      | 50.39 KB   | 57.33 bps | 20.39 KB    | 23.20 bps |
| echo                             |                      | 48.36 KB   | 55.02 bps | 48.36 KB    | 55.02 bps |
| TCP Protocol Unknown Application |                      | 10.54 KB   | 12.00 bps | 10.45 KB    | 11.89 bps |
| netbios-ns                       |                      | 6.63 KB    | 7.54 bps  | 2.82 KB     | 3.21 bps  |
| https                            |                      | 2.09 KB    | 2.37 bps  | 1.88 KB     | 2.14 bps  |
| isakmp                           |                      | 0.73 KB    | 0.84 bps  | 1.27 KB     | 1.44 bps  |
| http                             |                      | 0.47 KB    | 0.54 bps  | 0.42 KB     | 0.48 bps  |
| SSH                              |                      | 60.00 B    | 0.07 bps  | 40.00 B     | 0.04 bps  |

1-12 of 12. Page 1 of 1.

< << 1 >> > 50

## Application Traffic Trend

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all hosts in the selected traffic analysis task for the selected time range. If more than one host exists for the selected task, these statistics reflect traffic for all hosts configured in a task.

**Figure 154 Application Traffic Trend – In/Out**



## Individual application reports

NTA provides traffic trend statistics for the individual applications that were captured for the hosts for a selected task. Individual application reports include the **Application Traffic Trend** report that displays the average rate of traffic for the selected application and the **TopN Application Usage List** that identifies which source and destination hosts contributed the greatest volume of traffic for the selected application. Also included are reports for unknown TCP and UDP applications. Unknown applications are those applications for which the Layer 4 TCP or UDP port number has not been assigned a name and is not included as an application in NTA. For more information about assigning names to TCP or UDP ports and adding them as applications to NTA, see "[Managing applications.](#)"

To view individual application reports for a host traffic analysis task, click the name in the **Application** field of the **Application List** report for the application for which you want to view this report.

To view unknown application reports for a host traffic analysis task, click the icon in the **Application** field of the **Application List** report for the application for which you want to view this report.

For more information about **Application List**, see "[Application list](#)."

### Application Traffic Trend

The **Application Traffic Trend** graph provides average rate of traffic for an individual application captured for all hosts in the selected traffic analysis task. If more than one host exists for the selected task, this chart reflects traffic for all hosts configured in a task.

By default, the **Application Traffic Trend** graph displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Application** report page, click **Back**.

**Figure 155 Traffic Trend Report for an Individual Application**



### TopN Application Usage List

The **TopN Application Usage List** includes **Source Host List – In/Out** and the **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 156 TopN Application Usage List – Destination Host List**

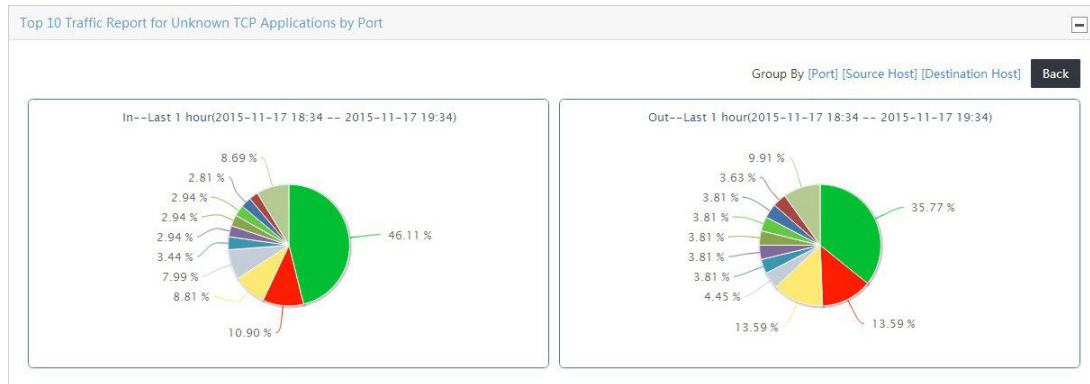
| Top 10 Application Usage List - Telnet |          |            |                             |          |            |
|----------------------------------------|----------|------------|-----------------------------|----------|------------|
| Source Host List - In                  |          |            | Source Host List - Out      |          |            |
| Source Host IP Address                 | Traffic  | Percentage | Source Host IP Address      | Traffic  | Percentage |
| 172.10.0.69                            | 2.57 MB  | 60.24%     | 172.10.0.69                 | 4.47 MB  | 81.58%     |
| 172.8.112.35                           | 0.21 MB  | 4.93%      | 172.8.112.35                | 0.21 MB  | 3.84%      |
| 172.8.112.5                            | 0.15 MB  | 3.62%      | 172.8.112.5                 | 0.15 MB  | 2.82%      |
| 172.20.0.24                            | 0.15 MB  | 3.51%      | 172.8.112.34                | 0.13 MB  | 2.42%      |
| 172.4.8.88                             | 0.15 MB  | 3.44%      | 172.8.112.2                 | 0.13 MB  | 2.39%      |
| 172.8.112.34                           | 0.13 MB  | 3.10%      | 172.8.112.45                | 71.17 KB | 1.27%      |
| 172.8.112.2                            | 0.13 MB  | 3.07%      | 172.8.112.75                | 60.67 KB | 1.08%      |
| 172.8.12.95                            | 74.55 KB | 1.70%      | 172.8.112.7                 | 52.15 KB | 0.93%      |
| 172.8.111.36                           | 71.60 KB | 1.64%      | 172.8.112.10                | 47.19 KB | 0.84%      |
| 172.8.112.45                           | 71.17 KB | 1.63%      | 172.8.112.17                | 32.26 KB | 0.57%      |
| Other Hosts                            | 0.56 MB  | 13.12%     | Other Hosts                 | 0.12 MB  | 2.25%      |
| Destination Host List - In             |          |            | Destination Host List - Out |          |            |
| Destination Host IP Address            | Traffic  | Percentage | Destination Host IP Address | Traffic  | Percentage |
| 172.10.0.69                            | 1.70 MB  | 39.76%     | 172.10.0.69                 | 1.01 MB  | 18.42%     |
| 172.8.112.35                           | 0.49 MB  | 11.40%     | 172.8.112.35                | 0.49 MB  | 8.89%      |
| 172.8.112.5                            | 0.39 MB  | 9.03%      | 172.20.0.24                 | 0.39 MB  | 7.17%      |
| 172.8.112.2                            | 0.35 MB  | 8.21%      | 172.8.112.5                 | 0.39 MB  | 7.04%      |
| 172.8.112.34                           | 0.35 MB  | 8.09%      | 172.8.112.2                 | 0.35 MB  | 6.40%      |
| 172.8.112.45                           | 0.21 MB  | 4.97%      | 172.8.112.34                | 0.35 MB  | 6.31%      |
| 172.8.112.10                           | 0.13 MB  | 2.97%      | 172.4.8.88                  | 0.32 MB  | 5.82%      |
| 172.8.112.75                           | 0.12 MB  | 2.86%      | 172.8.111.42                | 0.25 MB  | 4.59%      |
| 172.8.112.7                            | 0.12 MB  | 2.70%      | 172.8.111.36                | 0.22 MB  | 3.94%      |
| 172.8.112.17                           | 87.93 KB | 2.01%      | 172.8.112.45                | 0.21 MB  | 3.87%      |
| Other Hosts                            | 0.34 MB  | 8.01%      | Other Hosts                 | 1.51 MB  | 27.56%     |

### TopN Traffic Report for Unknown TCP/UDP Applications by Port

The **TopN Traffic Report for Unknown TCP/UDP Applications by Port** provides the distribution of traffic by TCP or UDP port number for all application traffic that cannot be attributed to an application or protocol captured for the hosts in the selected traffic analysis task for the selected time range. NTA enables you to change how the traffic is grouped.

1. From the **Group By** list in the upper right corner of the **TopN Traffic Report for Unknown TCP/UDP Applications by Port** area of the page, select **Port** to group by port.
2. From the **Group By** list, select **Source Host** to group by source host.
3. From the **Group By** list, select **Destination Host** to group by destination host.
4. Click **Back** to return to the main **Application** report page.

**Figure 157 TopN Traffic Report for Unknown TCP/UDP Applications**



### TopN Traffic List for Unknown TCP/UDP Applications by Port

The **TopN Traffic List for Unknown TCP/UDP Applications by Port** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the TCP or UDP port number, total volume of traffic, rate of traffic, and the percentage of all observed traffic. The port number is a link to individual reports for the selected port. The icon  in the **Define Application** field is a link for adding the selected port as a Layer 4 application to NTA. For more information about managing applications in NTA, see "[Managing applications](#)."

**Figure 158 TopN Traffic List for Unknown TCP/UDP Applications by Port**

| Top 10 Traffic List for Unknown TCP Applications by Port |         |           |                                                                                     |                               |        |         |           |                                                                                       |                               |
|----------------------------------------------------------|---------|-----------|-------------------------------------------------------------------------------------|-------------------------------|--------|---------|-----------|---------------------------------------------------------------------------------------|-------------------------------|
| In                                                       |         |           |                                                                                     |                               | Out    |         |           |                                                                                       |                               |
| Port                                                     | Traffic | Rate      | Define Application                                                                  | Percentage                    | Port   | Traffic | Rate      | Define Application                                                                    | Percentage                    |
| 6007                                                     | 2.78 MB | 6.49 Kbps |  | 46.11% <div><div></div></div> | 6007   | 3.10 MB | 7.22 Kbps |  | 35.77% <div><div></div></div> |
| 52512                                                    | 0.66 MB | 1.53 Kbps |  | 10.90% <div><div></div></div> | 53553  | 1.18 MB | 2.74 Kbps |  | 13.59% <div><div></div></div> |
| 54273                                                    | 0.53 MB | 1.24 Kbps |  | 8.81% <div><div></div></div>  | 135    | 1.18 MB | 2.74 Kbps |  | 13.59% <div><div></div></div> |
| 55025                                                    | 0.48 MB | 1.12 Kbps |  | 7.99% <div><div></div></div>  | 52155  | 0.39 MB | 0.90 Kbps |  | 4.45% <div><div></div></div>  |
| 52334                                                    | 0.21 MB | 0.48 Kbps |  | 3.44% <div><div></div></div>  | 52340  | 0.33 MB | 0.77 Kbps |  | 3.81% <div><div></div></div>  |
| 52165                                                    | 0.18 MB | 0.41 Kbps |  | 2.94% <div><div></div></div>  | 54168  | 0.33 MB | 0.77 Kbps |  | 3.81% <div><div></div></div>  |
| 54498                                                    | 0.18 MB | 0.41 Kbps |  | 2.94% <div><div></div></div>  | 54396  | 0.33 MB | 0.77 Kbps |  | 3.81% <div><div></div></div>  |
| 54593                                                    | 0.18 MB | 0.41 Kbps |  | 2.94% <div><div></div></div>  | 54814  | 0.33 MB | 0.77 Kbps |  | 3.81% <div><div></div></div>  |
| 52339                                                    | 0.17 MB | 0.40 Kbps |  | 2.81% <div><div></div></div>  | 55247  | 0.33 MB | 0.77 Kbps |  | 3.81% <div><div></div></div>  |
| 52501                                                    | 0.15 MB | 0.34 Kbps |  | 2.43% <div><div></div></div>  | 54498  | 0.31 MB | 0.73 Kbps |  | 3.63% <div><div></div></div>  |
| Others                                                   | 0.52 MB | 1.22 Kbps |                                                                                     | 8.69% <div><div></div></div>  | Others | 0.86 MB | 2.00 Kbps |                                                                                       | 9.91% <div><div></div></div>  |

### TopN Traffic List for Unknown TCP/UDP Applications by Source Host

The **TopN Traffic List for Unknown TCP/UDP Applications by Source Host** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, rate of traffic, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host** is a link for initiating a host query and a link to the results of the query.

**Figure 159 TopN Traffic List for Unknown TCP/UDP Applications by Source Host**

| Top 10 Traffic List for Unknown UDP Applications by Source Host |          |           |            |             |          |           |            |
|-----------------------------------------------------------------|----------|-----------|------------|-------------|----------|-----------|------------|
| In                                                              |          |           |            | Out         |          |           |            |
| Source Host                                                     | Traffic  | Rate      | Percentage | Source Host | Traffic  | Rate      | Percentage |
| 1.1.1.69                                                        | 30.00 KB | 34.13 bps | 59.53%     | 172.10.0.69 | 10.58 KB | 12.04 bps | 51.90%     |
| 172.10.0.69                                                     | 9.81 KB  | 11.16 bps | 19.47%     | 172.10.0.68 | 9.81 KB  | 11.16 bps | 48.10%     |
| 172.10.0.68                                                     | 9.81 KB  | 11.16 bps | 19.47%     |             |          |           |            |
| 172.4.0.201                                                     | 0.77 KB  | 0.88 bps  | 1.53%      |             |          |           |            |

### TopN Traffic List for Unknown TCP/UDP Applications by Destination Host

The **TopN Traffic List for Unknown TCP/UDP Applications by Destination Host** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the destination host IP address, total volume of traffic for the associated destination, rate of traffic, and the percentage of all observed traffic generated by the destination. The host query icon next to the **Destination Host** is a link for initiating a host query a link to the results of the query.

**Figure 160 TopN Traffic List for Unknown TCP/UDP Applications by Destination Host**

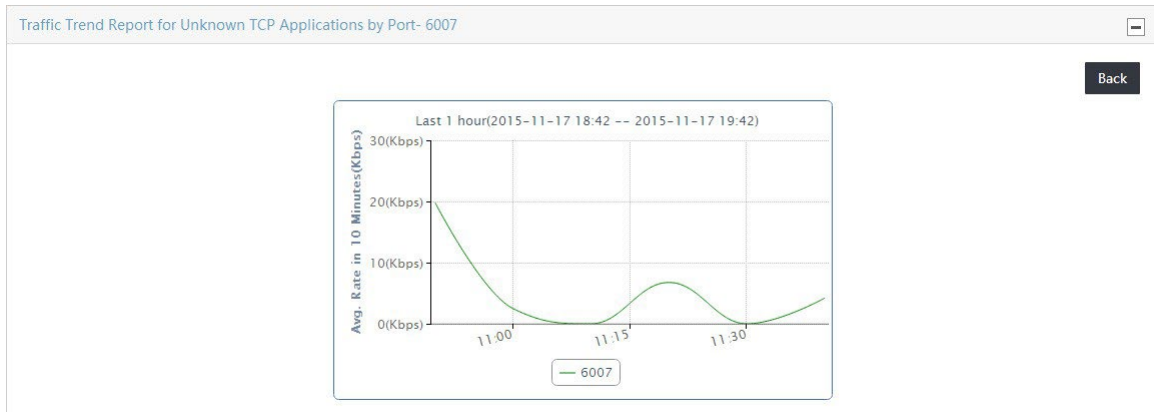
| Top 10 Traffic List for Unknown UDP Applications by Destination Host |          |           |            |                  |         |           |            |
|----------------------------------------------------------------------|----------|-----------|------------|------------------|---------|-----------|------------|
| In                                                                   |          |           |            | Out              |         |           |            |
| Destination Host                                                     | Traffic  | Rate      | Percentage | Destination Host | Traffic | Rate      | Percentage |
| 172.10.0.30                                                          | 30.00 KB | 34.13 bps | 59.53%     | 172.10.0.69      | 9.81 KB | 11.16 bps | 48.10%     |
| 172.10.0.69                                                          | 10.58 KB | 12.04 bps | 21.00%     | 172.10.0.68      | 9.81 KB | 11.16 bps | 48.10%     |
| 172.10.0.68                                                          | 9.81 KB  | 11.16 bps | 19.47%     | 172.4.0.201      | 0.77 KB | 0.88 bps  | 3.79%      |

### TopN Trend Report for Unknown TCP/UDP Applications by Port

To view this report for a host traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **Traffic Trend** graph provides the average rate for an individual unknown application captured for the hosts in the selected traffic analysis task. Click **Back** to return to the all unknown application report page.

**Figure 161 Traffic Trend Report for Unknown TCP/UDP Applications by Port**



### TopN Traffic Details List for Unknown TCP/UDP Applications by Port



To view this report for a host traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs, the volume of traffic sent and received between this source host and the destination, the rate of traffic observed between the pair, and the percentage of all traffic observed for this source host.

**Figure 162 TopN Traffic Details List for Unknown TCP/UDP Applications by Port**

| Top 10 Traffic Details List for Unknown TCP Applications by Port - 6007 |                  |         |           |                                                                                            |
|-------------------------------------------------------------------------|------------------|---------|-----------|--------------------------------------------------------------------------------------------|
| Source Host                                                             | Destination Host | Traffic | Rate      | Percentage                                                                                 |
| 192.168.40.150                                                          | 172.4.1.116      | 1.31 MB | 3.04 Kbps | 54.98%  |
| 192.168.40.77                                                           | 172.4.1.116      | 1.07 MB | 2.49 Kbps | 45.02%  |

## Protocol Reports

Protocol reports display traffic rate trend reports organized by the list of protocols predefined in NTA. Protocol reports for a host traffic analysis task include the **Protocol List**, which provides a list of protocols captured for the hosts in the selected host traffic analysis task. This report also enables you to provide detailed reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average inbound or outbound traffic rates for all protocol captured for the hosts in the selected traffic analysis task. Protocol reports also include traffic lists and trend reports for individual protocols.

As with all report types for a host traffic analysis task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a host traffic analysis task, click the **Application** tab to view application reports for the selected host traffic analysis task, and set **Query Type to Protocol** as described in "Query protocols." For more information on protocols in NTA, see "Managing protocols." This section describes the reports available for protocols.

### Query protocols

To view reports by protocol, you must configure the filter criteria for application reports. NTA enables you to change the filter criteria for protocol reports. You can change the default settings for query type, protocol, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the **Query Criteria** to expand the query criteria area.
2. Select **Protocol** from the **Query Type** list. The page will display the report for protocols.
3. Click **Select** next to the **Protocol** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the protocol you want to search for, you must first query the **Protocol List** as follows:

- a. In the **Query Protocols** area of the dialog box, specify one or more of the following search criteria:
  - **Protocol**—In the **Protocol** field, enter a partial or complete name for the protocols for which you want to search.
  - **Pre-defined**—From the **Pre-defined** list, select **Yes** to search for protocols that are predefined; from the list, select **No** to filter for protocols that are user-defined; finally, select **Not limited** to include system, predefined, or user-defined protocols.
- b. To display the full **Protocol List**, click **Query** without entering any search criteria.
- c. Click **Query**.

The query results are displayed in the **Protocol List** below the **Query Protocols** area.

- d. Select the check boxes next to the protocols for which you want to search.
- e. Click **OK** to add the protocols to the filter.  
The protocols you selected are displayed in the **Protocol** field.
- f. Click **Clear** to clear all selected protocols.
  - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the protocol report, click the icon  in the upper right corner of the protocol report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for protocols.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. Select the export file format from the **File Format** list. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
    - **HTML**
    - **JRXML**
  - f. From **Page Range**, select the page range.
  - g. Click **Export**.

### Protocol List

The **Protocol List** provides a list of the protocols captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the protocol name, total volume of traffic for the associated protocol, rate of traffic, and the percentage of traffic on the host generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.



**Figure 163 Protocol List**

| Protocol | In Traffic | In Speed  | Out Traffic | Out Speed |
|----------|------------|-----------|-------------|-----------|
| OSPF     | 0.00 B     | 0.00 bps  | 0.51 MB     | 0.60 Kbps |
| GRE      | 15.42 KB   | 17.55 bps | 0.00 B      | 0.00 bps  |
| AH       | 49.19 KB   | 55.96 bps | 0.31 MB     | 0.36 Kbps |
| ICMP     | 1.25 MB    | 1.46 Kbps | 1.21 MB     | 1.41 Kbps |
| UDP      | 3.62 MB    | 4.22 Kbps | 4.90 MB     | 5.71 Kbps |
| TCP      | 4.31 MB    | 5.02 Kbps | 5.51 MB     | 6.42 Kbps |

1-6 of 6. Page 1 of 1.

From the lower right of the main pane, click **8**, **15**, **50**, **100**, **200**, or **1000** to configure how many items per page you want to view.

### Protocol Traffic Trend

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocols captured for the hosts in the selected traffic analysis task for the selected time range.

**Figure 164 Protocol Traffic Trend – In/Out**



## Individual protocol reports

NTA provides traffic trend statistics for the individual protocol that were captured for the hosts for a selected task. Individual protocols reports include the **Protocol Traffic Trend** report that displays the average rate of traffic for the selected protocol and include the **TopN Protocol Usage List** that identifies which source and destination hosts contributed the greatest volume of traffic for the selected protocol.

To view individual protocol reports for a probe task, click the name in the **Protocol** field of the **Protocol List** report for the protocol for which you want to view this report. For more information about **Protocol List**, see "[Protocol List](#)."

### Protocol Traffic Trend

The **Protocol Traffic Trend** graph provides the average rate for an individual protocol captured for the hosts in the selected traffic analysis task.

By default, the **Protocol Traffic Trend** graph displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Protocol** report page, click **Back**.

**Figure 165 Traffic Trend Report for an Individual Protocol**



**TopN Protocol Usage List**

The **TopN Protocol Usage List** includes the **Source Host List – In/Out** and the **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.

**Figure 166 TopN Protocol Usage List – Destination Host List**

| Top 10 Protocol Usage List - TCP |          |            |                             |          |            |
|----------------------------------|----------|------------|-----------------------------|----------|------------|
| Source Host List - In            |          |            | Source Host List - Out      |          |            |
| Source Host IP Address           | Traffic  | Percentage | Source Host IP Address      | Traffic  | Percentage |
| 172.10.0.69                      | 2.58 MB  | 60.25%     | 172.10.0.69                 | 4.47 MB  | 81.57%     |
| 172.8.112.35                     | 0.21 MB  | 4.91%      | 172.8.112.35                | 0.21 MB  | 3.84%      |
| 172.8.112.5                      | 0.15 MB  | 3.61%      | 172.8.112.5                 | 0.15 MB  | 2.82%      |
| 172.20.0.24                      | 0.15 MB  | 3.50%      | 172.8.112.34                | 0.13 MB  | 2.42%      |
| 172.4.8.88                       | 0.15 MB  | 3.43%      | 172.8.112.2                 | 0.13 MB  | 2.39%      |
| 172.8.112.34                     | 0.13 MB  | 3.09%      | 172.8.112.45                | 71.17 KB | 1.27%      |
| 172.8.112.2                      | 0.13 MB  | 3.06%      | 172.8.112.75                | 60.67 KB | 1.08%      |
| 172.8.12.95                      | 74.55 KB | 1.70%      | 172.8.112.7                 | 52.15 KB | 0.93%      |
| 172.8.111.36                     | 71.60 KB | 1.63%      | 172.8.112.10                | 47.19 KB | 0.84%      |
| 172.8.112.45                     | 71.17 KB | 1.62%      | 172.8.112.17                | 32.26 KB | 0.57%      |
| Other Hosts                      | 0.57 MB  | 13.21%     | Other Hosts                 | 0.12 MB  | 2.27%      |
| Destination Host List - In       |          |            | Destination Host List - Out |          |            |
| Destination Host IP Address      | Traffic  | Percentage | Destination Host IP Address | Traffic  | Percentage |
| 172.10.0.69                      | 1.70 MB  | 39.75%     | 172.10.0.69                 | 1.01 MB  | 18.43%     |
| 172.8.112.35                     | 0.49 MB  | 11.36%     | 172.8.112.35                | 0.49 MB  | 8.88%      |
| 172.8.112.5                      | 0.39 MB  | 9.00%      | 172.20.0.24                 | 0.39 MB  | 7.17%      |
| 172.8.112.2                      | 0.35 MB  | 8.18%      | 172.8.112.5                 | 0.39 MB  | 7.04%      |
| 172.8.112.34                     | 0.35 MB  | 8.06%      | 172.8.112.2                 | 0.35 MB  | 6.39%      |
| 172.8.112.45                     | 0.21 MB  | 4.95%      | 172.8.112.34                | 0.35 MB  | 6.30%      |
| 172.8.112.10                     | 0.13 MB  | 2.96%      | 172.4.8.88                  | 0.32 MB  | 5.81%      |
| 172.8.112.75                     | 0.12 MB  | 2.85%      | 172.8.111.42                | 0.25 MB  | 4.59%      |
| 172.8.112.7                      | 0.12 MB  | 2.69%      | 172.8.111.36                | 0.22 MB  | 3.93%      |
| 172.8.112.17                     | 87.93 KB | 2.00%      | 172.8.112.45                | 0.21 MB  | 3.87%      |
| Other Hosts                      | 0.35 MB  | 8.20%      | Other Hosts                 | 1.51 MB  | 27.59%     |

## Application category reports

Application category reports display traffic rate trend reports organized by the application categories in NTA. Application category reports for a host traffic analysis task include the **Application Category List**, which provides a list of the application categories captured for the hosts in the selected host traffic analysis task. This list includes total volume of traffic for the associated application categories, rate of traffic, and the percentage of all traffic captured for the hosts. This report also enables you to provide detailed reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound or outbound traffic rates attributed to the application categories captured for the hosts in the selected traffic analysis task. Application category reports also include traffic lists and trend reports for the individual application categories.

As with all report types for a host traffic analysis task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a host traffic analysis task, click the **Application** tab to view application reports for the selected host traffic analysis task, and set **Query Type** to **Application Category** as described in "[Query application categories](#)."

NTA provides many system-defined application categories and also supports user defined application categories. For more information about application categories in NTA, see "[Managing application categories](#)." This section describes the reports available for application categories.

### Query application categories

To view reports by application category, you must configure the filter criteria for application category reports. NTA enables you to change the filter criteria for application category reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to **Query Criteria** to expand the query criteria area.
2. Select **Application Category** from the **Query Type** list.  
The page displays the report for application categories.
3. Click **Select** next to the **Application Category** field.  
The **Query Application Categories** dialog box displays an empty **Application Category List**. To select the application categories you want to search for, you must first query the **Application Category List** as follows:
  - a. Specify one or more of the following search criteria in the **Query Application Categories** area of the dialog box:
    - **Application Category**—In the **Application Category** field, enter a partial or complete name of the application categories for which you want to search.
    - **Pre-defined**—From the **Pre-defined** list, select **Yes** to search for application categories that are predefined; select **No** to filter for application categories that are user-defined; finally, select **Not limited** to include system or predefined and user-defined application categories.
  - b. To display the full **Application Category List**, click **Query** without entering any search criteria.
  - c. Click **Query**.  
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
  - d. Select the check boxes next to the application categories for which you want to search.
  - e. Click **OK** to add the application categories you have selected to the filter.  
The application categories you selected are displayed in the **Application Category** field.
  - f. Click **Clear** to clear all selected application categories.
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application category report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. Select the export file format from the **File Format** list. Options are:

- PDF
- XLS
- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

f. From **Page Range**, select the page range.

g. Click **Export**.

### Application Category List

The **Application Category List** provides a list of the application categories for which traffic was observed for the hosts in the selected host traffic analysis task for the selected time range. This list includes the application category name, total volume of traffic for the associated application category, rate of traffic, and the percentage of traffic on the host generated by the associated application category. The application category name in the **Application Category** field is a link to reports for the selected application category.

**Figure 167 Application Category List**

| Application Category List  |              |            |               |             |
|----------------------------|--------------|------------|---------------|-------------|
| Application Category ↕     | In Traffic ↕ | In Speed ↕ | Out Traffic ↕ | Out Speed ↕ |
| Enterprise Application     | 0.73 KB      | 0.84 bps   | 60.34 KB      | 68.66 bps   |
| HTTP                       | 2.56 KB      | 2.91 bps   | 2.30 KB       | 2.62 bps    |
| File Service               | 6.63 KB      | 7.54 bps   | 2.82 KB       | 3.21 bps    |
| qqqqqqq                    | 1.32 MB      | 1.53 Kbps  | 1.52 MB       | 1.77 Kbps   |
| Network Management         | 3.54 MB      | 4.12 Kbps  | 4.79 MB       | 5.58 Kbps   |
| Remote Management          | 4.27 MB      | 4.98 Kbps  | 5.48 MB       | 6.39 Kbps   |
| Other Application Category | 0.11 MB      | 0.12 Kbps  | 0.59 MB       | 0.69 Kbps   |

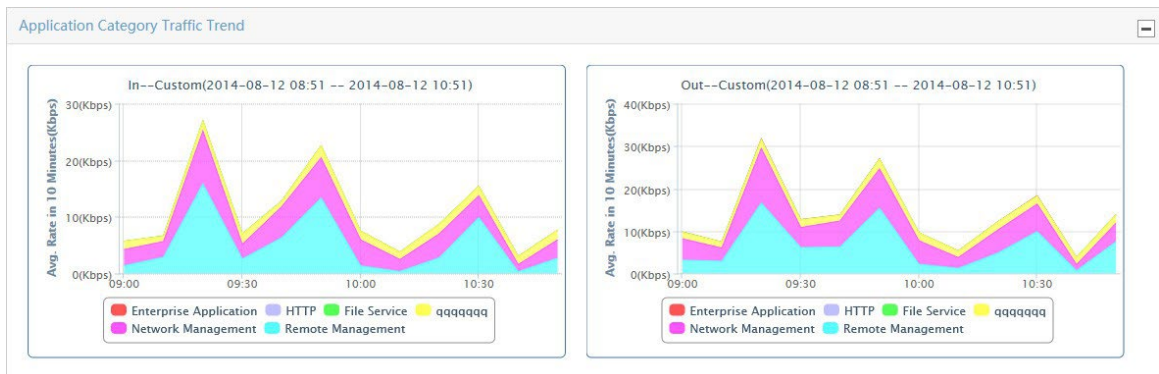
1-7 of 7. Page 1 of 1.

« < 1 > » 50 ▾

### Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all application categories captured for the hosts in the selected traffic analysis task for the selected time range.

**Figure 168 Application Category Traffic Trend – In/Out**



## Individual application category reports

NTA provides traffic trend statistics for the individual application categories that were captured for the hosts for a selected task. Individual application categories reports include the **Application Category Traffic Trend** report that displays the average rate of traffic for the selected application category. Individual application category reports also include the **TopN Application Category Usage List** that identifies the TopN source and destination hosts.

To view application category reports for a host task, click the name in the **Application Category** field of the **Application Category List** report for the application category for which you want to view this report. For more information about **Application Category List**, see "[Application Category List](#)."

### Application Category Traffic Trend

The **Application Category Traffic Trend** graph provides the average rate for an individual application category captured for the hosts in the selected traffic analysis task. By default, this graph displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Application Category** report page, click **Back**.

**Figure 169 Traffic Trend Report for an Individual Application Category**



### TopN Application Category Usage List

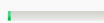
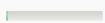
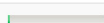
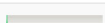
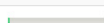
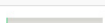
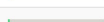
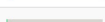
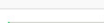
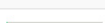
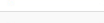
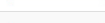
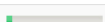
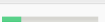
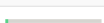
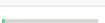
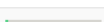
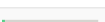
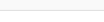
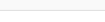
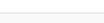
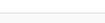
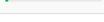
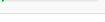
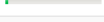
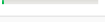
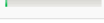
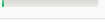
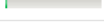
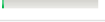
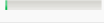
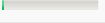
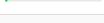
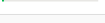
The **TopN Application Category Usage List** includes the **Source Host List – In/Out** and the **Destination Host List– In/Out** lists.

The **TopN Application Category Usage List – Source Host List** provides a list of the TopN source hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link to the results of the query.

The **TopN Application Category Usage List – Destination Host List** provides a list of the TopN destination hosts measured by volume of traffic captured for the hosts in the selected host traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link to the results of the query.



**Figure 170 TopN Application Category Usage List – Destination Host List**

| Top 10 Application Category Usage List - Network Management                                      |           |                                                                                            |                                                                                                  |           |                                                                                              |  |
|--------------------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------|--|
| Source Host List - In                                                                            |           |                                                                                            | Source Host List - Out                                                                           |           |                                                                                              |  |
| Source Host IP Address                                                                           | Traffic   | Percentage                                                                                 | Source Host IP Address                                                                           | Traffic   | Percentage                                                                                   |  |
|  172.10.0.69    | 1.39 MB   | 41.07%    |  172.10.0.69    | 3.56 MB   | 79.03%    |  |
|  172.4.21.10    | 0.13 MB   | 3.85%     |  172.8.112.24   | 101.35 KB | 2.20%     |  |
|  172.4.8.88     | 0.13 MB   | 3.74%     |  172.8.112.2    | 91.99 KB  | 2.00%     |  |
|  172.8.112.24   | 102.04 KB | 2.94%     |  172.8.112.35   | 87.39 KB  | 1.90%     |  |
|  172.8.110.121  | 97.78 KB  | 2.82%     |  172.8.112.78   | 84.77 KB  | 1.84%     |  |
|  172.8.112.2    | 91.99 KB  | 2.65%     |  172.8.112.5    | 76.07 KB  | 1.65%     |  |
|  172.8.111.50   | 90.88 KB  | 2.62%     |  172.8.112.13   | 70.21 KB  | 1.52%     |  |
|  172.8.111.36   | 89.07 KB  | 2.57%     |  172.8.112.45   | 56.03 KB  | 1.22%     |  |
|  172.8.112.35   | 87.39 KB  | 2.52%     |  172.8.112.26   | 55.97 KB  | 1.21%     |  |
|  172.8.112.78   | 86.51 KB  | 2.50%     |  172.8.112.11   | 53.22 KB  | 1.15%     |  |
| Other Hosts                                                                                      | 1.11 MB   | 32.71%    | Other Hosts                                                                                      | 0.28 MB   | 6.28%     |  |
| Destination Host List - In                                                                       |           |                                                                                            | Destination Host List - Out                                                                      |           |                                                                                              |  |
| Destination Host IP Address                                                                      | Traffic   | Percentage                                                                                 | Destination Host IP Address                                                                      | Traffic   | Percentage                                                                                   |  |
|  172.10.0.69    | 1.99 MB   | 58.93%    |  172.10.0.69    | 0.94 MB   | 20.97%    |  |
|  172.8.112.2    | 0.13 MB   | 3.85%     |  172.4.8.88     | 0.16 MB   | 3.62%     |  |
|  172.8.112.35   | 0.12 MB   | 3.55%     |  172.4.21.10    | 0.16 MB   | 3.49%     |  |
|  172.8.112.24   | 0.12 MB   | 3.44%     |  172.8.112.2    | 0.13 MB   | 2.79%     |  |
|  172.8.112.78   | 0.11 MB   | 3.12%     |  172.8.111.36   | 0.12 MB   | 2.71%     |  |
|  172.8.112.5    | 0.10 MB   | 3.04%     |  172.8.112.24   | 0.12 MB   | 2.57%     |  |
|  172.8.112.13   | 96.38 KB  | 2.78%     |  172.8.112.35   | 0.12 MB   | 2.56%     |  |
|  172.8.112.45  | 92.79 KB  | 2.68%    |  172.8.110.121 | 0.11 MB   | 2.54%    |  |
|  172.8.112.26 | 83.96 KB  | 2.42%   |  172.8.111.50 | 0.11 MB   | 2.41%   |  |
|  172.8.112.11 | 80.74 KB  | 2.33%   |  172.8.112.78 | 0.11 MB   | 2.35%   |  |
| Other Hosts                                                                                      | 0.47 MB   | 13.85%  | Other Hosts                                                                                      | 2.43 MB   | 53.99%  |  |

## Source reports

Source reports include inbound and outbound reports. The inbound report includes the **TopN Traffic Report for Source Host** bar/pie chart. This bar chart displays the average rate of traffic sent from the TopN source hosts to the hosts configured in the selected task. The pie chart displays the distribution of traffic sent from the TopN source hosts to the hosts configured in the selected task.

The inbound report also include the **TopN Traffic List for Source Host**, which provides a list showing volume and percentage of traffic generated for each of the TopN source hosts that sent traffic to the hosts that configured in the selected task. The outbound report includes the **TopN Traffic Report for Source Host** bar/pie chart.

This bar chart displays the average rate of traffic sent from the hosts configured in the selected task to any other hosts. This pie chart displays the distribution of traffic sent from the hosts configured in the selected task to any other hosts. The outbound report also includes the **TopN Traffic List for Source Host**, which provides a list showing volume and percentage of traffic generated for each of the TopN source hosts that configured in the selected task. These lists also contain a link for navigating to reports for the selected source host.

The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the host query. As with all report types for a host task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a host traffic analysis task, click the **Source** tab to view traffic reports for the selected host traffic analysis task.

## Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed under the **Source** tab.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Source Host**—In the **Source Host** field, enter the IP address or address range. To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24  
Example of a valid IPv6 address:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
    - **HTML**



– JRXML

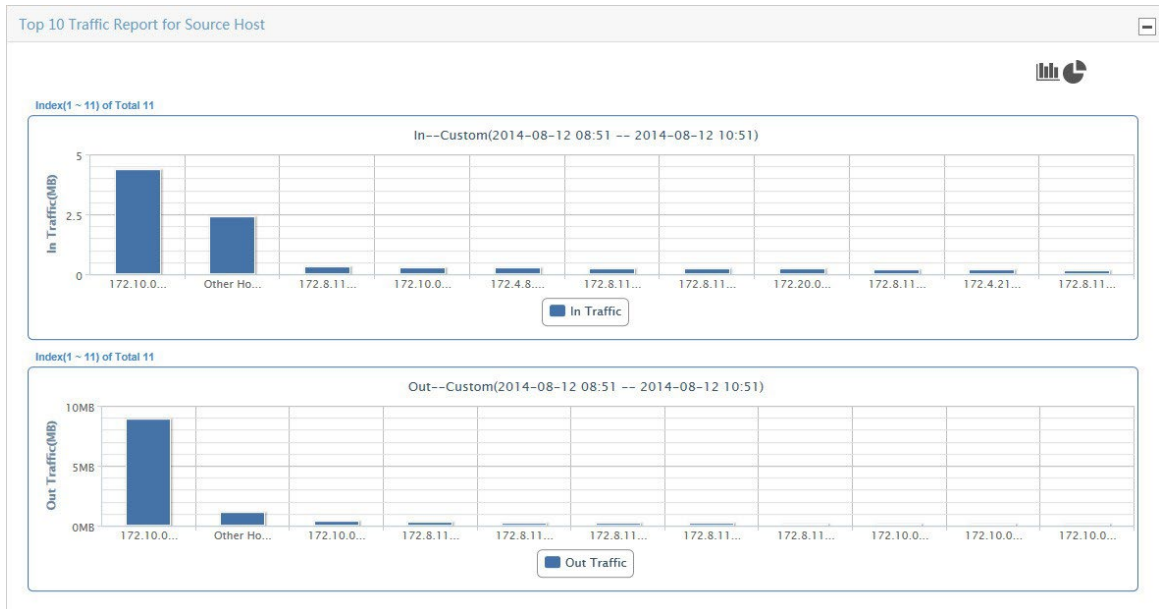
f. From **Page Range**, select the page range.

g. Click **Export**.

### TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host – In/Out** bar chart displays the average rate of inbound/outbound traffic for the TopN source hosts for the selected traffic analysis task for the selected time range. The pie chart icon  is a link to display the **TopN Traffic Report for Source Host – In/Out** data as a pie chart.

**Figure 171 TopN Traffic Report for Source Host – In/Out**



The **TopN Traffic Report for Source Host – In/Out** pie chart displays the distribution of inbound/outbound traffic for the TopN source hosts for the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the selected host.

### TopN traffic List for Source Host

The **TopN Traffic List for Source Host – In/Out** provides a list of the TopN source hosts measured by volume of inbound/outbound traffic observed for the selected host traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source host, and the percentage of all observed traffic generated by the source host.

The IP address is a link to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and a link to the results of the host query.

Figure 172 TopN Traffic List for Source Host- In/Out

| Top 10 Traffic List for Source Host |         |            |                |         |            |
|-------------------------------------|---------|------------|----------------|---------|------------|
| In                                  |         |            | Out            |         |            |
| Generate Chart                      |         |            | Generate Chart |         |            |
| Source                              | Traffic | Percentage | Source         | Traffic | Percentage |
| 172.10.0.69                         | 4.36 MB | 49.86%     | 172.10.0.69    | 8.91 MB | 75.93%     |
| 172.8.112.35                        | 0.30 MB | 3.40%      | 172.10.0.60    | 0.39 MB | 3.31%      |
| 172.10.0.60                         | 0.28 MB | 3.21%      | 172.8.112.35   | 0.30 MB | 2.52%      |
| 172.4.8.88                          | 0.27 MB | 3.14%      | 172.8.112.5    | 0.23 MB | 1.95%      |
| 172.8.112.5                         | 0.23 MB | 2.62%      | 172.8.112.2    | 0.22 MB | 1.88%      |
| 172.8.112.2                         | 0.22 MB | 2.53%      | 172.8.112.34   | 0.17 MB | 1.42%      |
| 172.20.0.24                         | 0.20 MB | 2.34%      | 172.8.112.45   | 0.12 MB | 1.06%      |
| 172.8.112.34                        | 0.17 MB | 1.91%      | 172.10.0.73    | 0.12 MB | 0.99%      |
| 172.4.21.10                         | 0.16 MB | 1.88%      | 172.10.0.72    | 0.11 MB | 0.93%      |
| 172.8.111.36                        | 0.16 MB | 1.81%      | 172.10.0.71    | 0.11 MB | 0.91%      |
| Other Hosts                         | 2.38 MB | 27.29%     | Other Hosts    | 1.07 MB | 9.08%      |

Traffic Trend Report for Source Host

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Trend Report for Source Host** line chart provides the average rate of traffic for the selected source host. By default, the **Traffic Trend Report for Source Host** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return the main **Source** host report page, click **Back**.

Figure 173 Traffic Trend Report for Source Host



Traffic details

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Details** for a source host table shows two lists. The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and the destination hosts, and the percentage of all traffic observed for this source and the destination hosts.

The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

**Figure 174 Source Host TopN Applications Communicating with Source Host**

Traffic Details

| Top 10 Destination Hosts Communicating with the Source Host                                    |         |            |                        | Top 10 Applications Communicating with the Source Host |         |                               |
|------------------------------------------------------------------------------------------------|---------|------------|------------------------|--------------------------------------------------------|---------|-------------------------------|
| Destination                                                                                    | Traffic | Percentage |                        | Application Name                                       | Traffic | Percentage                    |
|  172.8.112.35 | 0.61 MB | 13.96%     | <div><div></div></div> | Telnet                                                 | 2.57 MB | 59.11% <div><div></div></div> |
|  172.8.112.5  | 0.49 MB | 11.22%     | <div><div></div></div> | snmp                                                   | 1.39 MB | 31.90% <div><div></div></div> |
|  172.8.112.2  | 0.48 MB | 11.05%     | <div><div></div></div> | ICMP Protocol Application                              | 0.37 MB | 8.61% <div><div></div></div>  |
|  172.8.112.34 | 0.39 MB | 9.06%      | <div><div></div></div> | UDP Protocol Unknown Application                       | 7.57 KB | 0.17% <div><div></div></div>  |
|  172.8.112.45 | 0.30 MB | 6.95%      | <div><div></div></div> | TCP Protocol Unknown Application                       | 5.41 KB | 0.12% <div><div></div></div>  |
|  172.10.0.60  | 0.28 MB | 6.44%      | <div><div></div></div> | echo                                                   | 4.26 KB | 0.10% <div><div></div></div>  |
|  172.8.112.10 | 0.18 MB | 4.18%      | <div><div></div></div> |                                                        |         |                               |
|  172.8.112.7  | 0.17 MB | 3.96%      | <div><div></div></div> |                                                        |         |                               |
|  172.8.112.17 | 0.14 MB | 3.30%      | <div><div></div></div> |                                                        |         |                               |
|  172.8.112.13 | 0.14 MB | 3.22%      | <div><div></div></div> |                                                        |         |                               |
| Other Hosts                                                                                    | 1.16 MB | 26.65%     | <div><div></div></div> |                                                        |         |                               |

## Destination reports

Destination reports include inbound and outbound reports. The inbound report includes the **TopN Traffic Report for Destination Host** bar/pie chart. This bar chart displays the average rate of traffic sent to the hosts configured in the task by any other hosts. The pie chart displays the distribution of traffic sent to the hosts configured in the task by any other hosts.

The inbound report includes the **TopN Traffic List for Destination Host**, which provides a list showing volume and percentage of traffic sent to each of the TopN destination hosts that configured in the selected task by any other hosts. The outbound report also includes the **TopN Traffic Report for Destination Host** bar/pie chart.

This bar chart displays the average rate of traffic sent to the TopN destination hosts by the hosts configured in the task. This pie chart displays the distribution of traffic sent to the TopN destination hosts by the hosts configured in the task.

The outbound report also includes the **TopN Traffic List for Destination Host**, which provides a list showing volume and percentage of traffic sent to each of the TopN destination hosts by the hosts that configured in the selected task. These lists also contain a link to reports for the selected destination

host. The host query icon  next to the destination IP address is a link for initiating a host query and a link to the results of the host query. NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a host traffic analysis task, click the **Destination** tab to view traffic reports for the selected host traffic analysis task.

### Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed under the **Destination** tab.

1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.

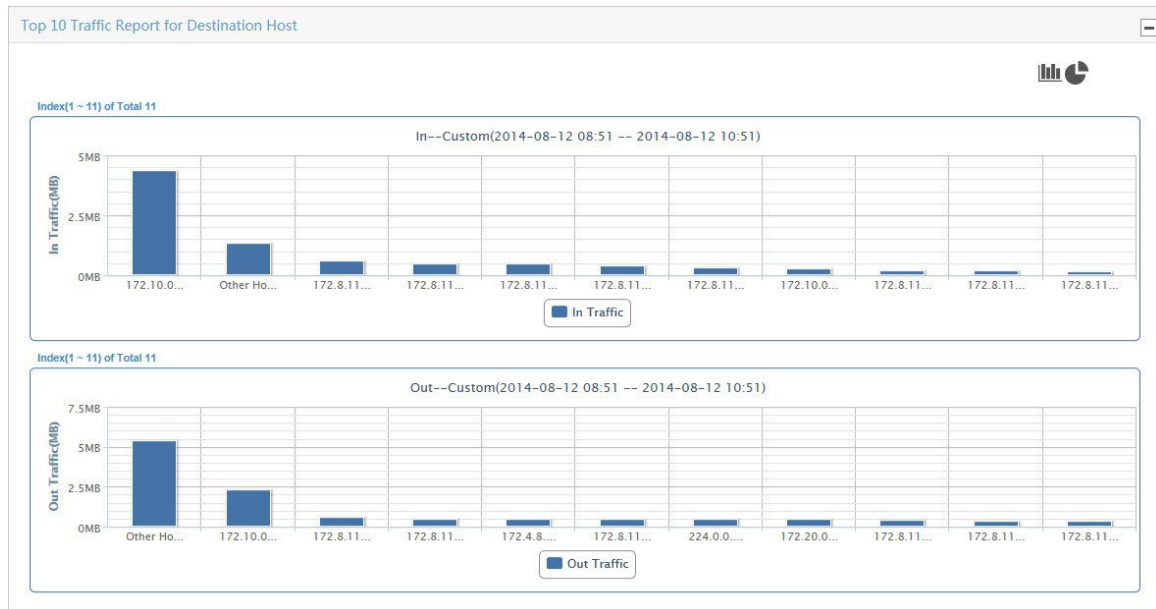
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Destination Host**—In the **Destination Host** field, enter the IP address or address range. To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24  
Example of a valid IPv6 address:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
  - f. From **Page Range**, select the page range.
  - g. Click **Export**.

#### TopN traffic Report for Destination Host

The **TopN Traffic Report for Destination Host – In/Out** bar chart displays the average rate of inbound/outbound traffic for TopN destination hosts for all hosts in the selected traffic analysis task

for the selected time range. The pie chart icon  is a link to display the **TopN Traffic Report for Destination Host – In/Out** data as a pie chart.

**Figure 175 TopN Traffic Report for Destination Host – In/Out**



The **TopN Traffic Report for Destination Host – In/Out** pie chart displays the distribution of inbound/outbound traffic for TopN destination hosts for all hosts in the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the selected host.

### TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host In/Out** provides a list of the TopN destination hosts measured by volume of inbound/outbound traffic observed for all hosts in the selected host traffic analysis task for the selected time range. This list includes the host IP address, total volume of traffic generated by the associated destination host, and the percentage of all observed traffic generated by the destination host.

The IP address is a link to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and a link to the results of the host query.

**Figure 176 TopN Traffic List for Destination Host – In/Out**

| Top 10 Traffic List for Destination Host                                                         |         |            |                                                                                                  |         |            |
|--------------------------------------------------------------------------------------------------|---------|------------|--------------------------------------------------------------------------------------------------|---------|------------|
| In                                                                                               |         |            | Out                                                                                              |         |            |
| Destination                                                                                      | Traffic | Percentage | Destination                                                                                      | Traffic | Percentage |
|  172.10.0.69  | 4.35 MB | 49.81%     |  172.10.0.69  | 2.32 MB | 19.75%     |
|  172.8.112.35 | 0.61 MB | 6.96%      |  172.8.112.35 | 0.60 MB | 5.13%      |
|  172.8.112.5  | 0.49 MB | 5.60%      |  172.8.112.5  | 0.48 MB | 4.13%      |
|  172.8.112.2  | 0.48 MB | 5.51%      |  172.4.8.88   | 0.48 MB | 4.11%      |
|  172.8.112.34 | 0.39 MB | 4.52%      |  172.8.112.2  | 0.48 MB | 4.06%      |
|  172.8.112.45 | 0.30 MB | 3.47%      |  224.0.0.5    | 0.48 MB | 4.05%      |
|  172.10.0.60  | 0.28 MB | 3.21%      |  172.20.0.24  | 0.46 MB | 3.96%      |
|  172.8.112.10 | 0.18 MB | 2.08%      |  172.8.112.34 | 0.39 MB | 3.36%      |
|  172.8.112.7  | 0.17 MB | 1.98%      |  172.8.111.36 | 0.34 MB | 2.88%      |
|  172.8.112.17 | 0.14 MB | 1.64%      |  172.8.111.42 | 0.32 MB | 2.77%      |
| Other Hosts                                                                                      | 1.33 MB | 15.23%     | Other Hosts                                                                                      | 5.38 MB | 45.81%     |

### Traffic Trend Report for Destination Host

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Destination** host report page, click **Back**.

**Figure 177 Traffic Trend Report for Destination Host**



## Traffic Details

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Details** for a destination host table shows two lists. The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.

The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.



**Figure 178 Traffic Details**

| Traffic Details                                                                                |         |                                                                                          |                                                             |          |                                                                                            |
|------------------------------------------------------------------------------------------------|---------|------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------|
| Top 10 Source Hosts Communicating with the Destination Host                                    |         |                                                                                          | Top 10 Applications Communicating with the Destination Host |          |                                                                                            |
| Source                                                                                         | Traffic | Percentage                                                                               | Application Name                                            | Traffic  | Percentage                                                                                 |
|  172.8.112.35 | 0.30 MB | 6.82%   | snmp                                                        | 1.99 MB  | 45.82%  |
|  172.10.0.60  | 0.28 MB | 6.45%   | Telnet                                                      | 1.70 MB  | 39.05%  |
|  172.4.8.88   | 0.27 MB | 6.31%   | ICMP Protocol Application                                   | 0.55 MB  | 12.72%  |
|  172.8.112.5  | 0.23 MB | 5.27%   | AH Protocol Application                                     | 49.19 KB | 1.10%   |
|  172.8.112.2  | 0.22 MB | 5.08%   | echo                                                        | 34.29 KB | 0.77%   |
|  172.20.0.24  | 0.20 MB | 4.69%   | GRE Protocol Application                                    | 15.15 KB | 0.34%   |
|  172.8.112.34 | 0.17 MB | 3.84%   | UDP Protocol Unknown Application                            | 7.57 KB  | 0.17%   |
|  172.4.21.10  | 0.16 MB | 3.77%   | isakmp                                                      | 0.73 KB  | 0.02%   |
|  172.8.111.36 | 0.16 MB | 3.63%   |                                                             |          |                                                                                            |
|  38.0.0.2     | 0.15 MB | 3.43%   |                                                             |          |                                                                                            |
| Other Hosts                                                                                    | 2.21 MB | 50.70%  |                                                             |          |                                                                                            |

## Session reports

A session is a unique source and destination host pair. Session reports include inbound and outbound reports. The inbound report presents the **TopN Traffic Report for Session Host** in a bar or pie chart. The bar chart displays the TopN source and destination session pairs with the most inbound traffic on all hosts in a certain period of time in a selected host traffic analysis task. The pie chart displays the distribution of traffic generated by the TopN source/destination pairs with destination hosts configured in the selected task.

The inbound report also includes **TopN Traffic List for Session Host**, which provides a list of TopN session hosts measured by volume and percentage of traffic generated by the TopN source/destination pairs with destination hosts configured in the selected task.

The outbound report also presents the **TopN Traffic Report for Session Host** in a bar or pie chart. The bar chart displays the TopN source and destination session pairs with the most outbound traffic on all hosts in a certain period of time in a selected host traffic analysis task. The pie chart displays the distribution of traffic generated by the TopN source/destination pairs with source hosts configured in the selected task. The outbound report includes **TopN Traffic List for Session Host**, which provides a list of TopN session hosts measured by volume and percentage of traffic generated by the TopN source/destination pairs with source hosts configured in the selected task.

These lists also contain a link to reports for the selected session host. The host query icon  next to the **Source Host** IP address is a link for initiating a host query and a link to the results of the host query. NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a host traffic analysis task, click the **Session** tab to view traffic reports for the selected host traffic analysis task.

### Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.

3. Specify one or more of the following query criteria:
  - o **Source Host**—In the **Source Host** field, enter the IP address or address range. To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24  
Example of a valid IPv6 address:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
  - f. From **Page Range**, select the page range.
  - g. Click **Export**.

#### TopN Traffic Report for Session Host

The **TopN Traffic Report for Source Host – In/Out** bar chart displays the TopN source and destination session pairs with the most inbound/outbound traffic on all hosts in a certain period of time in a selected host traffic analysis task. Click a bar in the bar chart to view the traffic analysis report of each source and destination session pair.



Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic for TopN source and destination session pairs for all hosts in the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the select source and destination session pair.

**Figure 179 TopN Traffic Report for Session Host – In/Out**



## TopN Traffic List for Session Host

The **TopN Traffic List for Session Host – In/Out** provides a list of the TopN session source and destination pairs measured by volume of inbound/outbound traffic observed on all hosts in the selected host traffic analysis task for the selected time range. This list includes the source and destination host IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair.

The **Details** icon  is a link for viewing reports for the selected session or source/destination pair.

The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link to the results of the host query.

**Figure 180 TopN Traffic Report for Session Host – In/Out**

| Top 10 Traffic List for Session Host                                                              |                                                                                                   |          |            |                                                                                     |                                                                                     |                                                                                                   |                                                                                                   |          |            |                                                                                       |                                                                                       |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------|------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------|------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| In                                                                                                |                                                                                                   |          |            |                                                                                     |                                                                                     | Out                                                                                               |                                                                                                   |          |            |                                                                                       |                                                                                       |
| Generate Chart                                                                                    |                                                                                                   |          |            |                                                                                     |                                                                                     | Generate Chart                                                                                    |                                                                                                   |          |            |                                                                                       |                                                                                       |
| Source Host                                                                                       | Destination Host                                                                                  | Traffic  | Percentage | Details                                                                             | Topology                                                                            | Source Host                                                                                       | Destination Host                                                                                  | Traffic  | Percentage | Details                                                                               | Topology                                                                              |
|  192.168.8.23  |  192.168.8.200 | 11.58 MB | 9.64%      |  |  |  192.168.8.23  |  192.168.8.200 | 11.58 MB | 9.77%      |  |  |
|  192.168.8.25  |  192.168.8.200 | 9.91 MB  | 8.25%      |  |  |  192.168.8.25  |  192.168.8.200 | 9.91 MB  | 8.36%      |  |  |
|  192.168.8.23  |  172.30.4.9    | 8.36 MB  | 6.96%      |  |  |  192.168.8.23  |  172.30.4.9    | 8.36 MB  | 7.05%      |  |  |
|  172.30.4.31   |  192.168.7.154 | 5.73 MB  | 4.77%      |  |  |  172.30.4.31   |  192.168.7.154 | 5.73 MB  | 4.83%      |  |  |
|  192.168.7.159 |  192.168.7.158 | 2.45 MB  | 2.04%      |  |  |  192.168.7.159 |  192.168.7.158 | 2.45 MB  | 2.07%      |  |  |
|  192.168.7.159 |  192.168.7.156 | 2.30 MB  | 1.92%      |  |  |  192.168.7.159 |  192.168.7.156 | 2.30 MB  | 1.94%      |  |  |
|  192.168.7.159 |  192.168.7.155 | 1.34 MB  | 1.11%      |  |  |  192.168.7.159 |  192.168.7.155 | 1.34 MB  | 1.13%      |  |  |
|  192.168.7.159 |  192.168.7.157 | 1.13 MB  | 0.94%      |  |  |  192.168.7.159 |  192.168.7.157 | 1.13 MB  | 0.96%      |  |  |
|  192.168.7.155 |  192.168.7.159 | 1.11 MB  | 0.92%      |  |  |  192.168.7.155 |  192.168.7.159 | 1.11 MB  | 0.93%      |  |  |
|  172.22.8.61   |  192.168.7.148 | 1.10 MB  | 0.91%      |  |  |  172.22.8.61   |  192.168.7.148 | 1.10 MB  | 0.92%      |  |  |
| Other Hosts                                                                                       | Other Hosts                                                                                       | 75.12 MB | 62.54%     |                                                                                     |                                                                                     | Other Hosts                                                                                       | Other Hosts                                                                                       | 73.58 MB | 62.05%     |                                                                                       |                                                                                       |

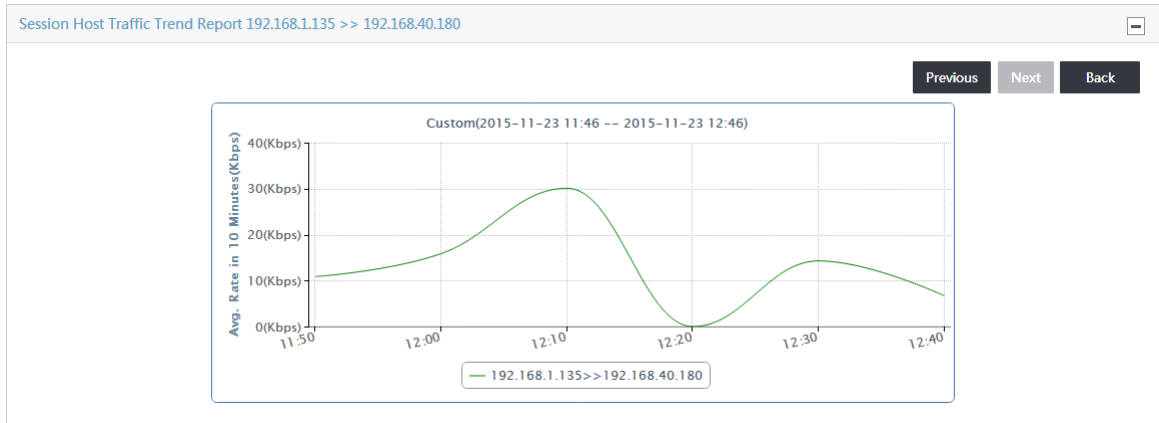
Session Host Traffic Trend Report

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Host Traffic Trend Report** chart displays statistics for the previous hour.

- In the upper right corner of the chart, click **Previous** to view data for an earlier period.
- In the upper right corner of the chart, click **Next** to view data for a later period.
- To return to the main **Session** report page, click **Back**.

Figure 181 Session Host Traffic Trend Report



TopN Applications for Session Host

To view this report for a host traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

Figure 182 TopN Applications for Session Host

| Top 10 Applications for Session Host 192.168.1.135 >> 192.168.40.180 |         |                                |
|----------------------------------------------------------------------|---------|--------------------------------|
| Application Category                                                 | Traffic | Percentage                     |
| TCP Protocol Unknown Application                                     | 5.56 MB | 100.00% <div><div></div></div> |

Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source and destination hosts.

# VPN monitoring

This chapter explains the NTA VPN monitoring features. It provides an overview of how NTA analyzes network flow data from the viewpoint of a VPN, and it describes the report structure for VPN traffic analyses. It reviews configuration issues around VPN analysis tasks and the reports they generate. It describes the process for adding VPN traffic analysis tasks, including instructions for adding, modifying, and deleting VPN tasks in NTA. Finally, it describes the summary reports for all VPN tasks and the more detailed reports for an individual VPN traffic analysis task.

## VPN traffic analysis overview

VPN traffic analysis tasks capture and analyze network flow data for VPNs. In general, the NTA VPN traffic analysis tasks provide traffic statistics for the VPNs configured in a VPN traffic analysis task. The VPN traffic reports include rate of traffic for all VPNs in all tasks and for all VPNs in a task. VPN statistics include traffic rate by application, source host, destination host, and a session or source/destination host pair. These reports are organized into layers from summarized information for all tasks to detailed reporting for specific VPNs configured for an individual VPN traffic analysis task.

## VPN traffic analysis reporting overview

After you create the first VPN traffic analysis task, NTA creates an entry called  **VPN Traffic Analysis Task** under the **Traffic Analysis and Audit** area on the left navigation tree.

Click **VPN Traffic Analysis Task** on the left navigation tree to view the summary report for all VPN traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **VPN Traffic Analysis Task**. The **VPN Traffic Analysis Task** shortcut menu displays all VPN traffic analysis tasks created in NTA. Click the name of a task to view the VPN traffic analysis report of the task.

The summary VPN traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—Summarizes the average rate per second reporting for all VPNs specified in all VPN traffic analysis tasks summarized by task. Each bar in the graph is a link to more detailed reporting for the selected task, including reporting for traffic rates, application, source, destination, and session statistics. Each of these detailed report types also include several reports for the selected task:
  - **Traffic**—Reports found under the **Traffic** tab for VPN reporting include traffic trends that display the average inbound and outbound rate per second and the individual data samples for the VPNs for the selected task.
  - **Application**—Reports found under the **Application** tab for VPN reporting include a tabular report displaying percentage of application traffic generated by all VPNs in a task and a graph displaying average rate of application traffic for all VPNs in the selected task.
  - **Source**—Reports found under the **Source** tab for VPN reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN source hosts and a table displaying volume and percentage of traffic generated for each of the TopN source hosts for all VPNs in the selected task. The contents of the pie chart link to more detailed reporting for the selected host.
  - **Destination**—Reports found under the **Destination** tab for VPN reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN destination hosts and a table displaying volume and percentage of traffic generated for each of the TopN destination hosts for all VPNs in the selected task. The contents of the pie chart link to more detailed reporting for the selected host.

- **Session**—Reports found under the **Session** tab for VPN reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN source and destination host pairs and a table displaying volume and percentage of traffic generated for each of the TopN source and destination host pairs for all VPNs in the selected task. The contents of the pie chart link to more detailed reporting for the selected host.
- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—Provides per second average traffic rate summarized by VPN traffic analysis task for inbound and outbound traffic for all VPNs for all tasks. A second set of pie charts reveals the distribution of traffic for the TopN applications, with one chart each for inbound and outbound traffic.
- **VPN Flux Distribution in Interfaces**—Can contain multiple VPN instances, and each VPN instance can contain multiple interfaces. The table displayed here displays the traffic statistics for every VPN instance for all interfaces of this task.
- **Interface Flux Distribution in VPNs**—Displays the traffic information for every interface for all VPN instances of this task.
- **Summary List (Last 1 Hour)**—Provides per second traffic rate of traffic statistics summarized by VPN traffic analysis task for inbound and outbound traffic for all VPNs for all tasks.

## VPN traffic analysis configuration considerations

Determining which VPNs belong to each task is the most important consideration. You must also consider the following:

- By default, NTA does not monitor any VPNs. Therefore, to monitor VPNs, you must create a task for every VPN or group of VPNs on which you want to monitor and report. If you do not add a VPN to a task, NTA does not report on it.
- NTA presents VPN traffic analysis in the NTA's left navigation system, and provides summarized VPN reporting based on the way you organized tasks. You define how NTA groups VPNs and presents them for viewing.
- You are not limited to adding VPNs from a single device into one task. You can group one or more VPNs from different devices into a single task.
- Consider how you want to access and view VPN data, and then structure your tasks around it. For example, if you want to view VPN traffic statistics by geography, group the VPNs into tasks organized by location. You can create a single task for every device, and add all VPNs from that device whose statistics you want to view into the task. Also, you can create a task for every VPN if you need more detailed reporting for a VPN.
- Add only those VPNs whose statistics you want to view. Do not add all VPNs on a device unless you want to view reporting for all VPNs. Adding VPNs for which you don't want to view statistics only clutters NTA's VPN navigation. This makes it more difficult for you to find the VPN for which you want to view data.
- When you add VPNs to a task, NTA will show you a list of all devices that NTA knows about. The list is generated from the devices that have been added to NTA using the Device Management feature. If this list does not contain the devices you want to select, it is most likely because the device has not been added to NTA or it has not been selected in the NTA server configuration found under server management. For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."
- You must enable network flow data on the devices for the VPNs you want to monitor and report on.

# Managing VPN traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA does not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need. This section describes the process for adding, modifying, or removing VPN traffic analysis tasks in NTA.

## Viewing a traffic analysis task

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view a traffic analysis task:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the Task Management page.

### Task list contents

- **Task Name**—Contains the name of the task. The contents of this field link to the **Traffic Analysis Task Details** page for the associated task.
  - **Task Description**—Contains the description for the associated task.
  - **Task Type**—Options are:
    - **Interface**
    - **VLAN/VXLAN**
    - **Probe**
    - **Application**
    - **Host**
    - **VPN**
    - **Inter-Business**
    - **BGP AS**
  - **Baseline Analysis**—Displays when the Baseline Analysis feature is enabled in NTA parameters. The Baseline Analysis feature provides an additional layer of analysis to reports provided by NTA by including baseline trend data when data has been collected for a minimum of one week.
  - **Modify**—Contains an icon  for modifying the associated task.
  - **Delete**—Contains an icon  for deleting the associated task.
3. In the upper left corner of the **Traffic Analysis Task List**, click **Refresh** to query NTA for the most recent **Traffic Analysis Task List**.

You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. The column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Viewing VPN traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

3. In the **Task Name** field of the **Traffic Analysis Task List**, click the contents of the **VPN Task Type** to view the details for an individual task.  
**Traffic Analysis Task Details** page
  - **Task Name**—Contains the name of the task.
  - **Task Description**—Contains the description for the associated task.
  - **Server**—Contains the server name or IP address of the NTA server.
  - **Task Type**—Options are:
    - **Interface**
    - **VLAN/VXLAN**
    - **Probe**
    - **Application**
    - **Host**
    - **VPN**
    - **Inter-Business**
    - **BGP AS**
  - **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by this traffic analysis task.
  - **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Enable Baseline Analysis** field is not displayed, it is because the Baseline Analysis feature is disabled on the NTA server. For more information on configuration options for the NTA server, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
  - **VPN Instance List**—Identifies the VPNs and their IP addresses, VPN IDs, and descriptions configured for this traffic analysis task.
4. Click **Back** to return to the **Traffic Analysis Task List**.

## Adding a VPN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
 NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.  
 The **Add Traffic Analysis Task** page is displayed.
4. To add a VPN traffic analysis task, select the option next to **VPN** in the **Select Task Type** area.
5. Click **Next**.  
 The **Add Traffic Analysis Task** page is refreshed.
6. In the **Task Name** field, enter a name for this task.  
 The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. In the **Task Description** field, enter a description for this task.
8. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.  
 Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.

9. Next to the **Reader** field, click **Select** to select the operator groups that have access to the analysis and reports provided by this host task.

The **Operator Group List** dialog box opens.

- a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.
- b. To select all operator groups, select the box located in the upper left corner of the column label field for all boxes.
- c. Click **OK** to accept your operator group selection.

The operator groups you selected are displayed in the **Reader** field.

10. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; select **Disable** to disable the Baseline Analysis feature.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

You can configure a VPN traffic analysis task to include traffic from one or more VPNs defined by the VPN ID. You must have at least one VPN defined.

For information about organizing VPNs into tasks, see "[VPN traffic analysis configuration considerations](#)."

11. At the top of the **VPN Instance List**, click **Add** to add a VPN.

The **VPN Instance Set** dialog box opens.

- a. From the **Device Name** list, select the device on which the VPN is configured.  
For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration found under server management. For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)." The device you want to add must be configured to forward NetStream, NetFlow or sFlow traffic to NTA as the traffic collector or collection server.
- b. In the **VPN ID** field, enter the VPN ID.
- c. In the **Description** field, enter a description for this VPN.
- d. Click **OK** to add the VPN to the VPN list for the VPN traffic analysis task.
- e. Repeat this step for every VPN you want to add to the VPN traffic analysis task.

12. Click **OK** to create the VPN traffic analysis task.

After you create a VPN traffic analysis task, NTA creates an entry called  **VPN Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the VPN traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon >>> next to  **VPN Traffic Analysis Task**. The **VPN Traffic Analysis Task** shortcut menu displays all VPN traffic analysis tasks created in NTA. Click the name of a task to view the VPN traffic analysis report of the task.

For information about accessing and viewing VPN traffic analysis reports, see "[Viewing VPN traffic analysis reports](#)."

# Modifying a VPN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  for the task you want to modify.
4. Modify the name for this task in the **Task Name** field as needed. The task name must be unique.

The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
5. In the **Task Description** field, modify the description for this task.
6. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.

Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add a new operator groups that will have access to the analysis and reports provided by this host task, click **Select** next to the **Reader** field.

The **Operator Group List** dialog box opens.

  - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.
  - b. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
  - c. Click **OK** to accept your operator group selection.

The operator groups you selected are displayed in the **Reader** field.
  - d. To revoke operator group access to the results of this traffic analysis task, highlight the groups in the **Reader** field you want to remove.
  - e. Click **Delete**.
  - f. Click **OK** to confirm the deletion of the selected operator groups from the task.

The **Reader** reflects the deleted operator group changes.
8. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task; to disable the Baseline Analysis feature, select **Disable**.

If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week's collection and is adjusted over time as more data is collected.

If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
9. To add a VPN, click **Add** located at the top of the **VPN Instance List**. You must have at least one VPN instance defined. The **VPN Instance Set** dialog box is displayed.
  - a. Select the device on which the VPN is configured from the Device Name list.

For a device to be displayed on this list, the device must first be added to NTA using the Device Management feature. Then, the device must be selected in the NTA server configuration found under server management. For more information on adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)." The device you want to add must be configured to forward NetStream, NetFlow, or sFlow traffic to NTA as the traffic collector or collection server.



- b. Enter the VPN ID in the **VPN ID** field.
  - c. Enter a description for this VPN in the **Description** field.
  - d. Click **OK** to add the VPN to the VPN list for the VPN traffic analysis task
  - e. Repeat this step for every VPN you want to add to the VPN traffic analysis task.  
For information about organizing VPNs into tasks, see "[VPN traffic analysis configuration considerations](#)."
  - f. To remove a VPN from the VPN list and task, click the **Delete** icon  for the VPN you want to delete.
10. Click **OK** to accept your modifications to the VPN traffic analysis task.

## Deleting a VPN traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the task you want to delete.
4. Click **OK** to confirm the deletion of the selected VPN traffic analysis task.  
The **Traffic Analysis Task List** reflects the deletion of the selected task.

## Viewing VPN traffic analysis reports

NTA provides various levels of reporting for all traffic analysis tasks. The highest level provides summarized reporting for all tasks of the same type whether the task type is interface, VLAN/VXLAN, application, probe, host, VPN, interbusiness or BGP AS. To view summarized reporting for all VPN tasks, click the  **VPN Traffic Analysis Task** entry of the left navigation tree.

NTA also provides more granular reporting for individual tasks, including reports for every VPN configured in a VPN traffic analysis task. NTA groups individual tasks by type. All VPN tasks can be found on the **VPN Traffic Analysis Task** menu.

To view the **VPN Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to  **VPN Traffic Analysis Task**. The shortcut menu displays all VPN traffic analysis tasks created in NTA. Click the name of a task to view the VPN traffic analysis report of the task.

This section describes the reporting options available for VPN traffic analysis tasks. It also describes the process for navigating to VPN traffic analysis tasks, the summary reports available for VPN tasks, and the reports and features available for a VPN traffic analysis task.

## Navigating to the VPN traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Under the **Traffic Analysis and Audit** area of the left navigation tree, click the  **VPN Traffic Analysis Task** entry to view summary reporting for all VPN tasks.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to  **VPN Traffic Analysis Task**. The **VPN Traffic Analysis Task** shortcut menu displays all VPN traffic analysis tasks created in NTA. Click the name of a task to view the VPN traffic analysis report of the task.

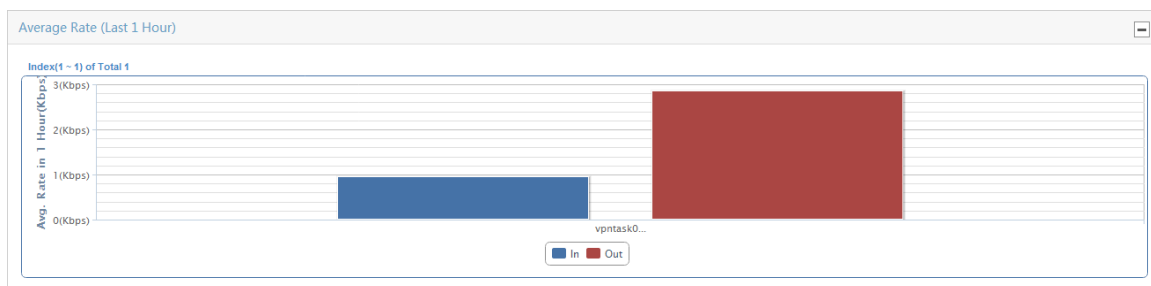
# Summary reports for all VPN tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **VPN Traffic Analysis Task** entry of the left navigation tree under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

## Average Rate (Last 1 Hour)

The **Average Rate (Last 1 Hour)** bar graph summarizes traffic rates for all VPNs in every VPN traffic analysis task, grouped by VPN traffic analysis task for the last hour. You can access this graph by clicking the  **VPN Traffic Analysis Task** entry of the left navigation tree at the top of the page. The bars in the graph link to the reports for the selected task.

**Figure 183 Average Rate (Last 1 Hour)**



## Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

The **Traffic Trend – In** line chart provides inbound traffic trend rates for all VPN traffic analysis tasks for the last hour.

The **Traffic Trend – Out** line chart provides outbound traffic rates for all VPN traffic analysis tasks for the last hour.

The **TopN Application – In** pie chart displays the distribution of traffic for the TopN applications for all VPN traffic analysis tasks for the last hour. The slices in the pie chart are links for navigating to the reports for the selected application.

The **TopN Applications – Out** pie chart displays the distribution of traffic for the TopN applications for the selected VPN task for the last hour. The slices in the pie chart are links for navigating to the reports for the selected application.

**Figure 184 TopN Application for Selected Task**



All VPN tasks are graphed on these charts until you specify a task.

1. In the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar, click the **Select Task** link to select the task.  
The **Choose NTA Task** dialog box opens.
2. Select the check box next to the host task for which you want to view this report.
3. Click **OK**.  
The page displays the **Traffic Trend – In**, **Traffic Trend – Out**, **TopN Application – In**, and **TopN Application – Out** reports for the selected task.

## VPN Flux Distribution in Interfaces

The **VPN Flux Distribution In Interfaces** table provides the total volume of inbound and outbound traffic for all interfaces in all VPNs.

**Figure 185 VPN Flux Distribution in Interfaces**

| VPN Flux Distribution In Interfaces (Last 1 Hour) |         |         |          |
|---------------------------------------------------|---------|---------|----------|
| VPN/Interface                                     | In      | Out     | Subtotal |
| 10(10.153.150.13)                                 | 0.00 B  | 1.22 MB | 1.22 MB  |
| 20(10.153.150.13)                                 | 0.41 MB | 0.00 B  | 0.41 MB  |

## Interface Flux Distribution in VPNs

The **Interface Flux Distribution In VPNs** table provides the total volume of inbound and outbound traffic for all VPNs grouped by interface.

**Figure 186 VPN Flux Distribution in VPNs**

| Interface Flux Distribution In VPNs (Last 1 Hour) |         |         |          |
|---------------------------------------------------|---------|---------|----------|
| Interface/VPN                                     | In      | Out     | Subtotal |
| vpntask001                                        | 0.00 B  | 1.22 MB | 1.22 MB  |
| vpntask001                                        | 0.41 MB | 0.00 B  | 0.41 MB  |

## Summary List (Last 1 Hour)

The **Summary List** provides inbound and outbound traffic rates statistics summarized by VPN task for the last hour.

### Summary List Contents

- **Task Name**—Contains the name of the VPN traffic analysis task. The contents of this field link to reports for the associated task.
  - **Total Rate**—Provides the combined inbound and outbound traffic for all VPNs configured for the associated task.
  - **In Rate**—Provides the rate of inbound traffic for all VPNs configured for the associated task.
  - **Out Rate**—Provides the rate of outbound traffic for all VPNs configured for the associated task.
  - **Traffic Log Audit**—Contains the  **Traffic Log Audit** icon. The icon is a link to the **Traffic Log Audit** result page.
1. Click **Add** at the top of the **Summary List** to open the **Add Traffic Analysis Task** page. For more information on adding VPN traffic analysis tasks, see "[Adding a VPN traffic analysis task.](#)"
  2. Click **Refresh** to update the reports with the most recent data.
  3. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
    - a. To print this report, click the **Print** icon  on the toolbar.
    - b. From **Page Range**, select the page range.
    - c. To export the data, click **Export**.
    - d. To export this report, click the **Export** icon  on the toolbar.
    - e. From the **File Format** list, select the export file format. Options are:
      - **PDF**
      - **XLS**
      - **CSV**
      - **DOCX**
      - **RTF**
      - **XLSX**
      - **PPTX**
      - **HTML**
      - **JRXML**
    - f. Select the desired page range from **Page Range**.
    - g. Click **Export**.

## Granular reports for a VPN traffic analysis task

NTA provides a suite of reports for viewing VPN data from different perspectives. Reports for VPNs are organized into the following reporting groups: traffic, application, source, destination, and session.

- Traffic reports for VPN tasks provide overall traffic trends and statistics, including details for the selected task for the selected time range.
- Application reports include the average traffic rate trend for the last hour by default though operators can configure the time range. Application reports also enable you to get the details for unknown applications if the unknown application traffic analysis parameter is enabled in the parameter management.

- Source reports include the TopN source hosts chart and list for all VPNs in a task for the selected time range.
- Destination reports include the TopN source hosts chart and list for all VPNs in a task for the selected time range.
- Session reports include the TopN session hosts chart and list for all VPNs in a task for the selected time range.

Source, destination, and session reports enable you to get detailed traffic reports for an individual host and session.

## Traffic reports

Traffic reports for VPN tasks provide overall traffic statistics for all VPNs configured in a VPN traffic analysis task. Traffic reports for a VPN traffic analysis task include the Traffic Trendline chart that provides inbound and outbound traffic rates for all VPNs in the selected traffic analysis task. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for both inbound and outbound traffic for the associated task. The traffic reports include the **Traffic Details** List that provides the data collection samples that includes timestamp, total volume of traffic, and traffic rate in seconds. You can filter reports by time range.

To view the reports for a VPN task, click the **Traffic** tab to view traffic reports for the selected VPN traffic analysis task.

### Query traffic

NTA enables you to change the filter criteria for VPN traffic reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed under the **Traffic** tab.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
  - a. Specify the following query criteria:
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
  - b. Click **OK**.  
The page displays the results of your query.
3. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. Select the desired page range from **Page Range**.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. From the **File Format** list, select the export file format. Options are:
    - **PDF**

- XLS
- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

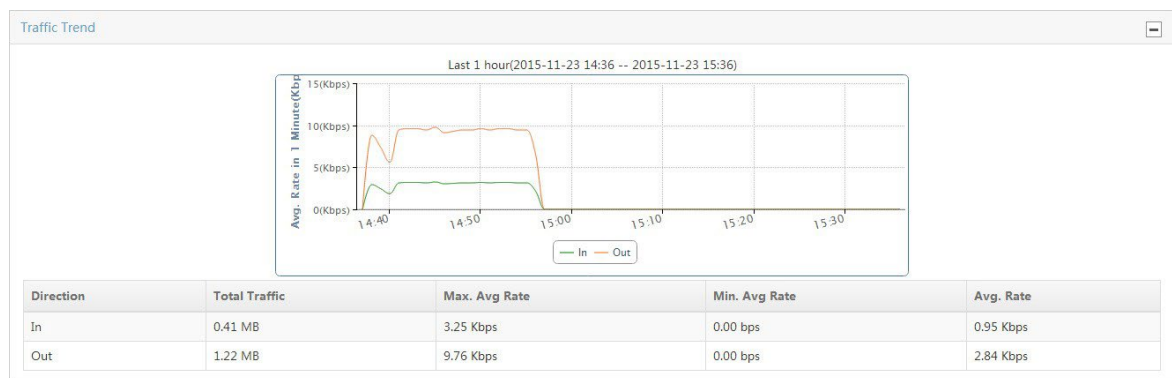
f. Select the desired page range from **Page Range**.

g. Click **Export**.

### Traffic Trend – Average

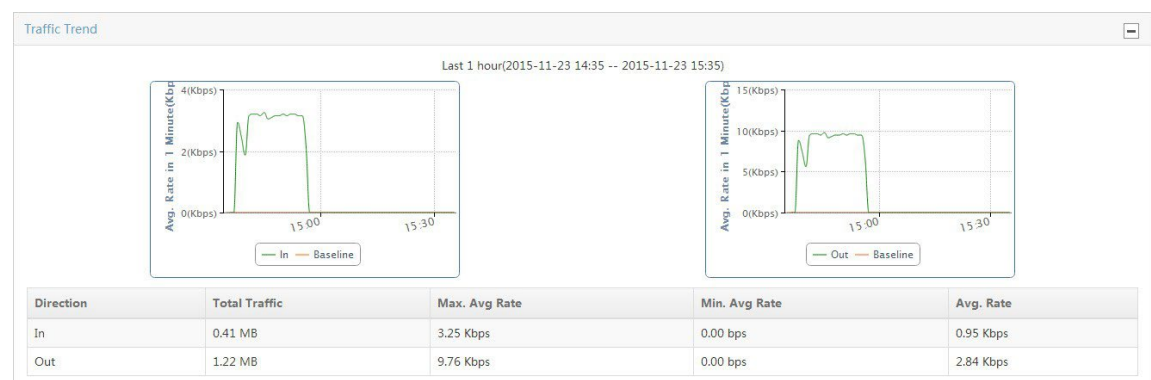
The **Traffic Trend** combination chart provides average rate statistics for both inbound and outbound traffic for all VPNs in the selected traffic analysis task. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for both inbound and outbound traffic for all VPNs in the associated task for the selected time range. If more than one VPN exists for the selected task, these statistics will reflect traffic for all VPNs configured in a task.

**Figure 187 Traffic Trend Report**



If the selected traffic analysis task enabled the Baseline Analysis feature, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. The green line is the baseline and the red area is the average traffic rate. For more information on configuring the Baseline Analysis feature for the VPN traffic analysis task, see ["Adding a VPN traffic analysis task."](#)

**Figure 188 Traffic Trend Report**



By default, the Traffic Trend chart displays statistics for the previous hour.

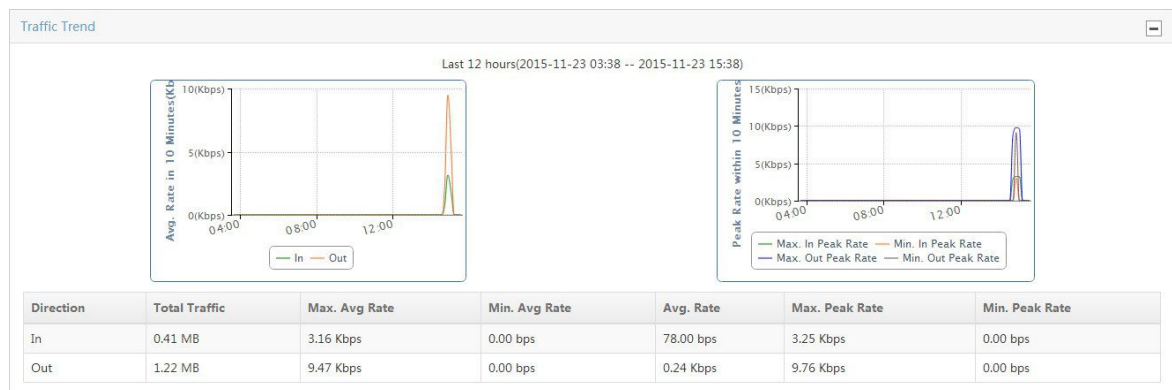
- To view data for an earlier period, click **Previous** located in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** located in the upper right corner of the **Traffic Trend** chart.

### Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

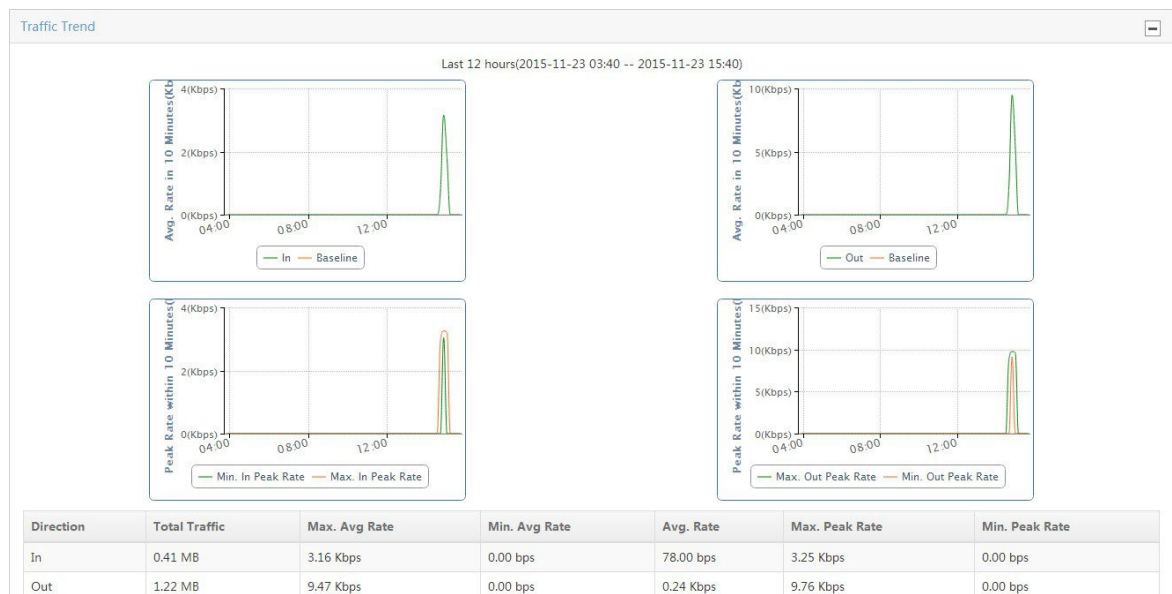
The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range for both inbound and outbound traffic. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

**Figure 189 Traffic Trend – Peak Rate Report**



If the selected traffic analysis task enabled the Baseline Analysis feature, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. NTA displays the **Max./Min. In Peak Rate** chart and **Max./Min. Out Peak Rate** chart under the **Traffic Trend** chart. For more information on configuring the Baseline Analysis feature for the VPN traffic analysis task, see ["Adding a VPN traffic analysis task."](#)

**Figure 190 Traffic Trend – Peak Rate Report**



- To view data for an earlier period, click **Previous** located in the upper right corner of the **Traffic Trend** chart.



- To view data for a later period, click **Next** located in the upper right corner of the **Traffic Trend** chart.

For more information on enabling Peak Traffic Analysis, see "[Configuring NTA traffic analysis parameters](#)."

### TopN Traffic List for ToS/MPLS Exp

If you have enabled the ToS/MPLS Exp Traffic Analysis feature, NTA displays the **TopN Traffic List for ToS/MPLS Exp** tabular list. The **TopN Traffic List for ToS/MPLS Exp** provides administrators with a tabular view of total traffic volume and percentage of total traffic volume grouped by ToS or MPLS Exp for both inbound and outbound traffic for the selected time range for a VPN traffic analysis task.

**Figure 191 TopN Traffic List for ToS/MPLS Exp**

| Top 10 Traffic List for ToS/MPLS Exp |         |                                                                                           |                         |         |                                                                                             |
|--------------------------------------|---------|-------------------------------------------------------------------------------------------|-------------------------|---------|---------------------------------------------------------------------------------------------|
| ToS/MPLS Exp Flux - In               |         |                                                                                           | ToS/MPLS Exp Flux - Out |         |                                                                                             |
| ToS/MPLS Exp                         | Traffic | Percentage                                                                                | ToS/MPLS Exp            | Traffic | Percentage                                                                                  |
| 0                                    | 0.41 MB | 100.00%  | 0                       | 1.22 MB | 100.00%  |

For more information on enabling ToS/MPLS Exp Traffic Analysis, see "[Configuring NTA traffic analysis parameters](#)."

### Traffic Details

The **Traffic Details** list provides the data collection samples for traffic statistics based on the report time range. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic.

**Figure 192 Traffic Details**

| Traffic Details     |          |           |                     |         |           |
|---------------------|----------|-----------|---------------------|---------|-----------|
| Traffic - In        |          |           | Traffic - Out       |         |           |
| Time                | Traffic  | Rate      | Time                | Traffic | Rate      |
| 2015-11-23 14:40:00 | 53.12 KB | 0.73 Kbps | 2015-11-23 14:40:00 | 0.16 MB | 2.18 Kbps |
| 2015-11-23 14:50:00 | 0.23 MB  | 3.16 Kbps | 2015-11-23 14:50:00 | 0.68 MB | 9.47 Kbps |
| 2015-11-23 15:00:00 | 0.13 MB  | 1.80 Kbps | 2015-11-23 15:00:00 | 0.39 MB | 5.41 Kbps |
| 2015-11-23 15:10:00 | 0.00 B   | 0.00 bps  | 2015-11-23 15:10:00 | 0.00 B  | 0.00 bps  |
| 2015-11-23 15:20:00 | 0.00 B   | 0.00 bps  | 2015-11-23 15:20:00 | 0.00 B  | 0.00 bps  |
| 2015-11-23 15:30:00 | 0.00 B   | 0.00 bps  | 2015-11-23 15:30:00 | 0.00 B  | 0.00 bps  |
| 2015-11-23 15:40:00 | 0.00 B   | 0.00 bps  | 2015-11-23 15:40:00 | 0.00 B  | 0.00 bps  |

## Application reports

Application reports provide rate of traffic statistics by application, by protocol, and by application category for all VPNs in a task. These reports enable you to get the details for an individual application. Application reports for a VPN traffic analysis task include the **Application List**, which provides a list of applications observed for all VPNs in the selected VPN traffic analysis task. This list includes total volume of traffic for the associated application, rate of traffic, and the percentage of all observed traffic observed on all VPNs generated by the associated application. This report also enables you to get the details for additional reports for the selected application. The **Application Traffic Trend** stacked area chart provides average inbound and outbound traffic rates for all applications observed for all VPNs in the selected traffic analysis task.

Protocol reports for a VPN traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all VPNs in the selected VPN traffic analysis task. This list includes total volume of traffic for the associated protocol, rate of traffic, and the percentage of all observed traffic observed on all VPNs generated by the associated protocol. This report also enables you to get the details for additional reports for the selected protocol. The **Protocol Traffic Trend** stacked area



chart provides average inbound and outbound traffic rates for all protocols observed for all VPNs in the selected traffic analysis task.

Application category reports for a VPN traffic analysis task include the **Application Category List**, which provides a list of the application categories observed for all VPNs in the selected VPN traffic analysis task. This list includes total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic observed on all VPN generated by the associated application category. This report also enables you to get the details for additional reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound and outbound traffic rates for all applications observed for all VPNs in the selected traffic analysis task.

As with all report types for a VPN task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a VPN task, click the **Application** tab to view traffic reports for the selected VPN traffic analysis task, and set **Query Type** to **Application** as described in "[Query applications](#)."

Application reports display reports organized by the list of applications in NTA. NTA provides many system-defined applications and NTA also supports user defined applications. For more information on applications in NTA, see "[Managing applications](#)." This section describes the reports available for applications.

### Query applications

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application, direction, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the **Query Criteria** to expand the query criteria area.
2. Select **Application** from the **Query Type** list. The page will display the report for Layer 4 through Layer 7 applications.
3. Click **Select** next to the **Application** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select the applications you want to search for, you must first query the **Application List** as follows:

- a. In the **Query Applications** area of the dialog box, specify one or more of the following search criteria:
  - **Application**—Enter a partial or complete name for the applications for which you want to search.
  - **Pre-defined**—Select **Yes** to search for applications that are predefined; select **No**, to filter for applications that are user-defined; select **Not limited** to include system or predefined and user-defined applications.
- b. To display the full **Application List**, click **Query** without entering any search criteria.
- c. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.

- d. Select the check boxes next to the applications for which you want to search.
- e. Click **OK** to add the applications to the filter.

The applications you selected are displayed in the **Application** field.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.

- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

- To print this report, click the **Print** icon  on the toolbar.
- From **Page Range**, select the page range.
- To export the data, click **Export**.
- To export this report, click the **Export** icon  on the toolbar.
- Select the export file format from the **File Format** list. Options are:
  - **PDF**
  - **XLS**
  - **CSV**
  - **DOCX**
  - **RTF**
  - **XLSX**
  - **PPTX**
  - **HTML**
  - **JRXML**
- From **Page Range**, select the page range.
- Click **Export**.

## Application List

The **Application List** provides a list of applications observed for all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the name of the application, an icon  for viewing the ports for all unknown applications, the total volume of traffic for the associated application, the rate of traffic, and the percentage of all observed traffic observed on all VPNs generated by the associated application. The application name in the **Application** field is a link to reports for the selected application.

**Figure 193 Application List**

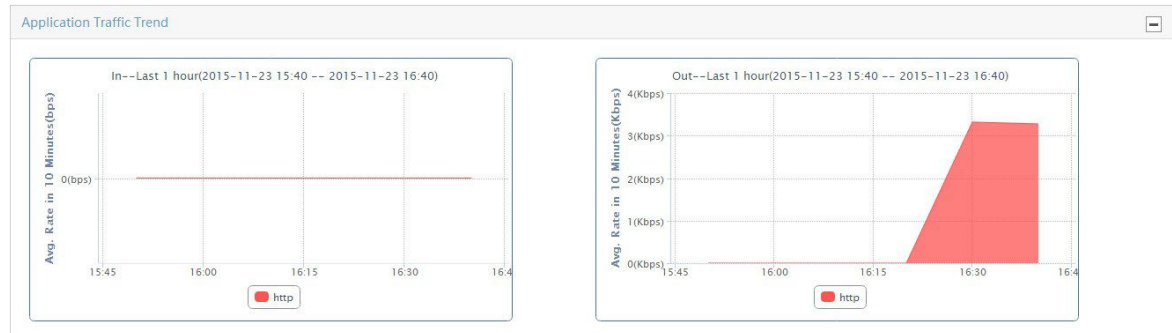
| Application List       |                      |            |          |             |           |
|------------------------|----------------------|------------|----------|-------------|-----------|
| Application            | Unknown Applications | In Traffic | In Speed | Out Traffic | Out Speed |
| http                   |                      | 0.00 B     | 0.00 bps | 0.24 MB     | 0.55 Kbps |
| 1-1 of 1. Page 1 of 1. |                      |            |          |             |           |

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

## Application Trend

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all VPNs in the selected traffic analysis task for the selected time range. If more than one VPN exists for the selected task, these statistics reflect traffic for all VPNs configured in a task.

**Figure 194 Application Traffic Trend – In/Out**



## Individual application reports

NTA provides traffic trend statistics for the individual applications that were observed on the VPNs for a selected task. Individual application reports include the **Application Traffic Trend** report that displays the average rate of traffic for the selected application. Individual application reports also include the **TopN Application Usage List** for source and destination hosts, which identifies which source and destination contributed the greatest volume of traffic for the selected application. Also included are reports for unknown TCP and UDP applications.

Unknown applications are those applications for which the Layer 4 TCP or UDP port number has not been assigned a name and is not included as an application in NTA. For more information on assigning names to TCP or UDP ports and adding them as applications to NTA, see ["Managing applications."](#)

To view individual application reports for a VPN traffic analysis task, click the name in the **Application** field of the **Application List** report for the application for which you want to view this report.

To view unknown application reports for a VPN traffic analysis task, click the icon  in the **Application** field of the **Application List** report for the application for which you want to view this report.

### Application Traffic Trend

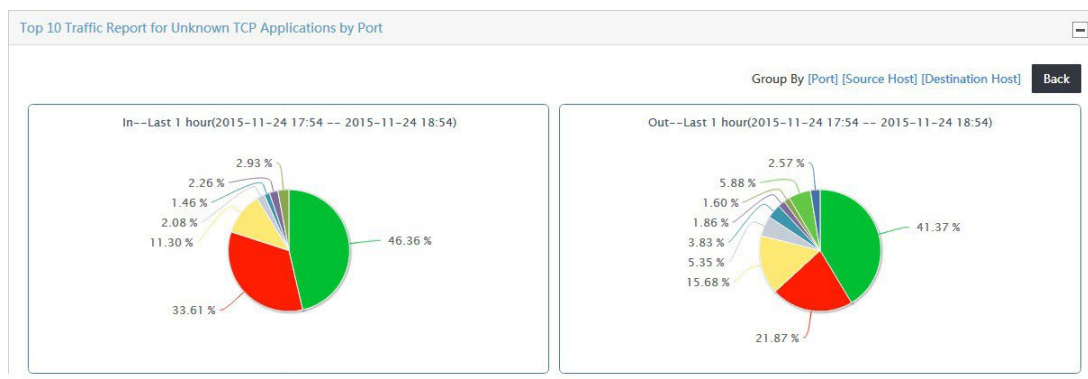
The **Application Traffic Trend – In/Out** graph provides average rate of traffic for an individual application for all VPNs in the selected traffic analysis task. If more than one VPN exists for the selected task, this chart reflects traffic for all VPNs configured in a task.

By default, the **Application Traffic Trend – In/Out** report graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Application** report page, click **Back**.



**Figure 197 TopN Traffic Report for Unknown TCP/UDP Applications by Port – In/Out**



### TopN Traffic List for Unknown TCP/UDP by Port

The **TopN Traffic List for Unknown TCP/UDP Applications by Port** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the TCP or UDP port number, total volume of traffic for the associated source, rate of traffic, and the percentage of all observed traffic generated by the source. The port number is a link for navigating to individual reports for the selected port. The icon  in the **Define Application** field is a link for adding the selected port as a Layer 4 application to NTA. For more information on managing applications in NTA, see ["Managing applications."](#)

**Figure 198 TopN Traffic List for Unknown TCP/UDP Applications by Port**

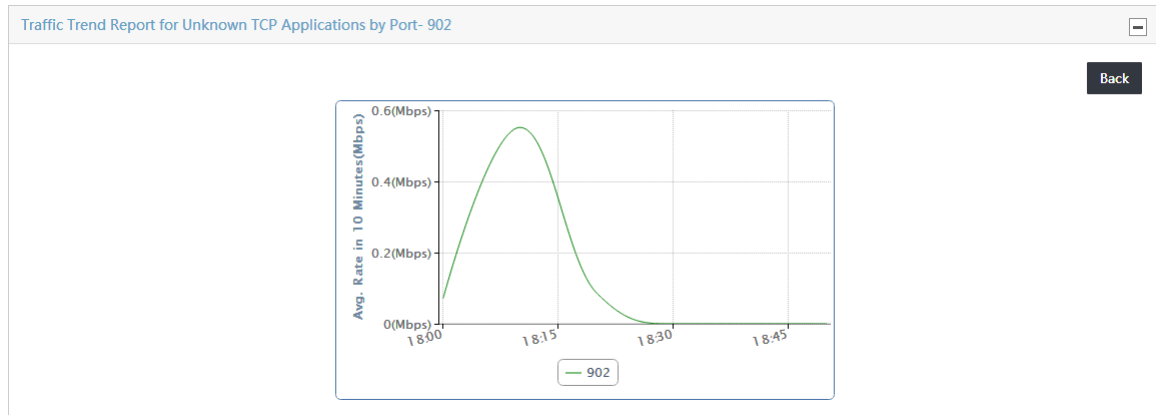
| Top 10 Traffic List for Unknown TCP Applications by Port |          |            |                                                                                     |                    |        |          |            |                                                                                       |                    |
|----------------------------------------------------------|----------|------------|-------------------------------------------------------------------------------------|--------------------|--------|----------|------------|---------------------------------------------------------------------------------------|--------------------|
| In                                                       |          |            |                                                                                     |                    | Out    |          |            |                                                                                       |                    |
| Port                                                     | Traffic  | Rate       | Define Application                                                                  | Percentage         | Port   | Traffic  | Rate       | Define Application                                                                    | Percentage         |
| 902                                                      | 50.76 MB | 0.12 Mbps  |  | 46.36% <div></div> | 902    | 37.46 MB | 87.28 Kbps |  | 41.37% <div></div> |
| 55614                                                    | 36.80 MB | 85.75 Kbps |  | 33.61% <div></div> | 50293  | 19.80 MB | 46.13 Kbps |  | 21.87% <div></div> |
| 50293                                                    | 12.37 MB | 28.81 Kbps |  | 11.30% <div></div> | 55614  | 14.20 MB | 33.08 Kbps |  | 15.68% <div></div> |
| 49154                                                    | 2.28 MB  | 5.32 Kbps  |  | 2.08% <div></div>  | 49154  | 4.84 MB  | 11.28 Kbps |  | 5.35% <div></div>  |
| 55640                                                    | 1.59 MB  | 3.71 Kbps  |  | 1.46% <div></div>  | 55640  | 3.47 MB  | 8.08 Kbps  |  | 3.83% <div></div>  |
| 135                                                      | 1.06 MB  | 2.48 Kbps  |  | 0.97% <div></div>  | 63149  | 1.68 MB  | 3.92 Kbps  |  | 1.86% <div></div>  |
| 54536                                                    | 1.06 MB  | 2.48 Kbps  |  | 0.97% <div></div>  | 52405  | 1.45 MB  | 3.37 Kbps  |  | 1.60% <div></div>  |
| 55963                                                    | 0.39 MB  | 0.91 Kbps  |  | 0.36% <div></div>  | 65485  | 0.85 MB  | 1.99 Kbps  |  | 0.94% <div></div>  |
| 57882                                                    | 0.35 MB  | 0.80 Kbps  |  | 0.32% <div></div>  | 5061   | 0.85 MB  | 1.99 Kbps  |  | 0.94% <div></div>  |
| 63149                                                    | 0.34 MB  | 0.80 Kbps  |  | 0.31% <div></div>  | 54111  | 0.62 MB  | 1.44 Kbps  |  | 0.68% <div></div>  |
| Others                                                   | 2.48 MB  | 5.77 Kbps  |                                                                                     | 2.26% <div></div>  | Others | 5.32 MB  | 12.40 Kbps |                                                                                       | 5.88% <div></div>  |

### Traffic Trend Report for Unknown TCP/UDP Applications by Port

To view this report for a VPN traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **Traffic Trend** graph provides the average rate for an individual unknown application for all VPNs in the selected traffic analysis task. If more than one VPN exists for the selected task, this chart will reflect traffic for all VPNs configured in a task.

**Figure 199 Traffic Trend Report for Unknown TCP/UDP Applications by Port**



### TopN traffic Details List for Unknown TCP/UDP Applications by Port

To view this report for a VPN traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs, the volume of traffic sent and received between the source and destination hosts, the rate of traffic observed between the pair, and the percentage of all traffic observed for the source and destination hosts.

**Figure 200 TopN Traffic Details List for Unknown TCP/UDP Applications by Port**

| Top 10 Traffic Details List for Unknown TCP Applications by Port - 902 |                  |          |           |                               |
|------------------------------------------------------------------------|------------------|----------|-----------|-------------------------------|
| Source Host                                                            | Destination Host | Traffic  | Rate      | Percentage                    |
| 192.168.40.22                                                          | 192.168.30.22    | 47.74 MB | 0.11 Mbps | 94.05% <div><div></div></div> |
| 192.168.30.22                                                          | 192.168.40.22    | 3.02 MB  | 7.04 Kbps | 5.95% <div><div></div></div>  |

## Protocol reports

Protocol reports display traffic rate trend reports organized by the list of protocols predefined in NTA. Protocol reports for a VPN traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all VPNs in the selected VPN traffic analysis task. This report also provides drill-down capabilities for additional reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average inbound traffic rates for all protocols observed for all VPNs in the selected traffic analysis task. Protocol reports also include traffic lists and trend reports for individual protocols.

As with all report types for a VPN traffic analysis task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a VPN traffic analysis task, click the **Application** tab to view application reports for the selected VPN traffic analysis task, and set **Query Type** to **Protocol** as described in "[Query protocols](#)."

For more information on protocols in NTA, see "[Managing protocols](#)." This section describes the reports available for protocols.

### Query protocols

To view reports by protocol, you must configure the filter criteria for application reports. NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, protocol, direction, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the **Query Criteria** to expand the query criteria area.

2. Select **Protocol** from the **Query Type** list.

The page will display the report for protocols.

3. Click **Select** next to the **Protocol** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the protocols you want to search for, you must first query the **Protocol List** as follows:

- a. Enter one or more of the following search criteria in the **Query Protocols** area of the dialog box:

- **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
- **Pre-defined**—To search for protocols that are predefined, select **Yes** from the **Pre-defined** list. To filter for protocols that are user-defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.

- b. To display the full **Protocol List**, click **Query** without entering any search criteria.

- c. Click **Query**.

The query results are displayed in the **Protocol List** below the **Query Protocols** area.

- d. Select the check boxes next to the applications for which you want to search.

- e. Click **OK** to add the protocols to the filter.

Click **Clear** to clear all selected protocols.

- **Start Time**—To autopopulate this field, click the **Calendar** icon . A popup calendar is displayed. Select the start date from the calendar. Adjust the hour value in the **Start Time** field.

- **End Time**—To autopopulate this field, click the **Calendar** icon . A popup calendar is displayed. Select the end date from the calendar. Adjust the hour value in the **End Time** field.

Additionally, to set the start time and end time for the protocol report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for protocols.

4. Click **OK**.

The page displays the results of your query.

5. Click **Export** to view reports using the **INC Intelligent Analysis Report Viewer** and to print or export all reports found on this page.

- a. To print this report, click the **Print** icon  on the toolbar.

- b. From **Page Range**, select the page range.

- c. To export the data, click **Export**.

- d. To export this report, click the **Export** icon  on the toolbar.

- e. Select the export file format from the **File Format** list. Options are:

- **PDF**
- **XLS**



- CSV
- DOCX
- RTF
- XLSX
- PPTX
- HTML
- JRXML

- f. From **Page Range**, select the page range.
- g. Click **Export**.

## Protocol List

The **Protocol List** provides a list of the protocols observed for all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the protocol name, total volume of traffic for the associated protocol, rate of traffic, and the percentage of traffic on all VPNs generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.

**Figure 201 Protocol List**

| Protocol List          |            |           |             |           |
|------------------------|------------|-----------|-------------|-----------|
| Protocol               | In Traffic | In Speed  | Out Traffic | Out Speed |
| UDP                    | 0.00 B     | 0.00 bps  | 0.69 MB     | 1.61 Kbps |
| IGMP                   | 0.56 MB    | 1.31 Kbps | 0.56 MB     | 1.31 Kbps |
| 1-2 of 2. Page 1 of 1. |            |           |             |           |

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

## Protocol Traffic Trend

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocols observed for all VPNs in the selected traffic analysis task for the selected time range. If more than one VPN exists for the selected task, these statistics reflects traffic for all VPNs configured in a task.

**Figure 202 Protocol Traffic Trend – In/Out**



## Individual protocol reports

NTA provides traffic trend statistics for the individual protocol that were observed on the VPNs for a selected task. Individual protocol reports include the **Protocol Traffic Trend** report that displays the average rate of traffic for the selected protocol. Individual protocol reports also include the **TopN Protocol Usage List** for source and destination hosts, which identifies which source and destination hosts contributed the greatest volume of traffic for the selected protocol.



To view individual protocol reports for a VPN task, click the name in the **Protocol** field of the **Protocol List** report for the protocol for which you want to view this report. For more information about **Protocol List**, see "[Protocol List](#)."

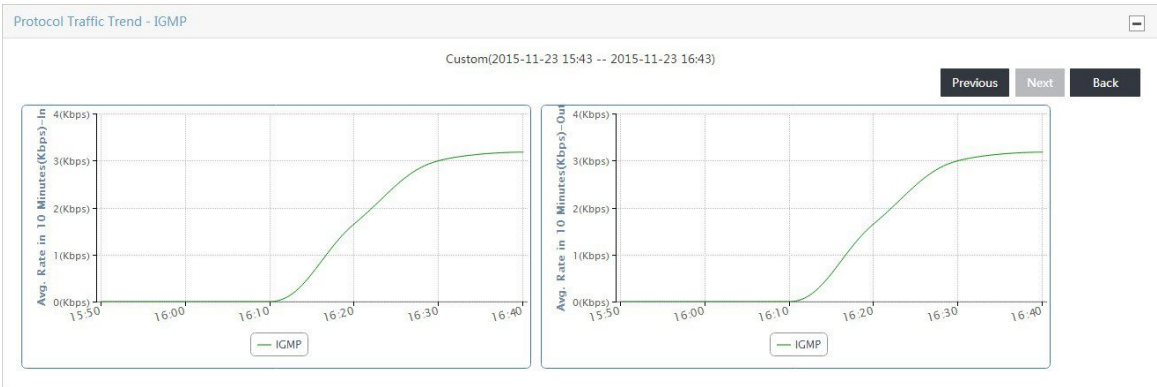
**Protocol traffic trend**

The **Protocol Traffic Trend – In/Out** graph provides average rate of traffic for an individual protocol for all VPNs in the selected traffic analysis task. If more than one VPN exists for the selected task, this chart reflects traffic for all VPNs configured in a task.

By default, the **Protocol Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Protocol** report page, click **Back**.

**Figure 203 Traffic Trend Report for an Individual Protocol – In/Out**



**TopN Protocol Usage List**

The **TopN Protocol Usage List** includes the **Source Host List – In/Out** and the **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 204 TopN Protocol Usage List – Destination Host List**

| Top 10 Protocol Usage List - IGMP                                                               |         |                                                                                             |                                                                                                 |         |                                                                                               |
|-------------------------------------------------------------------------------------------------|---------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------------------------------------|
| Source Host List - In                                                                           |         |                                                                                             | Source Host List - Out                                                                          |         |                                                                                               |
| Source Host IP Address                                                                          | Traffic | Percentage                                                                                  | Source Host IP Address                                                                          | Traffic | Percentage                                                                                    |
|  66.66.1.232 | 0.56 MB | 100.00%  |  66.66.6.180 | 0.56 MB | 100.00%  |
| Destination Host List - In                                                                      |         |                                                                                             | Destination Host List - Out                                                                     |         |                                                                                               |
| Destination Host IP Address                                                                     | Traffic | Percentage                                                                                  | Destination Host IP Address                                                                     | Traffic | Percentage                                                                                    |
|  32.32.5.231 | 0.56 MB | 100.00%  |  32.32.4.84  | 0.56 MB | 100.00%  |

## Application category reports

Application category reports display traffic rate trend reports organized by the application categories in NTA. Application category reports for a VPN traffic analysis task include the **Application Category List**, which provides a list of the application categories observed for all VPNs in the selected VPN traffic analysis task. This list includes total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic observed on all VPNs generated by the associated application category. This report also provides drill-down capabilities for additional reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound traffic rates for all applications observed for all VPNs in the selected traffic analysis task. Application category reports also include traffic lists and trend reports for the individual application categories.

As with all report types for a VPN traffic analysis task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a VPN traffic analysis task, click the **Application** tab to view application reports for the selected VPN traffic analysis task, and set **Query Type** to **Application Category** as described in "[Query application categories](#)."

NTA provides many system-defined application categories and also supports user defined application categories. For more information on application categories in NTA, see "[Managing application categories](#)." This section describes the reports available for application categories.

### Query application categories

To view reports by application category, you must configure the filter criteria for application category reports.

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and select **Custom** from the list that is displayed. Or, click the **Advanced** icon  next to the query field to expand the query criteria area.
2. Select **Application Category** from the **Query Type** list.  
The page will display the report for application categories.
3. Click **Select** next to the **Application Category** field.

The **Query Application Categories** dialog box displays an empty **Application Category List**.

To select the application categories you want to search for, you must first query the **Application Category List** as follows:

- a. Enter one or more of the following search criteria in the **Query Application Categories** area of the dialog box:
  - **Application Category**—Enter a partial or complete name for the application categories you want to search for in the **Application Category** field.
  - **Pre-defined**—To search for application categories that are predefined, select **Yes** from the **Pre-defined** list. To filter for application categories that are user-defined, select **No** from the list. To include system or predefined and user-defined application categories, select **Not limited**.
- b. To display the full **Application Category List**, click **Query** without entering any search criteria.
- c. Click **Query**.  
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
- d. Click the boxes next to the application categories for which you want to search.
- e. Click **OK** to add the application categories you have selected to the filter.

The application categories you selected are displayed in the **Application Category** field.

Click **Clear**, located next to the **Application Category** field, to clear all selected application categories.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or,

click the **Calendar** icon  next to the input box to manually specify a start time.

- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or,

click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application category report, click the icon  in the upper right corner of the application category report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**,

**Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.

#### 4. Click **OK**.

The page displays the results of your query.

### Application Category List

The **Application Category List** provides a list of the application categories observed for all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the application category name, the inbound/outbound traffic, and the inbound/outbound rate on all VPNs generated by the associated application category. The application category name in the **Application Category** field is a link for navigating to reports for the selected application category.

**Figure 205 Application Category List**

| Application Category       | In Traffic | In Speed  | Out Traffic | Out Speed |
|----------------------------|------------|-----------|-------------|-----------|
| HTTP                       | 0.00 B     | 0.00 bps  | 0.69 MB     | 1.61 Kbps |
| Other Application Category | 0.56 MB    | 1.31 Kbps | 0.56 MB     | 1.31 Kbps |

1-2 of 2. Page 1 of 1.

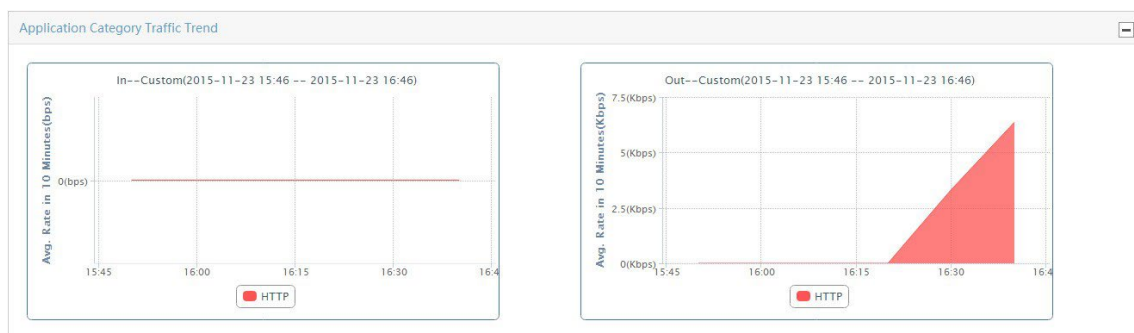
« < 1 > » 50 ▾

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

### Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all application categories observed for all VPNs in the selected traffic analysis task for the selected time range. If more than one VPN exists for the selected task, these statistics will reflect traffic for all VPNs configured in a task.

**Figure 206 Application Category Traffic Trend – In/Out**



## Individual application category reports

NTA provides traffic trend statistics for the individual protocol categories that were observed on the interfaces for a selected task. Individual protocol category reports include the **Application Category Traffic Trend** report that displays the average rate of traffic for the selected application category. Individual application category reports also include the **TopN Application Category Usage List** that identifies the TopN source and destination hosts.

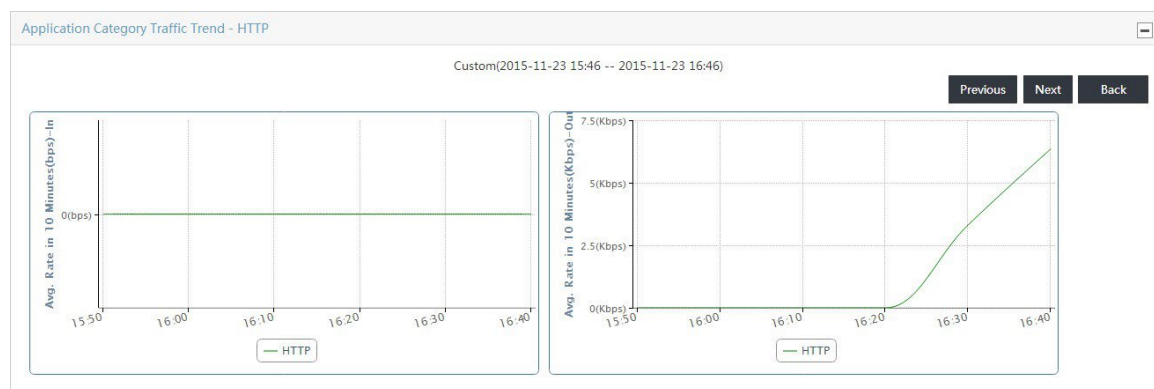
To view application category reports for an interface task or for a single interface in an interface task, click the name in the **Application Category** field of the **Application Category List** report for the application category for which you want to view this report. For more information about **Application Category List**, see "[Application Category List](#)."

### Application Category Traffic Trend

The **Application Category Traffic Trend** graph provides average rate of traffic for an individual application category for all VPNs in the selected traffic analysis task. If more than one VPN exists for the selected task, this chart will reflect traffic for all VPNs configured in a task. By default, this graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Application Category** report page, click **Back**.

**Figure 207 Application Category Traffic Trend Report for an Individual Application Category**



### TopN Application Category Usage List

The **TopN Application Category Usage List** includes the **Source Host List – In/Out** and **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination. The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 208 TopN Application Category Usage List – Destination Host List**

| Top 10 Application Category Usage List - HTTP |  |                             |                            |
|-----------------------------------------------|--|-----------------------------|----------------------------|
| Source Host List - In                         |  | Source Host List - Out      |                            |
| No data available.                            |  | Source Host IP Address      | Traffic Percentage         |
|                                               |  | 66.66.5.233                 | 0.35 MB 50.00% <div></div> |
|                                               |  | 66.66.5.130                 | 0.35 MB 50.00% <div></div> |
| Destination Host List - In                    |  | Destination Host List - Out |                            |
| No data available.                            |  | Destination Host IP Address | Traffic Percentage         |
|                                               |  | 32.32.0.62                  | 0.35 MB 50.00% <div></div> |
|                                               |  | 32.32.0.116                 | 0.35 MB 50.00% <div></div> |

## Source reports

Source reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Source Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN source hosts for all VPNs in the selected traffic analysis task. Both reports also include the TopN Traffic List for Source Host, which provides a list of the TopN source hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task. The pie chart contains a link for navigating to traffic reports for the selected host. The list also contains a link for navigating to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and the results of the host query. As with all report types for a VPN task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a VPN traffic analysis task, click the **Source** tab to view traffic reports for the selected VPN traffic analysis task.

### Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, traffic direction, or time range to customize the charts and lists displayed under the **Source** tab.

1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:

- o **Source Host**—In the **Source Host** field, enter the IP address or address range.  
To enter the IP address for a single host, enter the IP address using dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

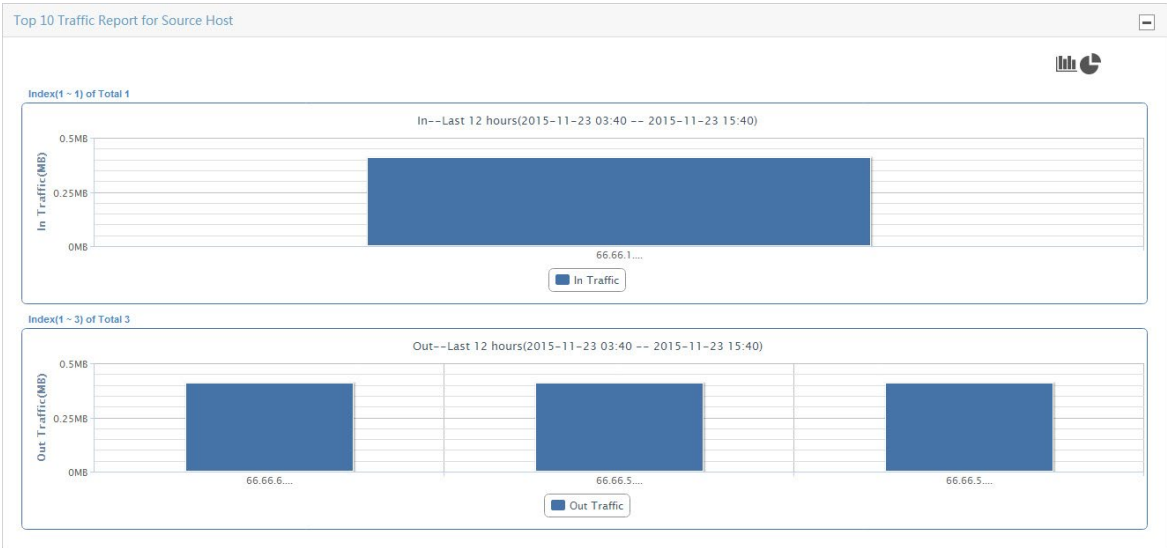
- o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
  5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
    - a. To print this report, click the **Print** icon  on the toolbar.
    - b. From **Page Range**, select the page range.
    - c. To export the data, click **Export**.
    - d. To export this report, click the **Export** icon  on the toolbar.
    - e. Select the export file format from the **File Format** list. Options are:
      - **PDF**
      - **XLS**
      - **CSV**
      - **DOCX**
      - **RTF**
      - **XLSX**
      - **PPTX**
      - **HTML**
      - **JRXML**
    - f. From **Page Range**, select the page range.
    - g. Click **Export**.

#### TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host** bar chart displays the TopN source hosts with the most inbound/outbound traffic in a certain period of time in a selected VPN traffic analysis task. Click a bar for a source host in the chart to view the traffic analysis report of the source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of the TopN source hosts for all VPNs in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

Figure 209 TopN Traffic Report for Source Host – In/Out



### TopN Traffic List for Source Host

The **TopN Traffic List for Source Host – In/Out** provides a list of the TopN source hosts measured by volume of inbound/outbound traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source host, and the percentage of all observed traffic generated by the source host. The IP address is a link for navigating to reports for the selected source host. The host query icon next to the source IP address is a link for initiating a host query and a link for navigating to the results of the host query.

Figure 210 TopN Traffic List for Source Host – In/Out

Top 10 Traffic List for Source Host

In **Generate Chart** Out **Generate Chart**

| Source      | Traffic | Percentage | Source      | Traffic | Percentage |
|-------------|---------|------------|-------------|---------|------------|
| 66.66.1.232 | 0.41 MB | 100.00%    | 66.66.6.180 | 0.41 MB | 33.33%     |
|             |         |            | 66.66.5.233 | 0.41 MB | 33.33%     |
|             |         |            | 66.66.5.130 | 0.41 MB | 33.33%     |

### Traffic Trend Report for Source Host

To view this report for a VPN traffic analysis task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Source** host report page, click **Back**.



**Figure 211 Traffic Trend Report for Source Host**



### Traffic Details for Source Host

To view this report for a VPN traffic analysis task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Details** for a source host table provides two lists:

- The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and destination hosts, and the percentage of all traffic observed for this source and destination hosts.
- The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

**Figure 212 TopN Destination Hosts Communicating with the Source Host**

| Traffic Details                                             |         |            |                                                        |         |            |
|-------------------------------------------------------------|---------|------------|--------------------------------------------------------|---------|------------|
| Top 10 Destination Hosts Communicating with the Source Host |         |            | Top 10 Applications Communicating with the Source Host |         |            |
| Destination                                                 | Traffic | Percentage | Application Name                                       | Traffic | Percentage |
| 32.32.5.231                                                 | 0.41 MB | 100.00%    | IGMP Protocol Application                              | 0.41 MB | 100.00%    |

## Destination reports

Destination reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Destination Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN destination hosts for all VPNs in the selected traffic analysis task. Both reports also include the **TopN Traffic List for Destination Host**, which provides a list of the TopN destination hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task. The pie chart contains a link for navigating to traffic reports for the selected host. The list also contains a link for navigating to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and the results of the host query. As with all report types for a VPN task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a VPN traffic analysis task, click the **Destination** tab to view traffic reports for the selected VPN traffic analysis task.

### Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed under the **Destination** tab.

1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the destination report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Destination Host**—In the **Destination Host** field, enter the IP address or address range.
 

To enter the IP address for a single host, enter the IP address using dotted decimal notation.

Example of a valid IP address:

```
10.153.89.10
```

Example of a valid network/subnet mask in dotted decimal notation:

```
10.153.89.0/255.255.255.0
```

Example of a valid network/subnet mask using CIDR notation:

```
10.153.89.0/24
```

Example of a valid IPv6 address:

```
a001:410:0:1::1
```

Example of a valid IPv6 address and subnet mask using CIDR notation:

```
a001:410:0:1::1/64
```
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.
  - e. Select the export file format from the **File Format** list. Options are:
    - **PDF**
    - **XLS**
    - **CSV**
    - **DOCX**
    - **RTF**
    - **XLSX**
    - **PPTX**
    - **HTML**
    - **JRXML**

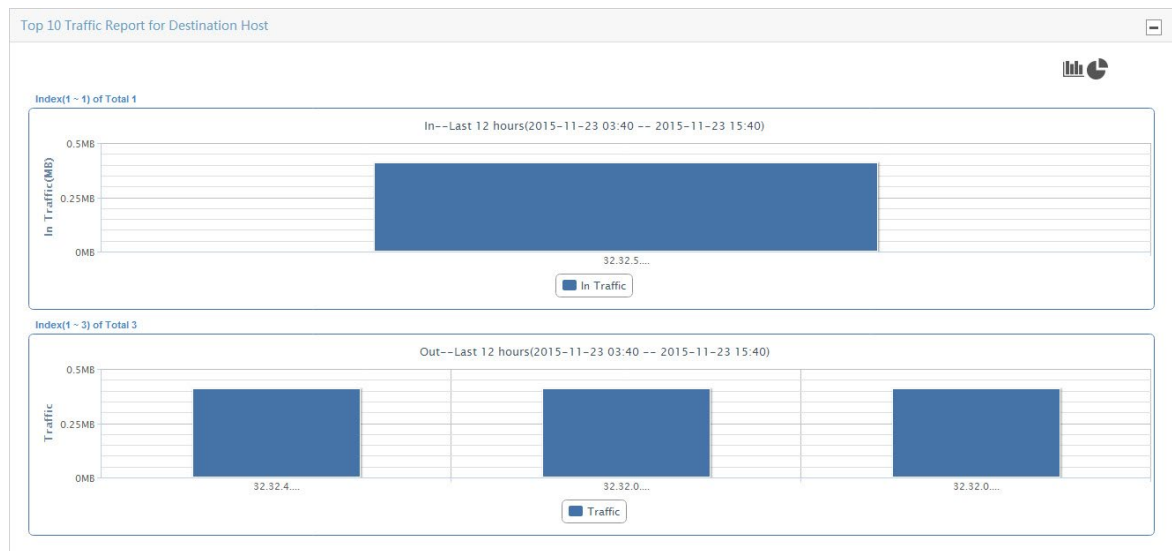
- f. From **Page Range**, select the page range.
- g. Click **Export**.

### TopN Traffic Report for Destination Host

The **TopN Traffic Report for destination Host** bar chart displays the TopN destination hosts with the most inbound/outbound traffic in a certain period of time in a selected VPN traffic analysis task. Click a bar for a destination host in the chart to view the traffic analysis report of the destination host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of TopN destination hosts for all VPNs in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

**Figure 213 TopN Traffic Report for Destination Host – In/Out**



### TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host – In/Out** provides a list of the TopN destination hosts measured by volume of inbound/outbound traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the host IP address, total volume of traffic generated by the associated destination host, and the percentage of all observed traffic generated by the destination host. The IP address is a link for navigating to reports for the selected destination

host. The host query icon  next to the destination IP address is a link for initiating a host query and for navigating to the results of the host query.

**Figure 214 TopN Traffic List for Destination Host – In/Out**

| Top 10 Traffic List for Destination Host                                                                        |         |                                |                                                                                                                 |         |                               |
|-----------------------------------------------------------------------------------------------------------------|---------|--------------------------------|-----------------------------------------------------------------------------------------------------------------|---------|-------------------------------|
| In                                                                                                              |         |                                | Out                                                                                                             |         |                               |
| <a href="#">Generate Chart</a>                                                                                  |         |                                | <a href="#">Generate Chart</a>                                                                                  |         |                               |
| Destination                                                                                                     | Traffic | Percentage                     | Destination                                                                                                     | Traffic | Percentage                    |
|  <a href="#">32.32.5.231</a> | 0.41 MB | 100.00% <div><div></div></div> |  <a href="#">32.32.4.84</a>  | 0.41 MB | 33.33% <div><div></div></div> |
|                                                                                                                 |         |                                |  <a href="#">32.32.0.62</a>  | 0.41 MB | 33.33% <div><div></div></div> |
|                                                                                                                 |         |                                |  <a href="#">32.32.0.116</a> | 0.41 MB | 33.33% <div><div></div></div> |

### Traffic Trend Report for Destination Host

To view this report for a VPN traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP

address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Destination** host report page, click **Back**.

**Figure 215 Traffic Trend Report for Destination Host**



## Traffic Details

To view this report for a VPN traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Details** for a destination host table provides the following lists:

- The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.
- The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

**Figure 216 Traffic Details**

| Traffic Details                                             |         |                     |                                                             |         |                     |
|-------------------------------------------------------------|---------|---------------------|-------------------------------------------------------------|---------|---------------------|
| Top 10 Source Hosts Communicating with the Destination Host |         |                     | Top 10 Applications Communicating with the Destination Host |         |                     |
| Source                                                      | Traffic | Percentage          | Application Name                                            | Traffic | Percentage          |
| 66.66.1.232                                                 | 0.41 MB | 100.00% <div></div> | IGMP Protocol Application                                   | 0.41 MB | 100.00% <div></div> |

## Session reports

A session is a unique source and destination host pair. Session reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Session Host** pie chart. The pie chart displays the distribution of the traffic generated by the TopN session hosts for all VPNs in the selected traffic analysis task. Both reports also include a **TopN Traffic List for Session Host**, which provides a list of the TopN session hosts measured by volume of traffic observed on all VPNs in the selected VPN traffic analysis task. The pie chart contains a link for navigating to traffic reports for the selected session. The list also contains a link for navigating to reports for the selected session host.

The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and the results of the host query. As with all report types for a VPN task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a VPN traffic analysis task, click the **Session** tab to view traffic reports for the selected VPN traffic analysis task.

### Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the session report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Source Host**—In the **Source Host** field, enter the IP address or address range.  
To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation is as follows:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation is as follows:  
10.153.89.0/24  
Example of a valid IPv6 address is as follows:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation is as follows:  
a001:410:0:1::1/64
  - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.
5. Click **Export** to view reports using the INC **Intelligent Analysis Report Viewer** and to print or export all reports found on this page.
  - a. To print this report, click the **Print** icon  on the toolbar.
  - b. From **Page Range**, select the page range.
  - c. To export the data, click **Export**.
  - d. To export this report, click the **Export** icon  on the toolbar.

- e. Select the export file format from the **File Format** list. Options are:
  - PDF
  - XLS
  - CSV
  - DOCX
  - RTF
  - XLSX
  - PPTX
  - HTML
  - JRXML
- f. From **Page Range**, select the page range.
- g. Click **Export**.

### TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host – In/Out** pie chart displays the distribution of inbound and outbound traffic for TopN source and destination session pairs for all VPNs in the selected traffic analysis task for the selected time range. Each pie chart slice is a link to traffic reports for the select source and destination session pair.

**Figure 217 TopN Traffic Report by Session Host – In**



### TopN Traffic List for Session Host

The **TopN Traffic List for Session Host – In/Out** provides a list of the TopN session source and destination pairs measured by volume of inbound/outbound traffic observed on all VPNs in the selected VPN traffic analysis task for the selected time range. This list includes the source and destination host IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair. The icon  in the **Details** field is a link for viewing reports for the selected session or source/destination pair. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link for navigating to the results of the host query.

**Figure 218 TopN Traffic Report for Session Host – In/Out**

| In                                                                                              |                                                                                                 |                        |                                |                                                                                     |                                                                                     | Out                                                                                             |                                                                                                 |                        |                               |                                                                                       |                                                                                       |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------|--------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------|-------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <a href="#">Generate Chart</a>                                                                  |                                                                                                 |                        |                                |                                                                                     |                                                                                     | <a href="#">Generate Chart</a>                                                                  |                                                                                                 |                        |                               |                                                                                       |                                                                                       |
| Source Host                                                                                     | Destination Host                                                                                | Traffic                | Percentage                     | Details                                                                             | Topology                                                                            | Source Host                                                                                     | Destination Host                                                                                | Traffic                | Percentage                    | Details                                                                               | Topology                                                                              |
|  66.66.1.232 |  32.32.5.231 | 0.13 MB                | 100.00% <div><div></div></div> |  |  |  66.66.5.130 |  32.32.0.116 | 0.13 MB                | 51.45% <div><div></div></div> |  |  |
| Other Hosts                                                                                     | Other Hosts                                                                                     | Failed to obtain data. | 0.00% <div><div></div></div>   |                                                                                     |                                                                                     |  66.66.6.180 |  32.32.4.84  | 0.13 MB                | 51.45% <div><div></div></div> |  |  |
|                                                                                                 |                                                                                                 |                        |                                |                                                                                     |                                                                                     |  66.66.5.233 |  32.32.0.62  | 0.13 MB                | 51.45% <div><div></div></div> |  |  |
|                                                                                                 |                                                                                                 |                        |                                |                                                                                     |                                                                                     | Other Hosts                                                                                     | Other Hosts                                                                                     | Failed to obtain data. | 0.00% <div><div></div></div>  |                                                                                       |                                                                                       |

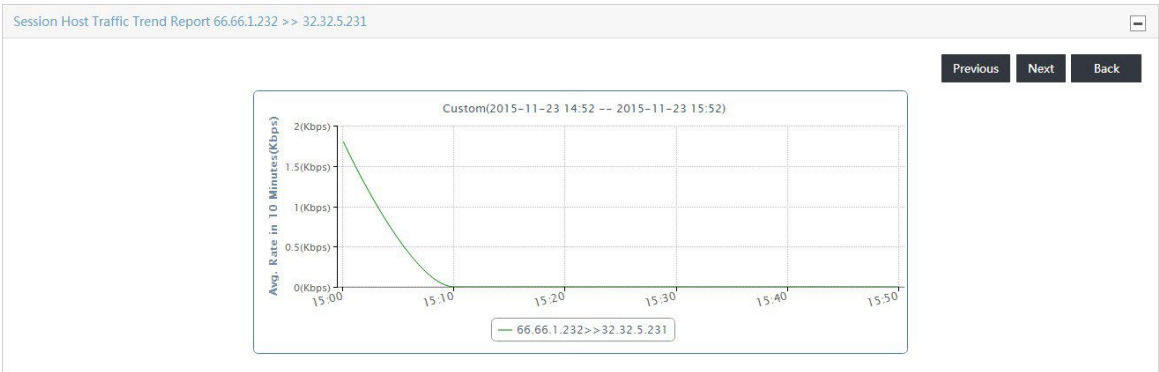
Session Host Traffic Trend Report

To view this report for a VPN traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Host Traffic Trend Report** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Session** report page, click **Back**.

Figure 219 Session Host Traffic Trend Report



TopN Applications for Session Host

To view this report for a VPN traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

Figure 220 TopN Applications for Session Host

| Top 10 Applications for Session Host 66.66.1.232 >> 32.32.5.231 |         |                     |
|-----------------------------------------------------------------|---------|---------------------|
| Application Category                                            | Traffic | Percentage          |
| IGMP Protocol Application                                       | 0.13 MB | 100.00% <div></div> |

Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source and destination hosts.



# Interbusiness monitoring

This chapter provides an overview of interbusiness traffic analysis, explains how to manage interbusiness traffic analysis tasks, and describes how to navigate different types of interbusiness traffic analysis reports.

## Interbusiness traffic analysis overview

Interbusiness traffic analysis tasks allow you to combine host and application information and assign it a business service name. NTA parses network flow records based on the combination of hosts and applications that you create, and provides traffic statistics for those hosts and applications. Because interbusiness analyses are based on hosts and applications and are not tied to an interface, a device, or probe network flow data sources, interbusiness reports provide visibility for all areas of the network that generate network flow records.

In general, traffic reports include the rate of traffic for all hosts and applications in all tasks, and for the hosts and applications in a specific task. They include per-second traffic for each configured interbusiness analysis task, the average rate for a single business and for interbusiness traffic, and interbusiness reports that operators have saved to the **Interest** list under the **Interest** tab. The reports provide both summarized information for tasks and detailed information about specific applications configured for a traffic analysis task.

## Interbusiness traffic analysis reporting overview

Click **Inter-Business Traffic Analysis Task** on the left navigation tree to view the summary report for all interbusiness traffic analysis tasks.

To view the interbusiness traffic analysis report for a single task, move your mouse pointer to the shortcut menu icon **>>>** next to **Inter-Business Traffic Analysis Task**. The **Inter-Business Traffic Analysis Task** shortcut menu displays all interbusiness traffic analysis tasks created in NTA. Click the name link for a task to view the interbusiness traffic analysis report of the task.

Each interbusiness traffic analysis report contains three granular reports, including **Single Business**, **Inter-Business**, and **Interest**. Click the **Expand** icon **▸** next to a task on the **Inter-Business Traffic Analysis Task** shortcut menu to display the three granular reports for the interbusiness traffic analysis task. Click the granular report name link to view the granular report.

The summary interbusiness traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—This bar graph provides average-rate-per-second reporting for all interbusiness tasks. Each bar in the graph is a link for navigating to more granular reporting for the selected task:
  - **Single Business**—These reports provide a bar graph depicting the TopN average rate per second generated by the hosts and applications you have configured as a single business application or service for the selected task. Click the contents of this graph to navigate to detailed information about the selected application. The **Traffic Details** area lists traffic volume and rate statistics for both inbound and outbound traffic.
  - **Inter-Business**—These reports provide a bar graph showing the average traffic rate for the hosts and applications in a business service and for other business traffic. The **Traffic Details** area lists traffic flux and rate statistics for all business-to-business traffic.
  - **Interest**—These are the reports saved by operators to the **Interest** list.
- **Summary List (Last 1 Hour)**—This list provides the per-second traffic rate by interbusiness traffic analysis task. This list provides navigation to more granular host reporting for the selected task.

# Interbusiness traffic analysis configuration issues

Consider the following when you create an interbusiness task:

- Interbusiness tasks rely on the configuration of both hosts and applications. If you add hosts without adding applications, no data will be attributed to the task.
- You must determine the locations on your network where you plan to capture host and application data. You must enable network flow data for the devices and their interfaces for those locations. You must then add these devices and probes to NTA using the Device Management and Probe Management features. NTA will then summarize host and application data for all devices and probes on which it observes interbusiness traffic.
- When you add applications to a task, NTA provides a list of all known applications. It is generated from the list of predefined applications in NTA, or applications that you have added using the Application Management feature. If the applications you want to add are not listed, it is probably because the application has not been added to NTA. For more information on adding applications to NTA, see "[Managing applications](#)."

## Managing interbusiness traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through tasks created by administrators. Until a task is created, NTA will not analyze the data that devices forward to it or that it is configured to receive. This section explains how to add, modify, and remove interbusiness traffic analysis tasks in NTA.

### Viewing a traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

#### Traffic analysis task list contents

- **Task Name**—This field contains the name of the task. The contents of this field link to the **Traffic Analysis Task Details** page for the associated task.
- **Task Description**—This field contains the description for the associated task.
- **Task Type**—Options are:
  - **Interface**
  - **VLAN/VXLAN**
  - **Probe**
  - **Application**
  - **Host**
  - **VPN**
  - **Inter-Business**
  - **BGP AS**
- **Baseline Analysis**—This field is displayed when the Baseline Analysis feature is enabled in NTA parameters. Interbusiness traffic analysis tasks do not support baseline analysis, and the baseline analysis field for an interbusiness traffic analysis task is displayed as **Disabled**.
- **Modify**—This field contains an icon  for modifying the associated task.

- **Delete**—This field contains an icon  for deleting the associated task.
- 3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** in the upper left corner of the **Traffic Analysis Task List**.  
You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Viewing traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the contents in the **Task Name** field of the **Traffic Analysis Task List** whose **Task Type** is **Inter-Business**.  
NTA displays details for the traffic analysis task.
4. Click **Back** to return to the **Traffic Analysis Task List**.

### Traffic Analysis Task Details page

- **Task Name**—This field contains the name of the task.
- **Task Description**—This field contains the description of the associated task.
- **Server**—This field contains the server name or IP address of the NTA server.
- **Task Type**—Options are:
  - **Interface**
  - **VLAN/VXLAN**
  - **Probe**
  - **Application**
  - **Host**
  - **VPN**
  - **Inter-Business**
  - **BGP AS**
- **Statistics Direction**—Identifies the statistics direction. Options are **In** and **Out**.
- **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by this traffic analysis task.
- **Business Info.**—Identifies the interbusiness host and application groups that have been configured for the traffic analysis task.
- **Interface Information**—Displays information about the interfaces selected for the traffic analysis task.
- **Probe Information**—Displays information about the probes selected for the traffic analysis task.

## Adding an interbusiness traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

3. Click **Add**.  
The **Add Traffic Analysis Task** page is displayed.
4. To add an interbusiness traffic analysis task, select the **Inter-Business** option on the **Select Task Type** page.
5. Click **Next**.  
The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.  
The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. Enter a description for this task in the **Task Description** field.
8. Select the NTA, NetStream, NetFlow, or sFlow collection server from the **Server** list.  
Unless configured otherwise by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
9. Select a direction from the **Statistics Direction** list for network flow records. Options are **In**, **Out**, and **.Not limited**.
10. To select the operator groups that will have access to the analysis and reports provided by this traffic analysis task, click **Select** next to the **Reader** field.  
The **Operator Group List** dialog box is displayed.
  - a. Select the check box next to the **Name** of each operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
  - b. Click **OK** to accept your operator group selection.  
The operator groups are displayed in the **Reader** field.  
You can configure a traffic analysis task to include traffic from one or more business services. A business service consists of a combination of one or more host IP addresses and applications, which are optional.
11. To add a business service, click **Add** at the top of the **Business Info.** list.  
The **Add Business** page is displayed.
  - a. Enter a unique name for the business service in the **Business Name** field.
  - b. Enter a brief description for the business service in the **Business Description** field.
  - c. To enable threshold alarm for the reports generated by this task, select **Enable** from the **Threshold Alarm** list. To disable threshold alarm, select **Disable**.  
If you select **Enable**, the threshold alarm configuration parameters are displayed under this list.
  - d. Set the threshold alarm configuration parameters:
    - **Direction**—This field specifies the direction of traffic monitoring. Options are **In**, **Out**, and **In/Out**.
    - **Trigger**—This field indicates under what conditions the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
    - **In Threshold**—This field indicates the threshold value or volume of inbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
    - **Out Threshold**—This field indicates the threshold value or volume of outbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.

- **Severity**—This field indicates the severity level of the triggered threshold alarms. The value must be **Major**.
- **Discard Length**—This field specifies the time interval in which a triggered alarm will not be sent again. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

If the **Threshold Alarm** list is not displayed, the Threshold Alarm feature has been disabled on the NTA server. For more information on configuration options for the NTA server, including the Threshold Alarm feature, see "[Configuring NTA traffic analysis parameters](#)."

In a traffic analysis task, you add a combination of hosts and applications that define a business service. For each business service you create, you specify whether you want NTA to include or exclude traffic from the hosts and applications.

- To include traffic from the hosts and applications you specify as a business service, select **Include** from the **IP Stat. Direction** list. To exclude traffic from the hosts and applications you specify as a business service, select **Exclude**.

You can do the following:

- Add one or more IP hosts or IP address ranges to a traffic analysis task. However, you must have at least one host defined, and no more than 10 host entries defined for each task. You can add multiple businesses in a traffic analysis task.
- Configure a traffic analysis task to include traffic for one or more hosts defined by IP address. Alternatively, enter a range of IP addresses to be included in the analysis, or enter a combination of IP host addresses and IP address ranges. However, no two addresses or address ranges entered in the **Host IP** field can overlap.

- Add IP address entries in the **Host IP** field.

To enter the IP address for a single host, use dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

- Click **Add** next to the **Host IP** field.

The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.

- To add applications to the task, click **Select** next to the **Application List** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select applications to add to the task, you must first query the **Application List** as follows:

- Enter one or more of the following search criteria in the **Query Applications** area of the dialog box:

**Application:** Enter the partial or complete name of each application you want to search.

**Pre-defined:** To search for applications that are predefined, select **Yes**. To filter for applications that are user defined, select **No**. To include both predefined and user-defined applications, select **Not limited**.

To display the complete **Application List**, click **Query** without entering any search criteria.

- Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area. Select the check boxes next to the applications you want to add to the task.

- c. Click **OK** to add the applications to the traffic analysis task you want to create.

The applications you selected are displayed in the **Application List**.

If the application you want to add to this task does not exist in the **Application List**, add it as a user-defined application. For more information on adding applications to NTA, see "[Managing applications](#)."

13. Click **OK** to create the business service.
14. To create additional business services, repeat steps 11 through 13.
15. To select one or more interfaces that will provide the traffic flow data, click **Select** in the **Interface Information** list area.

The **Add Interface** page opens.

Add interfaces automatically or configure them manually.

To add interfaces automatically:

- a. Click the **Obtain Automatically** tab.

The **Interface Information** list displays all interfaces that you can select for use in an interbusiness traffic analysis task.

Before a device interface can be displayed on this list, you must add the device to NTA using the Device Management feature, and then select the device in the NTA server configuration.

For more information about adding a device for traffic analysis to NTA, see "[Device management](#)." For more information on selecting devices in NTA server management, see "[Modifying an NTA server configuration](#)."

- b. To display the interfaces of only a specific device, select the device label from the **Device** list.
- c. Select the interfaces you want to add to the task.
- d. Click **OK**.

To add interfaces manually to the interbusiness traffic analysis task:

- e. Click the **Configure Manually** tab.
- f. In the **Interface Description** field, enter the description for the interface.
- g. In the **Interface Alias** field, enter the alias for the interface.
- h. From the **Device** list, select the device to which the interface belongs.
- i. In the **Interface Index** field, enter the interface index.
- j. In the **Max. Speed** field, enter the maximum speed of the interface, and then select **bps**, **kbps**, or **Mbps**.
- k. Click **OK**.

16. In the **Probe Information** list, select the probes that provide the network flow data for the task.

17. Click **OK** to create the traffic analysis task.

After you create an interbusiness traffic analysis task, NTA creates an entry called  **Inter-Business Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the interbusiness traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to  **Inter-Business Traffic Analysis Task**. The **Inter-Business Traffic Analysis Task** shortcut menu displays all interbusiness traffic analysis tasks created in NTA. Click the name of a task to view the interbusiness traffic analysis report of the task.

For information about accessing and viewing interbusiness traffic analysis reports, see "[Viewing interbusiness traffic analysis reports](#)."

# Modifying a traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  for the task you want to modify.
4. Modify the name for this task in the **Task Name** field.  
The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
5. Modify the description for this task in the **Task Description** field as needed.
6. Select the NTA, NetStream, NetFlow, or sFlow collection server from the **Server** list.  
Unless configured otherwise by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. Select a direction from the **Statistics Direction** list for network flow records. Options are **In**, **Out**, and **Not limited**.
8. To add operator groups that will have access to the analysis and reports provided by this task, click **Select** next to the **Reader** field.  
The **Operator Group List** dialog box is displayed.
  - a. Select the check box next to the **Name** of each operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
  - b. Click **OK** to accept the operator group selection.  
The operator groups are displayed in the **Reader** field.
  - c. To revoke operator group access to the results of this task, select operator groups in the **Reader** field.
  - d. Click **Delete**.
  - e. Click **OK** to confirm deletion of the selected operator groups from the task.  
The **Reader** list is updated to reflect the changes.  
You can configure a task to include traffic from one or more business services. A business service consists of a combination of one or more host IP addresses and applications, which are optional.
9. To modify an existing business service, click the **Modify** icon  for the business service in the **Business Info.** list.  
The **Modify Business** page is displayed.
  - a. Enter a brief description for the business service in the **Business Description** field.
  - b. To enable threshold alarm for the reports generated by this task, select **Enable**. To disable threshold alarm, select **Disable**.  
If you select **Enable**, the threshold alarm configuration parameters are displayed.
  - c. Set the threshold alarm configuration parameters:
    - **Direction**—This field specifies the direction of traffic monitoring. Options are **In**, **Out**, and **In/Out**.
    - **Trigger**—This field indicates under what conditions the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.



- **In Threshold**—This field indicates the threshold value or volume of inbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **In** or **In/Out**.
- **Out Threshold**—This field indicates the threshold value or volume of outbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
- **Severity**—This field indicates the severity level of the triggered threshold alarms. The value must be **Major**.
- **Discard Length**—This field specifies the time interval in which a triggered alarm will not be sent again. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

If the **Threshold Alarm** list is not displayed, the Threshold Alarm feature has been disabled on the NTA server. For more information on configuration options for the NTA server, including the Threshold Alarm feature, see "[Configuring NTA traffic analysis parameters](#)."

In a traffic analysis task, you add a combination of hosts and applications that define a business service. For each business service you create, you specify whether you want NTA to include or exclude traffic from the hosts and applications.

10. To include traffic from the hosts and applications you specify in a business service, select **Include** from the **IP Stat. Direction** list. To exclude traffic from the hosts and applications, select **Exclude**.

You can do the following:

- Add one or more IP hosts or IP address ranges to a traffic analysis task. However, you must have at least one host defined, and no more than 10 host entries defined for each task. You can add multiple businesses in a traffic analysis task.
- Configure a traffic analysis task to include traffic for one or more hosts defined by IP address. Alternatively, enter a range of IP addresses to be included in the analysis, or enter a combination of IP host addresses and IP address ranges. However, no two addresses or address ranges entered in the **Host IP** field can overlap.

11. Add IP address entries in the **Host IP** field. To enter the IP address for a single host, use dotted decimal notation.

Example of a valid IP address:

10.153.89.10

Example of a valid network/subnet mask in dotted decimal notation:

10.153.89.0/255.255.255.0

Example of a valid network/subnet mask using CIDR notation:

10.153.89.0/24

Example of a valid IPv6 address:

a001:410:0:1::1

Example of a valid IPv6 address and subnet mask using CIDR notation:

a001:410:0:1::1/64

12. Click **Add** next to the **Host IP** field.

The addresses and masks you entered are added to the **Host IP List** field below the **Host IP** field.

13. To add applications to the task, click **Select** next to the **Application List** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select applications to add to the task, you must first query the **Application List** as follows:

- a. Enter one or more of the following search criteria in the **Query Applications** area of the dialog box:

**Application**—Enter the partial or complete name of each application for which you want to search.

**Pre-defined**—To search for applications that are predefined, select **Yes**. To filter for applications that are user defined, select **No**. To include both predefined and user-defined applications, select **Not limited**.

To display the complete **Application List**, click **Query** without entering any search criteria.

- b. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.

- c. Select the check boxes next to the applications you want to add to the task.

- d. Click **OK** to add the applications to the task you want to create.

The applications are displayed in the **Application List**.

If the application you want to add to this task does not exist in the **Application List**, add it as a user-defined application. For more information on adding applications to NTA, see ["Managing applications."](#)

- e. Click **OK** to create the business service.

14. To add more business services, repeat steps 11 through 13.

15. To remove business services from the **Business Info.** list, click the **Delete** icon  for those business services.

The **Business Info.** list is updated to reflect the deletions.

16. When you have finished adding services to or removing services from the **Business Info.** list, continue with the next step.

17. To select one or more interfaces to provide the traffic flow data, click **Select** in the **Interface Information** list area.

The **Add Interface** page opens, which contains the **Obtain Automatically** and **Configure Manually** tabs.

If selected devices are deployed with server configuration in NTA server management, NTA can automatically obtain and display these device interfaces for interface selection. If no interface is displayed in the list, add interfaces manually.

To obtain interfaces automatically:

- a. At the top of the **Add Interface** page, click the **Obtain Automatically** tab.

All interfaces that can be selected for use in a traffic analysis task are displayed in the **Interface Information** list under the **Obtain Automatically** tab of the **Add Interface** page.

- b. To add interfaces to the task, select the check box next to the **Interface Description** field for every interface you want to add.

- c. Click **OK** to accept your interface selection.

To add interfaces manually:

- a. At the top of the **Add Interface** page, click the **Configure Manually** tab.

The page will update to display the configuration options for manually adding an interface to a traffic analysis task.

- b. In the **Interface Description** field, enter the description for the interface, for example, GigabitEthernet1/0/2.

- c. In the **Interface Alias** field, enter the alias for the interface.

- d. From the **Device** list, select the device to which the interface belongs.

- e. In the **Interface Index** field, enter the unique interface index or ifIndex number for the interface.

- f. In the **Max. Speed** field, enter the maximum speed of the interface and select the measurement unit for the interface speed. Options are **bps**, **kbps**, and **Mbps**.

- g. Click **OK**.

18. In the **Probe Information** list, select the probes that provide the network flow data for the task.

19. Click **OK** to accept your modifications to the interbusiness traffic analysis task.

## Deleting a traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the task you want to delete.
4. Click **OK** to confirm the deletion of the task.  
The **Traffic Analysis Task List** is updated to reflect the deletion.

## Viewing interbusiness traffic analysis reports

An interbusiness traffic analysis task combines host and application information into a business service. NTA parses network flow records based on the combination of hosts and applications you specify. NTA provides several levels of reporting for all interbusiness tasks. NTA also provides summarized reports for all tasks, granular reports for an individual task, and more granular reports for the host and application groups within an interbusiness task. All reports can be accessed by clicking the highest level entry of the left navigation tree under the **Traffic Analysis and Audit** area.

To view summarized reporting for all interbusiness tasks, click the  **Inter-Business Traffic Analysis Task** entry of the left navigation tree.

NTA groups individual tasks by type. All interbusiness tasks can be found on the **Inter-Business Traffic Analysis Task** menu.

To view the **Inter-Business Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to  **Inter-Business Traffic Analysis Task**. The shortcut menu displays all interbusiness traffic analysis tasks created in NTA. Click the name of a task to view the interbusiness traffic analysis report of the task.

This section describes the reporting options available for interbusiness traffic analysis tasks. It also describes the process for navigating to interbusiness traffic analysis tasks, the summary reports available for interbusiness tasks, and the reports and features available for an interbusiness traffic analysis task.

## Navigating to the interbusiness traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. To view summary reporting for all interbusiness traffic analysis tasks, click the  **Inter-Business Traffic Analysis Task** entry under the **Traffic Analysis and Audit** area of the left navigation tree.
3. To view the report for a single task, move your mouse pointer to the shortcut menu icon  next to  **Inter-Business Traffic Analysis Task**. The **Inter-Business Traffic Analysis Task** shortcut menu displays all interbusiness traffic analysis tasks created in NTA. Click the name of a task to view the interbusiness traffic analysis report of the task.

## Summary reports for all interbusiness traffic analysis tasks

Summary reports provide the highest level of reporting for all tasks of the same type. To access the summary reports, select the  **Inter-Business Traffic Analysis Task** of the left navigation tree

under the **Traffic Analysis and Audit** area. The reports provide navigation aids to the reports for a specific task. This section describes the summary reports and their features.

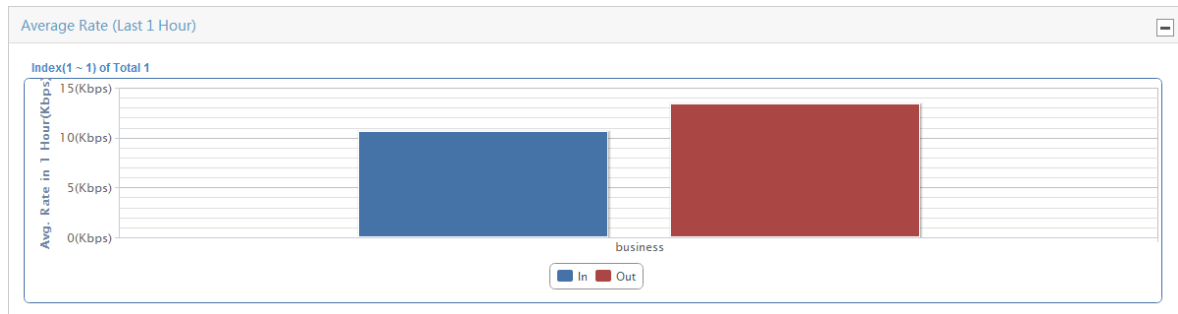
### Average rate (last 1 hour)

This bar graph summarizes traffic rates for all host and application groups in every interbusiness traffic analysis task, grouped by interbusiness traffic analysis task.

To access this graph, click the  **Inter-Business Traffic Analysis Task** entry of the left navigation tree.

The bars in the graph are links to the reports for the selected task.

**Figure 221 Average Rate (Last 1 Hour)**



### Summary list (last 1 hour)

The **Summary List** provides traffic statistics summarized by interbusiness task.

#### Summary List contents

- **Task Name**—This field contains the name of the interbusiness traffic analysis task. Click the contents of this field to navigate to reports for the associated task.
- **Total Rate**—This field provides the total rate of traffic observed for all applications configured for the associated interbusiness task for the last hour.
- **In Rate**—This metric provides the rate traffic for all inbound traffic for the host and application groups configured for the associated task for the last hour.
- **Out Rate**—This metric provides the rate traffic for all outbound traffic for the host and application groups configured for the associated task for the last hour.

The **Add** button located at the top of the **Summary List** provides a shortcut to the **Add Inter-Business Traffic Analysis Task** page. For more information on adding interbusiness traffic analysis tasks, see "[Adding an interbusiness traffic analysis task.](#)"

Click **Refresh** to update the reports with the most recent data.

## Granular reports for an interbusiness traffic analysis task

NTA provides a suite of reports that provide different perspectives for host and application data in interbusiness traffic analysis tasks. Reports for interbusiness tasks are organized into three reporting groups: Single Business, Interbusiness, and Interest.

- **Single Business reports** provide overall traffic statistics and summary statistics for all host and application groups in the selected task for the specified time range.
- **Inter-Business reports** provide traffic statistics for host and application groups within the task and for applications or hosts outside the task.
- **Interest reports** are reports that operators have added to the **Interest** list.

These reports provide navigation aids to more granular reports for the individual task.

## Single Business reports

Single Business reports for an interbusiness traffic analysis task include the **TopN Avg. Rate** bar chart, which provides average-per-second inbound and outbound traffic rates for all hosts and applications in the selected task for the specified time range. Single Business reports also include the **Traffic Details** list, which provides a summary of the total traffic volume and the rate (in seconds) for inbound and outbound traffic for all host and application groups in the selected task. As with all report types, NTA provides a query option for filtering reports based on the criteria you define.

To view the reports for an interbusiness traffic analysis task, click the **Single Business** tab to view traffic reports for the selected interbusiness traffic analysis task.

### Query traffic

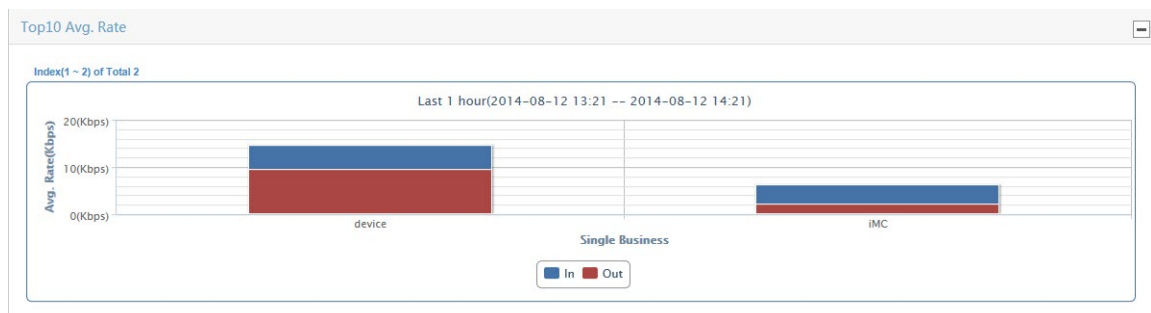
NTA enables you to change the filter criteria for traffic reports. You can refine the data presented in interbusiness reports using the **Query Traffic** option. Use this feature to change the default settings for the business name and the time range for the graphs and tables to customize the reports.

1. In the query criteria area in the upper right corner of the single business report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the single business report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
  - a. Specify the following query criteria:
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
  - b. Click **OK**.

### TopN Avg. Rate

The **TopN Avg. Rate** stacked bar chart provides average per second inbound and outbound traffic rate summarized by all host and application groups in the selected traffic analysis task. The bars are linked to allow you to navigate to more granular reports for the selected single business.

**Figure 222 TopN Avg. Rate Report**



By default, the TopN Avg. Rate stacked bar chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.

### Traffic Details

The **Traffic Details** list provides a summary of traffic statistics for all host and application groups in the task based on the report time range. This list includes total volume of inbound and outbound traffic and traffic rate in seconds for both inbound and outbound traffic for the selected time range. The business name is a link for navigating to reports for a single host and application group.

**Figure 223 Traffic Details List**

| Traffic Details        |              |           |               |            |
|------------------------|--------------|-----------|---------------|------------|
| Business Name ↕        | In Traffic ↕ | In Rate ↕ | Out Traffic ↕ | Out Rate ↕ |
| IMC                    | 1.75 MB      | 4.07 Kbps | 0.96 MB       | 2.23 Kbps  |
| device                 | 2.17 MB      | 5.06 Kbps | 4.11 MB       | 9.57 Kbps  |
| 1-2 of 2. Page 1 of 1. |              |           |               |            |
| « < 1 > » 50 ▾         |              |           |               |            |

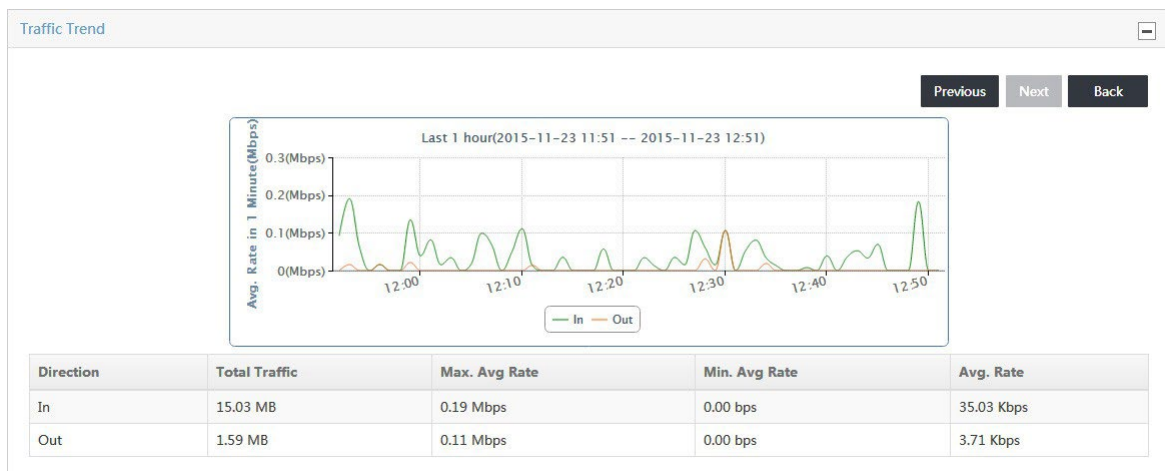
Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

### Traffic Trend – Average

The **Traffic Trend** chart provides the average rate of traffic for the single business in the associated task. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for a single business in the associated task. By default, the **Traffic Trend** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

**Figure 224 Traffic Trend Reports**



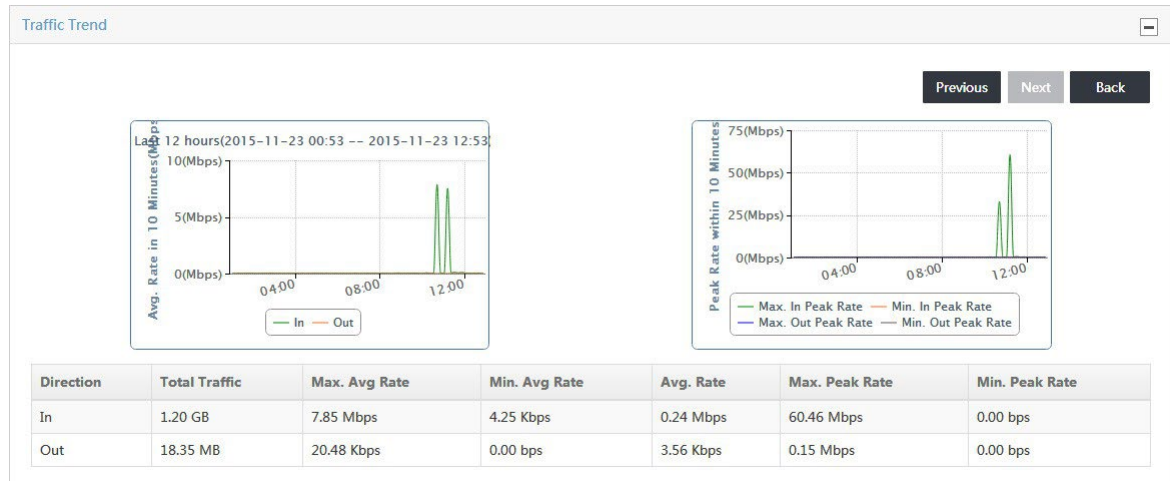
To view this report for a single business traffic in a task, click the bar in the **TopN Avg. Rate** chart report for the business whose reports you want to view.

### Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range for both inbound and outbound traffic. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

**Figure 225 Peak Rate**



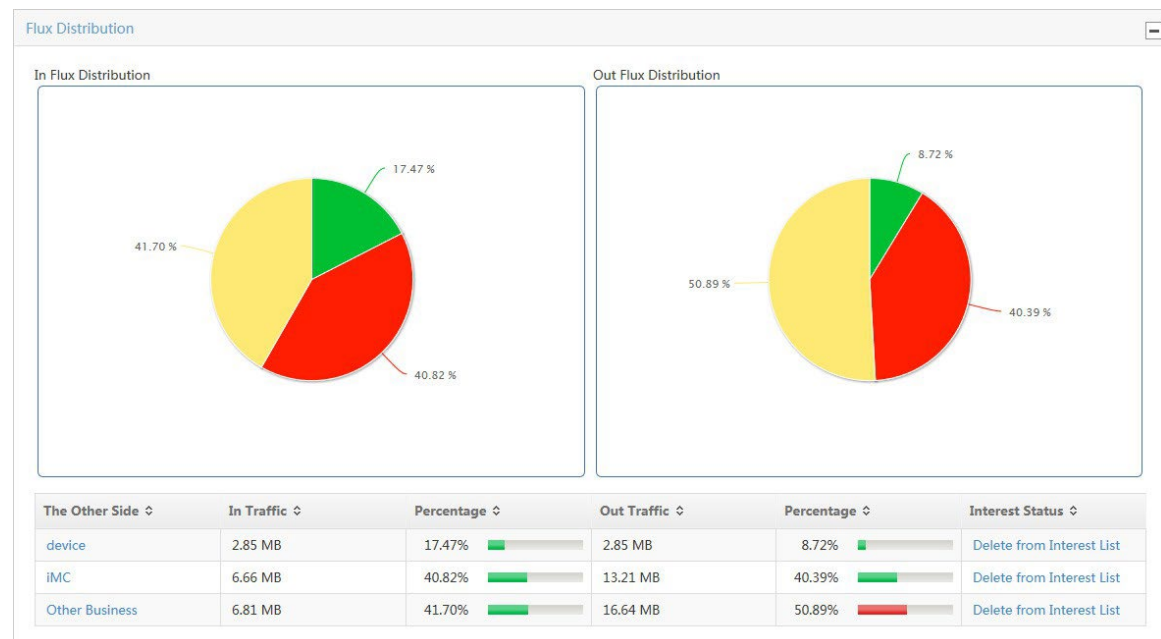
To view this report for a single business traffic in a task, click the bar in the TopN Avg. Rate chart report for the business whose reports you want to view, and set the time range for the report to a value longer than six hours.

For more information on enabling **Peak Traffic Analysis**, see "[Configuring NTA traffic analysis parameters](#)."

### Flux Distribution

The **In/Out Flux Distribution** chart displays the distribution of inbound and outbound traffic for the select business. This chart also provides the total volume of traffic and the percentage of all observed traffic for the associated business.

**Figure 226 Flux Distribution Report**



To view this report for a single business traffic in a task, click the bar in the **TopN Avg. Rate** chart report for the business whose reports you want to view.

To add a single host and application group in a task to the **Interest List**, click the **Add to Interest List** link for the associated business service you want to add.



## Interbusiness reports

Interbusiness reports for an interbusiness traffic analysis task include the **TopN Avg. Rate** stacked bar chart that provides average per second inbound and outbound traffic rates between all hosts and applications in the selected traffic analysis task for the selected time range and all other business services. The interbusiness reports also include the **Traffic Details** list that provides a summary of total traffic volume and rate in seconds between inbound and outbound traffic for all host and application groups in the selected task and all other business services. As with each of the report types, NTA also provides a query option for filtering reports based on criteria you define.

Click the **Inter-Business** tab in the interbusiness traffic analysis report to view the interbusiness reports of the task.

### Query traffic

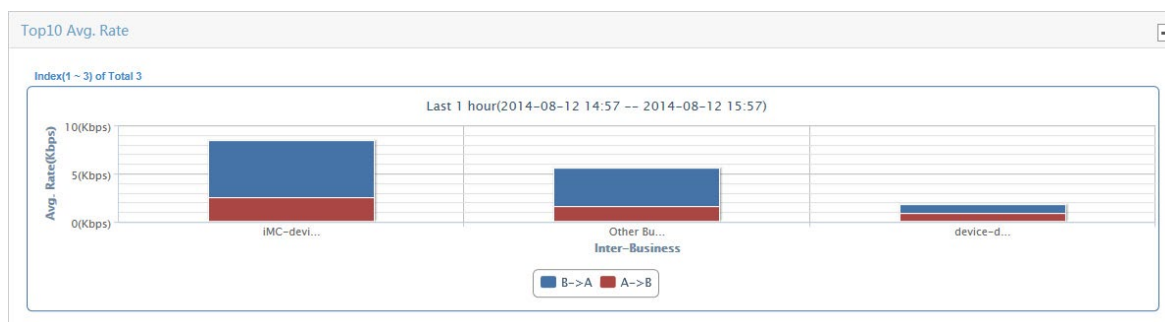
NTA enables you to change the filter criteria for traffic reports. You can refine the data presented in interbusiness reports using the **Query Traffic** option. Use this feature to customize the reports by changing the default settings for the business name and the time range for the graphs and tables.

1. In the query criteria area in the upper right corner of the interbusiness report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the interbusiness report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
  - a. Specify the following query criteria:
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
  - b. Click **OK**.

### TopN Avg. Rate

The **TopN Avg. Rate** stacked bar chart provides average per second inbound and outbound traffic rate observed between all host and application groups configured in the selected traffic analysis task and all other businesses. The bars are linked to allow you to navigate to more granular reports for the selected task.

Figure 227 TopN Avg. Rate Report



### Traffic Details



The **Traffic Details** list provides a breakdown of traffic bidirectional traffic rates between hosts and application groups configured in the task and all other business traffic. This report includes volume and rate statistics for bidirectional traffic for the selected time range.

**Figure 228 Traffic Details List**

| Traffic Details       |           |           |           |           |                                           |
|-----------------------|-----------|-----------|-----------|-----------|-------------------------------------------|
| A-B                   | B->A Flux | B->A Rate | A->B Flux | A->B Rate | Interest Status                           |
| device-device         | 0.38 MB   | 0.88 Kbps | 0.38 MB   | 0.88 Kbps | <a href="#">Delete from Interest List</a> |
| Other Business-device | 1.69 MB   | 3.94 Kbps | 0.68 MB   | 1.59 Kbps | <a href="#">Delete from Interest List</a> |
| IMC-device            | 2.50 MB   | 5.84 Kbps | 1.09 MB   | 2.53 Kbps | <a href="#">Delete from Interest List</a> |

1-3 of 3. Page 1 of 1.

Navigation: << < 1 > >> 50

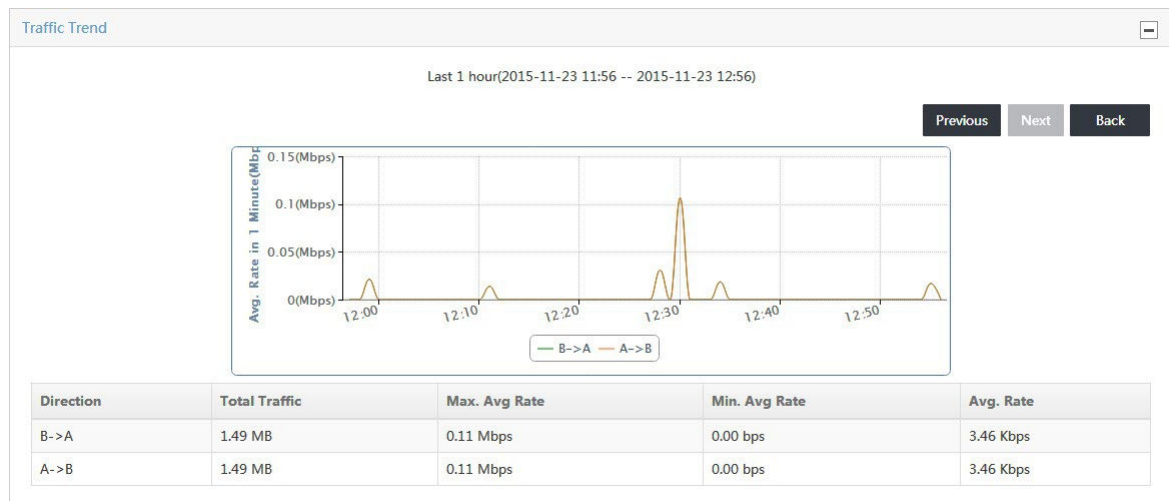
To add a bidirectional pair to the Interest List, click the **Add to Interest List** link for the associated bidirectional pair you want to add.

### Traffic Trend – Average

The **Traffic Trend** chart provides the average rate of traffic for the interbusiness in the associated task. This chart also provides average, minimum average, maximum average, and total traffic volume statistics in a tabular format for interbusiness in the associated task. By default, the **Traffic Trend** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.

**Figure 229 Traffic Trend Reports**



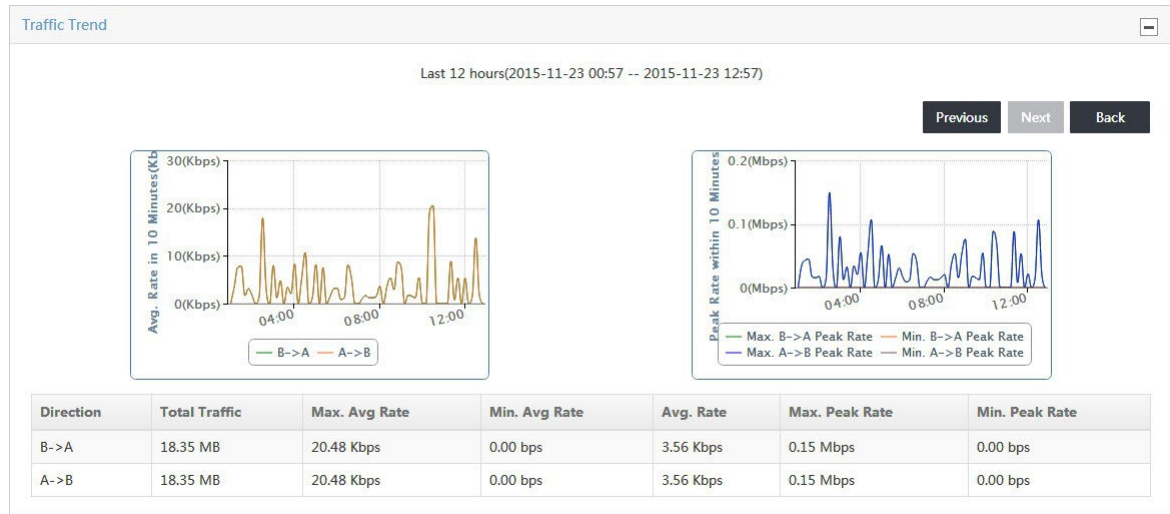
To view this report for an interbusiness traffic in a task, click the bar in the **TopN Avg. Rate** chart report for the interbusiness whose reports you want to view.

### Traffic Trend – Peak Rate

If you have enabled the Peak Traffic Analysis feature, and you have selected a time range from the **Query Time** list of the **Query Traffic** area that is at least six hours earlier than the current time, NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart.

The **Traffic Trend – Peak Rate** line chart displays, for the selected time range, the minimum and maximum inbound and outbound peak traffic rates for the associated task. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

**Figure 230 Peak Rate**



To view this report for an interbusiness traffic in a task, click the bar in the **TopN Avg. Rate** chart report for the interbusiness whose reports you want to view.

For more information on enabling Peak Traffic Analysis, see "[Configuring NTA traffic analysis parameters.](#)"

### Traffic Details

The **Traffic Details** list provides a breakdown of bidirectional traffic. This report includes total volume and rate of traffic statistics for bidirectional traffic for the selected time range.

**Figure 231 Traffic Details List**

Traffic Details

| B->A Flux           |          |           | A->B Flux           |          |           |
|---------------------|----------|-----------|---------------------|----------|-----------|
| Time                | Traffic  | Rate      | Time                | Traffic  | Rate      |
| 2015-11-23 01:00:00 | 0.00 B   | 0.00 bps  | 2015-11-23 01:00:00 | 0.00 B   | 0.00 bps  |
| 2015-11-23 01:10:00 | 0.25 MB  | 3.47 Kbps | 2015-11-23 01:10:00 | 0.25 MB  | 3.47 Kbps |
| 2015-11-23 01:20:00 | 0.54 MB  | 7.55 Kbps | 2015-11-23 01:20:00 | 0.54 MB  | 7.55 Kbps |
| 2015-11-23 01:30:00 | 0.56 MB  | 7.81 Kbps | 2015-11-23 01:30:00 | 0.56 MB  | 7.81 Kbps |
| 2015-11-23 01:40:00 | 0.12 MB  | 1.69 Kbps | 2015-11-23 01:40:00 | 0.12 MB  | 1.69 Kbps |
| 2015-11-23 01:50:00 | 0.22 MB  | 3.08 Kbps | 2015-11-23 01:50:00 | 0.22 MB  | 3.08 Kbps |
| 2015-11-23 02:00:00 | 0.12 MB  | 1.73 Kbps | 2015-11-23 02:00:00 | 0.12 MB  | 1.73 Kbps |
| 2015-11-23 02:10:00 | 0.00 B   | 0.00 bps  | 2015-11-23 02:10:00 | 0.00 B   | 0.00 bps  |
| 2015-11-23 02:20:00 | 97.66 KB | 1.33 Kbps | 2015-11-23 02:20:00 | 97.66 KB | 1.33 Kbps |

To view this list for an interbusiness traffic in a task, click the bar in the **TopN Avg. Rate** chart report for the interbusiness whose reports you want to view.

### Interest reports

Interest reports for an interbusiness traffic analysis task include those reports operators have chosen to save to the Interest List because they are of interest to the operator. Interest reports display traffic between business tasks defined in NTA and other business traffic. Reports include the **TopN Avg. Rate** stacked bar chart that provides average per second inbound and outbound traffic rates for all interbusiness tasks for the selected time range. The Interest reports also include the **Traffic Details** list that provides a summary of flux and rate statistics between business tasks and other traffic. As with each of the report types, NTA also provides a query option for filtering reports based on criteria you define.

Click the **Interest** tab in the interbusiness traffic analysis report to view the interest reports of the task.

## Query Traffic

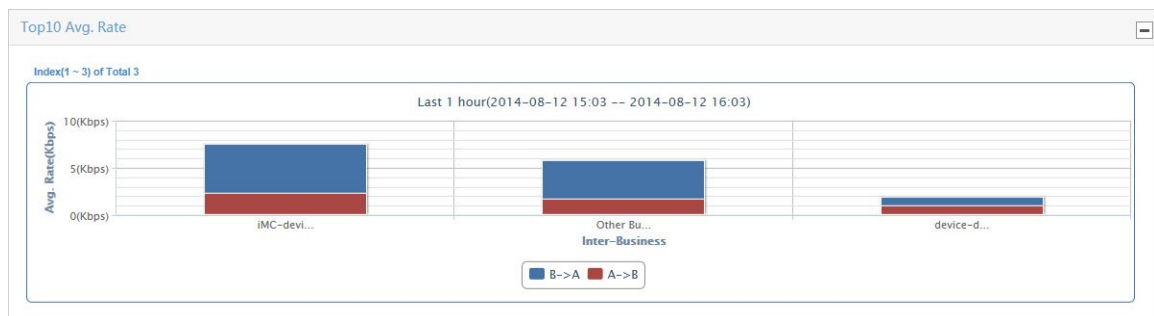
NTA enables you to change the filter criteria for traffic reports. Using the **Query Traffic** option, you can refine the data presented in interbusiness reports. To customize the reports displayed under the **Interest** tab, change the default settings for the business name and the time range for the graphs and tables.

1. In the query criteria area in the upper right corner of the interbusiness report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the interbusiness report, select **Custom** from the list that is displayed in the query criteria area, or click the **Advanced** icon  next to the query field to expand the query criteria area.
  - a. Specify the following query criteria:
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
  - b. Click **OK**.

## TopN Avg. Rate

The **TopN Avg. Rate** stacked bar chart provides average per second inbound and outbound traffic rate observed between all single business and interbusiness traffic and other traffic entries in the **Traffic Details** list saved by operators to the Interest List. The bars are linked to allow you to navigate to more granular reports.

**Figure 232 TopN Avg. Rate Report**



By default, the TopN Avg. Rate stacked bar chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To view the report for an entry, click the bar in the chart whose reports you want to view.

## Traffic Details

The **Traffic Details** list provides a breakdown of bidirectional traffic rates for all single business and interbusiness traffic and other traffic entries in the **Traffic Details** report saved by an operator to the Interest List. This report includes total volume and rate of traffic statistics for bidirectional traffic for the selected time range.

**Figure 233 Traffic Details List**

| Traffic Details                       |             |             |             |                |                                           |
|---------------------------------------|-------------|-------------|-------------|----------------|-------------------------------------------|
| A-B ↕                                 | B->A Flux ↕ | B->A Rate ↕ | A->B Flux ↕ | A->B Rate ↕    | Interest Status ↕                         |
| <a href="#">device-device</a>         | 0.40 MB     | 0.94 Kbps   | 0.40 MB     | 0.94 Kbps      | <a href="#">Delete from Interest List</a> |
| <a href="#">Other Business-device</a> | 1.75 MB     | 4.08 Kbps   | 0.72 MB     | 1.67 Kbps      | <a href="#">Delete from Interest List</a> |
| <a href="#">IMC-device</a>            | 2.23 MB     | 5.19 Kbps   | 0.98 MB     | 2.29 Kbps      | <a href="#">Delete from Interest List</a> |
| 1-3 of 3, Page 1 of 1.                |             |             |             | « < 1 > » 50 ▼ |                                           |

Select **8**, **15**, **50**, **100**, or **200** from the lower right of the main pane to configure how many items per page you want to view.

To remove a bidirectional pair from the **Traffic Details** interest list, click the **Delete from Interest List** link for the associated bidirectional pair you want to remove.

# BGP AS monitoring

This chapter provides information about BGP AS monitoring in NTA, including how NTA analyzes network flow records from an AS perspective. This chapter describes the reporting options for BGP AS traffic analyses and reviews configuration issues around BGP AS monitoring and traffic analysis tasks and the reports they generate.

This chapter also explains the process for adding BGP AS traffic analysis tasks, including instructions for adding, modifying, and deleting tasks from NTA. It provides a survey of the summary reports for all BGP AS tasks and a look at the more granular reports for an individual AS traffic analysis task.

## BGP AS traffic analysis overview

BGP AS traffic analysis tasks capture and analyze network flow data for BGP ASs. In general, the NTA BGP AS traffic analysis tasks provide traffic statistics for the BGP ASs configured in a BGP AS traffic analysis task. The BGP AS traffic reports include rate of traffic for all BGP ASs in all tasks, for all ASs in each task, and for individual ASs in a task. BGP AS statistics include traffic rate by application, source host, destination host, and a session or source/destination host pair. These reports are organized into layers from summarized information for all tasks to detailed reporting for specific BGP ASs configured for an individual BGP AS traffic analysis task.

## BGP AS traffic analysis reporting overview

After you create the first BGP AS traffic analysis task, NTA creates an entry called  **BGP AS Traffic Analysis Task** under the **Traffic Analysis and Audit** area on the left navigation tree.

Click **BGP AS Traffic Analysis Task** on the left navigation tree to view the summary report for all BGP AS traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to  **BGP AS Traffic Analysis Task**. The **BGP AS Traffic Analysis Task** shortcut menu displays all BGP AS traffic analysis tasks created in NTA. Click the name of a task to view the BGP AS traffic analysis report of the task.

To view the AS traffic analysis report of an AS in a BGP AS traffic analysis task, click the **Expand** icon  next to the task on the shortcut menu to display all ASs in the task. Click the name of an AS to view the AS traffic analysis report of the AS.

The summary BGP AS traffic analysis report provides the following information:

- **Average Rate (Last 1 Hour)**—Summarizes the average rate per second reporting for all BGP ASs specified in all BGP AS traffic analysis tasks summarized by task. Each bar in the graph is a link to more detailed reporting for the selected task, including reporting for traffic rates, application, source, destination, and session statistics. Each of these detailed report types also include several reports for the selected task:
  - **Traffic**—Reports found under the **Traffic** tab for BGP AS reporting include traffic trends that display the average inbound and outbound rate per second and the individual data samples for the BGP ASs for the selected task or for an individual AS in a task.
  - **Application**—Reports found under the **Application** tab for BGP AS reporting include a tabular report showing volume, rate, and percentage of application traffic generated by all BGP ASs in a task and a graph displaying the average rate of application traffic for all BGP ASs in the selected task or for an individual AS in a task.
  - **Source**—Reports found under the **Source** tab for BGP AS reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN source hosts and a table displaying the volume and percentage of

traffic generated for each of the TopN source hosts for all BGP ASs in the selected task or for an individual AS in a task. The contents of the pie chart link to more detailed reporting for the selected host.

- **Destination**—Reports found under the **Destination** tab for BGP AS reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN destination hosts and a table displaying the volume and percentage of traffic generated for each of the TopN destination hosts for all BGP ASs in the selected task or for an individual AS in a task. The contents of the pie chart link to more detailed reporting for the selected host.
- **Session**—Reports found under the **Session** tab for BGP AS reporting include inbound and outbound reports. Both reports include a pie chart displaying the percentage of traffic generated by the TopN source and destination host pairs and a table displaying the volume and percentage of traffic generated for each of the TopN source and destination host pairs for all BGP ASs in the selected task or for an individual AS in a task. The contents of the pie chart link to more detailed reporting for the selected host.
- **Traffic Trend and TopN Application for Selected Task (Last 1 Hour)**—Provides a per second average traffic rate summarized by BGP AS traffic analysis task for inbound and outbound traffic for all BGP ASs for all tasks. A second set of pie charts reveals the distribution of traffic for the TopN applications, with one chart each for inbound and outbound traffic.
- **Summary List (Last 1 Hour)**—Provides a per second traffic rate of traffic statistics summarized by BGP AS traffic analysis task for inbound and outbound traffic for all BGP ASs for all tasks.

## BGP AS traffic analysis configuration considerations

When adding ASs to a task, you need to consider several things. The most important decision to make is which ASs belong to each task—this determines how NTA groups ASs for analysis, reporting, and navigation purposes. Viewing statistics in juxtaposition to each other provides another level of analysis and interpretation of data. Additional considerations follow:

- By default, NTA does not monitor any ASs. You must create a task for every AS or group of ASs on which you want to monitor and report. If you do not add an AS to a task, NTA does not report on it.
- NTA presents BGP AS traffic analysis in the NTA's left navigation system, and provides summarized BGP AS reporting based on the way you organized tasks. You define how NTA groups ASs and presents them for viewing.
- You can add one or more ASs from one or more devices into a single task. You are not limited to adding ASs from a single device into one task.
- Consider how you want to access and view BGP AS data and then structure your tasks around it. For example, if you want to view BGP AS traffic statistics by geography, group the ASs into tasks organized by location. You can create a single task for every device and add all ASs from that device whose statistics you want to view into the task. Also, you can create a task for every AS if you need more detailed reporting for an AS.
- Add only those ASs whose statistics you want to view. Do not add all the ASs on a device unless you want to view reporting for all ASs. Adding ASs for which you do not want to view statistics only clutters NTA BGP AS navigation. This makes it more difficult for you to find the AS for which you do want to view data.
- You must enable network flow data on the devices for the ASs you want to monitor and report on using NTA.

# Managing BGP AS traffic analysis tasks

NTA processes, analyzes, and reports on network flow data through the tasks that administrators create. Until a task is created, NTA will not analyze the data that devices forward to it or that it is configured to receive. Effective management of tasks results in the reporting you need.

## Viewing BGP AS traffic analysis tasks

NTA displays all traffic analysis tasks in the **Traffic Analysis Task List**.

To view the NTA traffic analysis task list:

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

### Traffic Analysis Task List contents

- **Task Name**—Name of the task. This field is a link to the **Traffic Analysis Task Details** page for the task.
  - **Task Description**—Description for the task.
  - **Task Type**—Options are:
    - **Interface**
    - **VLAN/VXLAN**
    - **Probe**
    - **Application**
    - **Host**
    - **VPN**
    - **Inter-Business**
    - **BGP AS**
  - **Baseline Analysis**—Displayed when the Baseline Analysis feature is enabled in NTA parameters. The Baseline Analysis feature provides an additional layer of analysis to NTA reports by including baseline trend data that has been collected for a minimum of one week.
  - **Modify**—Contains an icon  for modifying the associated task.
  - **Delete**—Contains an icon  for deleting the associated task.
3. To query NTA for the most recent **Traffic Analysis Task List**, click **Refresh** located in the upper left corner of the **Traffic Analysis Task List**.

You can sort the **Traffic Analysis Task List** by the **Task Name**, **Task Description**, **Task Type**, and **Baseline Analysis** fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Viewing BGP AS traffic analysis task details

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link in the **Settings** portion of the **Traffic Analysis and Audit** page.

NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.

3. To view the details of a BGP AS traffic analysis task, click the name of a task of the **BGP AS** task type.

**Traffic analysis task details page**

- **Task Name**—Name of the task.
  - **Task Description**—Description of the task.
  - **Server**—Name or IP address of the NTA server.
  - **Task Type**—Options are:
    - **Interface**
    - **VLAN/VXLAN**
    - **Probe**
    - **Application**
    - **Host**
    - **VPN**
    - **Inter-Business**
    - **BGP AS**
  - **Reader**—Identifies the operator groups in INC that have been granted access to view the reports generated by the associated traffic analysis task.
  - **Baseline Analysis**—Indicates whether the Baseline Analysis feature is enabled for the task. If the **Baseline Analysis** field is not displayed, the Baseline Analysis feature is disabled. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."
  - **Enable Automatic Anomaly Detection Based On The Baseline**—Indicates whether the automatic detection of traffic anomalies based on the baseline is enabled for the task. This parameter is displayed only when baseline analysis is enabled.
  - **Baseline Threshold Setting**—Displays parameters of the baseline threshold setting. This area is displayed only when baseline analysis is enabled. The baseline threshold setting includes the following parameters:
    - **Baseline Upper/Lower Threshold**—Indicates the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
    - **Trigger**—Indicates under what condition the threshold is triggered. This condition has two configuration parameters: the time interval and the number of times that the threshold must be met.
    - **In Threshold**—Indicates the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
    - **Out Threshold**—Indicates the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
    - **Severity**—Indicates the severity level of the triggered threshold alarms, which can only be **Major**.
    - **Discard Length**—Indicates the time interval in which a triggered alarm is not sent again.
  - **AS Information**—Displays information about the AS traffic statistics that are collected and analyzed in the BGP AS analysis tasks. The AS information includes the AS ID and AS name.
  - **Device Information**—Displays information about the device traffic statistics that are collected and analyzed in the BGP AS analysis tasks. The device information includes the device name and device IP. Only traffic sent from these devices can be collected and analyzed by NTA.
4. Click **Back** to return to the **Traffic Analysis Task List**.



# Adding a BGP AS traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click **Add**.  
The **Add Traffic Analysis Task** page is displayed.
4. To add a BGP AS traffic analysis task, click the option next to **BGP AS** on the **Select Task Type** area.
5. Click **Next**.  
The **Add Traffic Analysis Task** page is refreshed.
6. Enter a name for this task in the **Task Name** field.  
The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
7. Enter a description for this task in the **Task Description** field.
8. From the **Server** list, select the NTA NetStream, NetFlow, or sFlow collection server.  
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
9. Next to the **Reader** field, click **Select** to select the operator groups that have access to the analysis and reports provided by this BGP AS task.  
The **Operator Group List** dialog box opens.
  - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access. To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.
  - b. Click **OK** to accept your operator group selection.  
The selected operator groups are displayed in the **Reader** field.
10. From the **Baseline Analysis** list, select **Enable** to enable the Baseline Analysis feature for the reports generated by this task or select **Disable** to disable the Baseline Analysis feature.  
If you selected **Enable** from this list, the baseline analysis trendline is displayed on graphs that support this feature approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week of collection. Statistics are adjusted over time as more data is collected.  
If the **Baseline Analysis** list is not displayed, it is because the Baseline Analysis feature is disabled in the NTA parameters. For more information about configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."  
When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
11. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.  
NTA automatically detects traffic anomalies and generates alarms for the anomalies according to the traffic baseline.
12. Configure the baseline threshold settings.
  - o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.

- **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
    - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
    - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
  - **In Threshold**—Specify the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
  - **Out Threshold**—Specify the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
  - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
  - **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
13. At the top of the **AS Information** list, click **Select** to add an AS.  
The **Add AS** page opens.
- a. In the **AS ID** field, manually enter the ID of AS for which traffic statistics are collected and analyzed.
  - b. In the **AS Name** field, enter a name of the AS.
  - c. Click **Add** to add the AS to the AS list for the BGP AS traffic analysis task.
  - d. Repeat this step for every AS you want to add to the BGP AS traffic analysis task.
14. To enable **Threshold Alarm** for an AS, click the  icon for the AS on the AS list to enter the page for modifying the AS.
15. From the **Threshold Alarm** list, select **Enable** if you want to generate alarms based on the data collected by this AS and the thresholds you configure, and select **Disable** if you do not want to generate alarms.  
If you selected **Enable** from the **Threshold Alarm** list, the page will update to show the **Threshold Alarm Settings** configuration parameters.
16. Configure the threshold alarm settings.
- **Direction**—Specify the direction of traffic monitoring. Options are **In**, **Out**, and **In/Out**.
  - **Trigger**—Configure the condition under which the threshold is triggered. The condition has two configuration parameters: the time interval and the number of times that the threshold must be exceeded.
    - The time interval defines the amount of time within which the threshold must be exceeded for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 5 minutes**, **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
    - You must also configure the number of times that the threshold value must be exceeded before NTA generates an alarm. Enter the number of times the threshold must be exceeded in the **times** field. The default setting is **3** times.
  - **In Threshold**—Specify the threshold value or amount of the inbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **In** or **In/Out**.

- **Out Threshold**—Specify the threshold value or amount of the outbound traffic that must be exceeded before NTA generates an alarm. Configure this field when you specify the **Direction** field as **Out** or **In/Out**.
  - **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
  - **Discard Length**—Specify the time interval in which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.
17. Click **Modify** to accept your modifications to the AS.
  18. On the **Device Information** List, select the devices for which the traffic statistics are collected and analyzed.
  19. Click **OK** to create the BGP AS traffic analysis task.

When you create a BGP AS traffic analysis task, NTA creates an entry called  **BGP AS Traffic Analysis Task** on the left navigation tree. Click the entry to view the summary report for the BGP AS traffic analysis tasks.

Move your mouse pointer to the shortcut menu icon  next to **BGP AS Traffic Analysis Task**. The **BGP AS Traffic Analysis Task** shortcut menu displays all BGP AS traffic analysis tasks created in NTA. Click the name of a task to view the BGP AS traffic analysis report of the task.

Click the **Expand** icon  next to a BGP AS traffic analysis task on the shortcut menu to display all ASs in the task. Click the name of an AS to view the BGP AS traffic analysis report of the individual AS.

For more information on accessing and viewing BGP AS traffic analysis reports, see "[Viewing BGP AS traffic analysis reports](#)."

---

 **IMPORTANT:**

You must also configure NetStream traffic from the configured devices to the NTA server. For instructions, see the device configuration guides.

---

## Modifying a BGP AS traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Traffic Analysis Task Management** link. NTA displays all tasks in the **Traffic Analysis Task List** in the main pane of the **Task Management** page.
3. Click the **Modify** icon  for the task you want to modify.
4. Modify the name for this task in the **Task Name** field as needed.  
The task name must be unique. The name you assign to a task is the link you use to navigate to the task reports. Assigning a descriptive and meaningful name to a task will help you navigate quickly and easily to reports.
5. In the **Task Description** field, modify the description for this task.
6. From the **Server** list, select the NTA, NetStream, NetFlow, or sFlow collection server.  
Unless otherwise configured by the administrator, the NTA server name is the IP address of the NTA server. If NTA is deployed on the master server, the IP address is the loopback address of the server.
7. To add new operator groups that will have access to the analysis and reports provided by this BGP AS task, click **Select** next to the **Reader** field.  
The **Operator Group List** dialog box opens.
  - a. From the **Operator Group List**, select the check box next to the operator group **Name** for every operator group to which you want to grant access.

To select all operator groups, select the check box in the upper left corner of the column label field for all boxes.

- b. Click **OK** to accept your operator group selection.

The operator groups you selected are displayed in the **Reader** field.

- c. To revoke operator group access to the results of this traffic analysis task, highlight the groups in the **Reader** field you want to remove.

- d. Click **Delete**.

- e. Click **OK** to confirm the deletion of the selected operator groups from the task.

The **Reader** reflects the deleted operator group changes.

8. To enable baseline analysis for the reports generated by this task, select **Enable** from the **Baseline Analysis** list. To disable baseline analysis, select **Disable**. If you select **Enable**, the baseline analysis trendline is displayed on graphs approximately seven days after the creation of the task. Initially, the baseline trendline displays statistics based on the first week of data collection and is adjusted as more data is collected.

If the **Baseline Analysis** list is not displayed, the Baseline Analysis feature is not enabled in the NTA parameters. For more information on configuration options for the NTA parameters, including the Baseline Analysis feature, see "[Configuring NTA traffic analysis parameters](#)."

When you select **Enable**, the **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.

9. Select **Enable** from the **Enable Automatic Anomaly Detection Based On The Baseline** list as needed.

NTA automatically detects traffic anomalies and generates alarms for the anomalies according to the traffic baseline.

10. Configure the baseline threshold settings.

- o **Baseline Upper/Lower Threshold**—Select the type of the baseline threshold. Options are **Upper Threshold**, **Lower Threshold**, and **Upper/Lower Threshold**.
- o **Trigger**—Configure the condition under which the baseline threshold is triggered. The condition has two parameters: the time interval and the number of times that the threshold must be met.
  - The time interval defines the amount of time within which the threshold must be met for the threshold to be triggered and for NTA to generate an alarm. Select the time interval you want to apply from the **Trigger** list. Options are **Last 10 minutes**, **Last 20 minutes**, and **Last 30 minutes**. The default setting is **Last 10 minutes**.
  - You must also configure the number of times that the threshold value must be met before NTA generates an alarm. Enter the number of times the threshold must be met in the **times** field. The default setting is **3** times.
- o **In Threshold**—Specify the percentage threshold for inbound traffic that must be met before NTA generates an alarm.
- o **Out Threshold**—Specify the percentage threshold for outbound traffic that must be met before NTA generates an alarm.
- o **Severity**—Specify the severity level of the triggered threshold alarms, which can only be **Major**.
- o **Discard Length**—Specify the time interval during which a triggered alarm is not sent again. Select the time interval you want to apply from the **Discard Length** list. Options are **None**, **Last 30 minutes**, **Last 1 hour**, and **Last 2 hours**. The default setting is **Last 30 minutes**.

11. To add an AS, click **Select** located at the top of the **AS Information** List. You must have at least one AS defined. The **Add AS** page is displayed.

- a. In the **AS ID** field, Manually enter the ID of AS for which traffic statistics are collected and analyzed.

- b. In the **AS Name** field, enter a name of the AS.

- c. Click **Add** to add the AS to the AS list for the BGP AS traffic analysis task.
  - d. Repeat this step for every AS you want to add to the BGP AS traffic analysis task.
  - e. To modify an AS from the AS list, click the Modify icon  for the AS you want to modify.
  - f. To remove an AS from the AS list and task, click the **Delete** icon  for the AS you want to delete.
12. On the **Device Information** List, select the devices for which the traffic statistics are collected and analyzed.
  13. Click **OK** to accept modifications to the BGP AS traffic analysis task.

## Deleting a BGP AS traffic analysis task

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. In the settings area of the **Traffic Analysis and Audit** page, click the **Traffic Analysis Task Management** link.  
NTA displays all tasks in the **Traffic Analysis Task List** displayed in the main pane of the **Task Management** page.
3. Click the **Delete** icon  for the task you want to delete.
4. Click **OK** to confirm the deletion of the selected BGP AS traffic analysis task.  
The **Traffic Analysis Task List** reflects the deletion of the selected task.

## Viewing BGP AS traffic analysis reports

NTA provides levels of reporting for all traffic analysis tasks. The highest level provides summarized reporting for all tasks of the same type. The task types are interface, VLAN/VXLAN, probe, application, host, VPN, or interbusiness or BGP AS. To access these reports, click the highest level entry on the left navigation tree in the **Traffic Analysis and Audit** area. To view summarized reporting for all BGP AS tasks, click the  **BGP AS Traffic Analysis Task** entry on the left navigation tree.

NTA also provides more detailed reporting for individual tasks, including reports for every AS configured in a BGP AS traffic analysis task. NTA groups individual tasks by type. All BGP AS tasks can be found on the **BGP AS Traffic Analysis Task** menu.

To view the **BGP AS Traffic Analysis Task** shortcut menu, move your mouse pointer to the shortcut menu icon  next to the  **BGP AS Traffic Analysis Task**. The shortcut menu displays all BGP AS traffic analysis tasks created in NTA. Click the name of a task to view the BGP AS traffic analysis report of the task. Click the **Expand** icon  next to a task on the shortcut menu to display all ASs in the BGP AS traffic analysis task. Click the name of an AS to view the BGP AS traffic analysis report of the individual AS.

This section describes the reporting options available for BGP AS traffic analysis tasks, the process for navigating to BGP AS traffic analysis tasks, the summary reports available for BGP AS tasks, and the reports and features available for a BGP AS traffic analysis task.

## Navigating to the BGP AS traffic analysis reports

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Under the **Traffic Analysis and Audit** area of the left navigation tree, click the  **BGP AS Traffic Analysis Task** entry to view summary reporting for all BGP AS tasks.

3. To view the report for a single task, move your mouse pointer to the shortcut menu icon >>> next to  **BGP AS Traffic Analysis Task**. The **BGP AS Traffic Analysis Task** shortcut menu displays all BGP AS traffic analysis tasks created in NTA. Click the name of a task to view the BGP AS traffic analysis report of the task.
4. To view the BGP AS traffic analysis report of an AS in a BGP AS traffic analysis task, click the **Expand** icon ▶ next to a task on the shortcut menu to display all ASs in the BGP AS traffic analysis task. Click the name of an AS to view the BGP AS traffic analysis report of the individual AS.

## Summary reports for all BGP AS traffic analysis tasks

Summarized reports are the highest level of reporting for all tasks of the same type. These reports are accessed by clicking the  **BGP AS Traffic Analysis Task** entry of the left navigation tree under the **Traffic Analysis and Audit** area. These reports provide navigation aids to the reports for an individual task. This section describes the summarized reports and their features.

### Average Rate (Last 1 Hour)

The **Average Rate (Last 1 Hour)** bar graph summarizes traffic rates for all ASs in every BGP AS traffic analysis task, grouped by BGP AS traffic analysis task for the last hour. You can access this graph by clicking the  **BGP AS Traffic Analysis Task** entry of the left navigation tree at the top of the page. The bars in the graph link to the reports for the selected task.

**Figure 234 Average Rate (Last 1 Hour)**



### Traffic Trend and TopN Application for Selected Task (Last 1 Hour)

The **Traffic Trend and TopN Application for Selected Task** includes a line chart and a pie chart. The line chart provides traffic trend rates for inbound or outbound traffic for the selected BGP AS traffic analysis tasks for the last hour. The pie chart displays the distribution of inbound or outbound TopN applications traffic for the selected BGP AS traffic analysis tasks for the last hour. You can access this chart by clicking the  **BGP AS Traffic Analysis Task** entry of the left navigation tree.

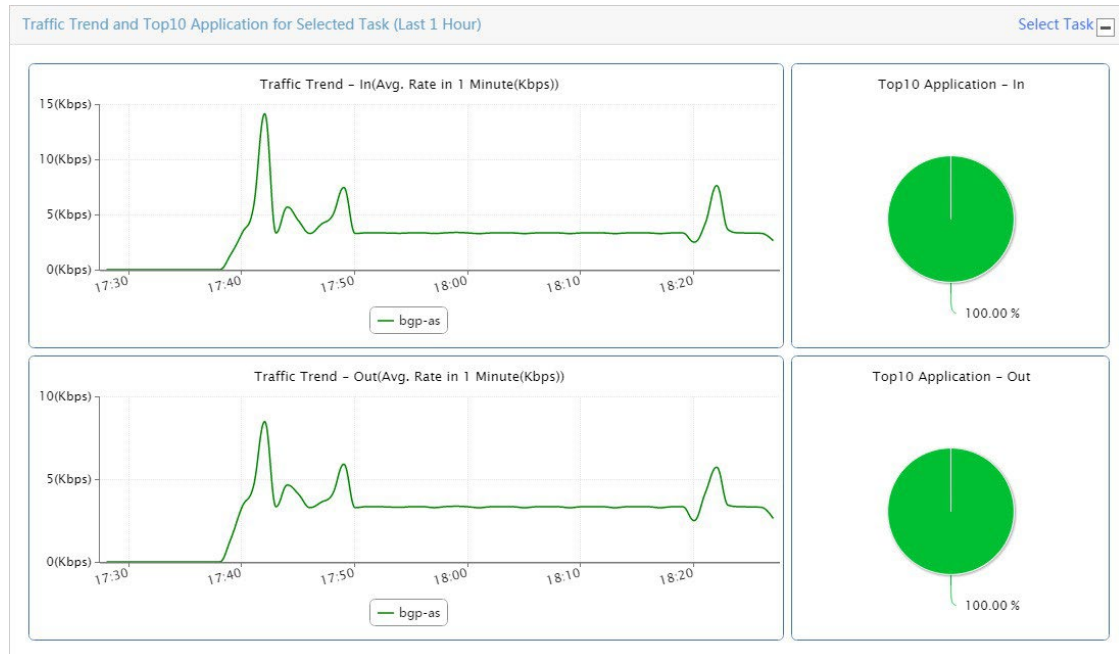
The **Traffic Trend – In** line chart provides traffic trend rates for inbound traffic for the selected BGP AS traffic analysis tasks for the last hour.

The **Traffic Trend – Out** line chart provides traffic trend rates for outbound traffic for the selected BGP AS traffic analysis tasks for the last hour.

The **TopN Application – In** pie chart displays the distribution of inbound TopN applications traffic for the selected BGP AS traffic analysis tasks for the last hour.

The **TopN Applications – Out** pie chart displays the distribution of outbound TopN applications traffic for the selected BGP AS traffic analysis tasks for the last hour.

**Figure 235 Traffic Trend and TopN Application for Selected Task**



1. To select the task, click **Select Task** in the upper right corner of the **Traffic Trend and TopN Application for Selected Task** title bar.  
The **Choose NTA Task** dialog box opens.
2. Select the check box next to the BGP AS task for which you want to use for this report.
3. Click **OK**.

The page displays an updated line chart for the selected BGP AS task.

### Summary List (Last 1 hour)

The **Summary List** provides traffic rates statistics summarized by BGP AS task.

#### Summary list contents

- **Task Name**—Contains the name of the BGP AS traffic analysis task. The contents of this field link to reports for the associated task.
- **In Rate**—Provides the rate of inbound traffic for all ASs configured for the associated task for the last hour.
- **Out Rate**—Provides the rate of outbound traffic for all ASs configured for the associated task for the last hour.

The **Add** button located at the top of the **Summary List** provides a shortcut to the **Add BGP AS Traffic Analysis Task** page.

For more information about adding BGP AS traffic analysis tasks, see "[Adding a BGP AS traffic analysis task](#)."

Click **Refresh** to update the reports with the most recent data.

## Detailed reports for a BGP AS traffic analysis task

NTA provides a suite of reports for viewing BGP AS data. BGP AS reports are organized into the following reporting groups: traffic, application, source, destination, and session.

- **Traffic reports**—Provide overall traffic statistics and the data samples collected for the specified time period.



- **Application reports**—Provide traffic statistics by application, protocol, and application category. Application reports are for Layer 4 through Layer 7 applications. The application report types follow:
  - Application reports
  - Protocol reports
  - Application category reports
- **Source reports**—Provide rate and percentage distribution of traffic by source host.
- **Destination reports**—Provide rate and percentage distribution of traffic by destination host.
- **Session reports**—Provide rate and percentage distribution of traffic for source and destination pairs.

Source, destination, and session reports enable you to get detailed information about traffic reports for an individual host/session pair.

## Traffic reports

Traffic reports provide overall traffic statistics for all ASs configured in a BGP AS traffic analysis task or for an individual AS in a task. Click the **Traffic** tab to view traffic reports.

The traffic report contains the following fields:

- **Query Traffic**—Time range for the data displayed in the traffic report.
- **Traffic Trend**—Average inbound and outbound traffic rates for all ASs in the selected traffic analysis task. This chart also provides total traffic volume, minimum average, maximum average, and average statistics in a table.
- **BGP AS Traffic Distribution**—Average rate of both inbound and outbound traffic for every AS configured in the task.
- **BGP AS Traffic Trend**—Average inbound and outbound traffic rates for selected ASs configured in the selected traffic analysis task.
- **Traffic Details**—Data collection samples that include timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic.

To view the reports for a BGP AS task, click the **Traffic** tab to view traffic reports for the selected BGP AS traffic analysis task.

### Query traffic

NTA enables you to change the filter criteria for BGP AS reports. You can change the default settings for the time range for the graphs and tables to customize the reports displayed.

1. In the query criteria area in the upper right corner of the traffic report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report.
2. To customize the time range for the traffic report, select **Custom** from the list that is displayed in the query criteria area.
  - a. Specify the following query criteria:
    - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
    - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
  - b. Click **OK**.

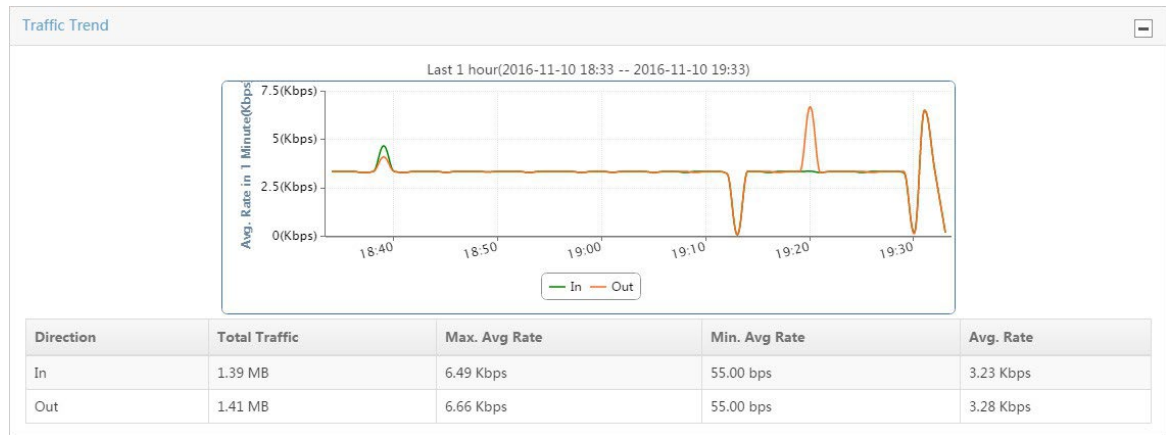
The page displays the results of your query.



## Traffic Trend – Average

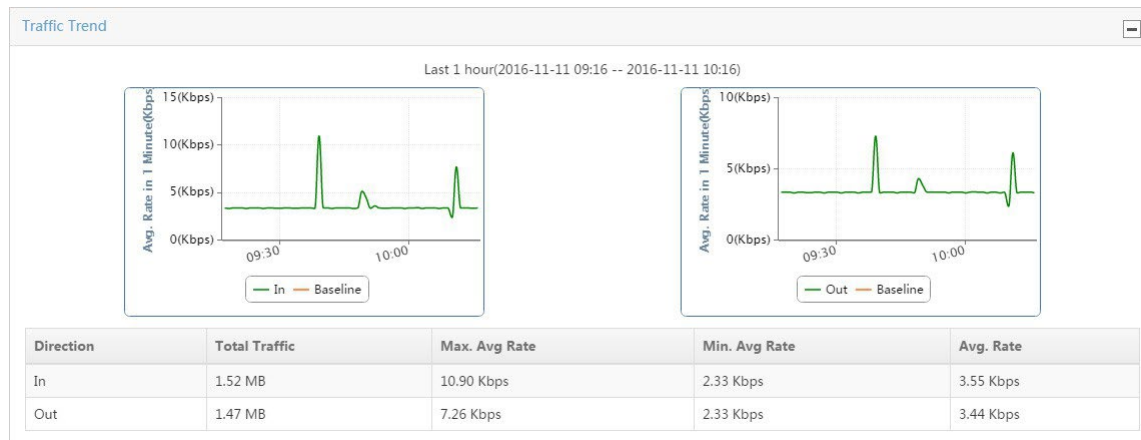
The **Traffic Trend** combination line chart provides average inbound and outbound traffic rates for all ASs in the selected traffic analysis task or for a specific AS in a BGP AS task. This chart also provides total traffic volume statistics, maximum average, minimum average, and average for both inbound and outbound traffic for the associated task or AS for the selected time range. If more than one AS exists for the selected task, these statistics reflect traffic for all ASs configured in a task.

**Figure 236 Traffic Trend**



If the selected traffic analysis task enabled the Baseline Analysis feature, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. The green line indicates the average incoming or outgoing traffic rate, and the orange line indicates the baseline. For more information about configuring the Baseline Analysis feature for the BGP AS traffic analysis task, see "[Adding a BGP AS traffic analysis task.](#)"

**Figure 237 Traffic Trend with Baseline**



To view these charts for a specific AS, click the bar in the **BGP AS Traffic Distribution** graph for the AS whose report you want to view.

By default, the **Traffic Trend** chart displays statistics for the previous hour.

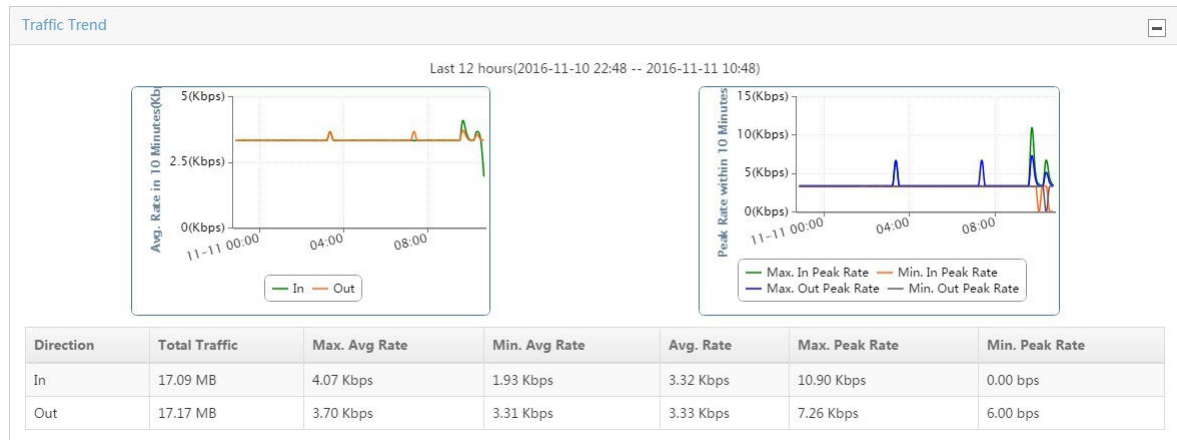
- To view data for an earlier period, click **Previous** in the upper right corner of the **Traffic Trend** chart.
- To view data for a later period, click **Next** in the upper right corner of the **Traffic Trend** chart.

## Traffic Trend – Peak Rate

NTA displays the **Max./Min. Peak Rate** chart next to the **Traffic Trend** chart when the Peak Traffic Analysis feature is enabled and the time range for the report exceeds six hours.

The **Traffic Trend – Peak Rate** line chart displays the minimum and maximum peak traffic rate for the associated task for the selected time range for both inbound and outbound traffic. This chart contains four lines: **Max. In Peak Rate**, **Min. In Peak Rate**, **Max. Out Peak Rate**, and **Min. Out Peak Rate**.

**Figure 238 Peak Rate**



If the Baseline Analysis feature is enabled for the selected traffic analysis task, the **Traffic Trend** combination line chart shows two charts: inbound **Traffic Trend** and outbound **Traffic Trend**. NTA displays the **Max./Min. In Peak Rate** chart and **Max./Min. Out Peak Rate** chart under the **Traffic Trend** chart. For more information about configuring the Baseline Analysis feature for the BGP AS traffic analysis task, see "[Adding a BGP AS traffic analysis task.](#)"

**Figure 239 Peak Rate with Baseline**



To view these charts for an individual AS, click the bar in the **BGP AS Traffic Distribution** graph for the AS whose report you want to view.

By default, the **Traffic Trend** chart displays statistics for the previous hour.

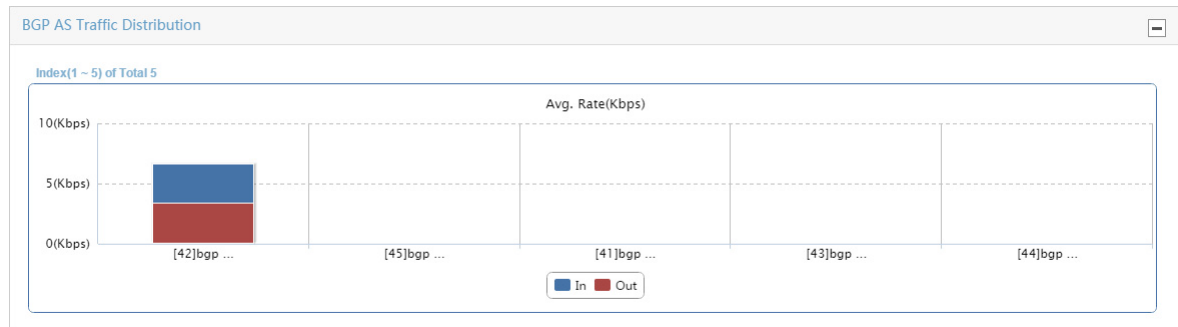
- To view data for an earlier period, click **Previous** in the upper right corner of the **Traffic Trend** chart.

- To view data for a later period, click **Next** in the upper right corner of the **Traffic Trend** chart.

### BGP AS Traffic Distribution

If the task you selected has multiple ASs configured for it, the **BGP AS Traffic Distribution** stacked bar chart displays the average rate of both inbound and outbound traffic for every AS configured in the task for the selected time range. The bars in the graph link to the reports for the selected AS.

**Figure 240 BGP AS Traffic Distribution**



This chart is displayed only when the selected task has more than one interface selected.

### BGP AS Traffic Trend

The **BGP AS Traffic Trend** line graph provides the average traffic trend for the selected ASs.

**Figure 241 BGP AS Traffic Trend**



No data will be graphed on these line charts until you specify one or more ASs.

1. To select the AS, click the **Select BGP ASes** link in the upper right corner of the **BGP AS Traffic Trend** title bar.  
The **Choose AS** dialog box is displayed.
2. Select the check boxes next to the ASs for which you want to view this report.
3. Click **OK**. The page displays the **BGP AS Traffic Trend** reports for the selected ASs.

### Traffic Details

The **Traffic Details** list provides the data collection samples for traffic statistics based on the report time range for the selected BGP AS traffic analysis task or for a selected AS in a task. This report includes timestamp, total volume of traffic, and traffic rate in seconds for both inbound and outbound traffic.

**Figure 242 Traffic Details**

| Traffic Details     |         |           |                     |         |           |
|---------------------|---------|-----------|---------------------|---------|-----------|
| Traffic - In        |         |           | Traffic - Out       |         |           |
| Time                | Traffic | Rate      | Time                | Traffic | Rate      |
| 2016-11-10 22:50:00 | 0.24 MB | 3.32 Kbps | 2016-11-10 22:50:00 | 0.24 MB | 3.32 Kbps |
| 2016-11-10 23:00:00 | 0.24 MB | 3.31 Kbps | 2016-11-10 23:00:00 | 0.24 MB | 3.31 Kbps |
| 2016-11-10 23:10:00 | 0.24 MB | 3.32 Kbps | 2016-11-10 23:10:00 | 0.24 MB | 3.32 Kbps |
| 2016-11-10 23:20:00 | 0.24 MB | 3.31 Kbps | 2016-11-10 23:20:00 | 0.24 MB | 3.32 Kbps |
| 2016-11-10 23:30:00 | 0.24 MB | 3.32 Kbps | 2016-11-10 23:30:00 | 0.24 MB | 3.31 Kbps |
| 2016-11-10 23:40:00 | 0.24 MB | 3.31 Kbps | 2016-11-10 23:40:00 | 0.24 MB | 3.31 Kbps |
| 2016-11-10 23:50:00 | 0.24 MB | 3.32 Kbps | 2016-11-10 23:50:00 | 0.24 MB | 3.32 Kbps |
| 2016-11-11 00:00:00 | 0.24 MB | 3.31 Kbps | 2016-11-11 00:00:00 | 0.24 MB | 3.32 Kbps |

To view this chart for an individual AS, click the bar in the **BGP AS Traffic Distribution** graph for the AS for which you want to view this report.

## Application Reports

Application reports provide traffic statistics by application, by protocol, and by application category for all ASs in a task or for an individual AS in a task, with information on the details for an individual application, protocol, or application category.

Application reports for a BGP AS traffic analysis task have the **Application List**, which provides a list of applications observed for all ASs in the selected BGP AS traffic analysis task or for a selected AS in a task. This list includes total volume of traffic for the associated application, rate of traffic observed on all ASs generated by the associated application. This report also provides capabilities for in-depth additional reports for the selected application.

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all ASs in the selected traffic analysis task or for an individual AS in a task.

Protocol reports for a BGP AS traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all ASs in the selected BGP AS traffic analysis task or for a selected AS in a task. This list includes total volume of traffic for the associated protocol, rate of traffic, and the percentage of all observed traffic observed on all ASs generated by the associated protocol. This report also provides capabilities for additional in-depth reports for the selected protocol.

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocol observed for all ASs in the selected traffic analysis task or for a selected AS in a task. Protocol reports also have traffic lists and trend reports for individual protocols.

Application category reports for a BGP AS traffic analysis task have the **Application Category List**, which provides a list of the application categories observed for all ASs in the selected BGP AS traffic analysis task or for a selected AS in a task. This list includes total volume of traffic for the associated application categories and rate of traffic observed on all ASs generated by the associated application category. This report also provides capabilities for in-depth additional reports for the selected application category.

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications categories observed for all ASs in the selected traffic analysis task or for an AS in a selected task. Application category reports also have traffic lists and trend reports for the individual application categories.

NTA provides a query option for filtering reports based on criteria you define. To view the reports for a BGP AS task, click the **Application** tab to view application reports for the selected BGP AS traffic analysis task, and set the **Query Type** to **Application** as described in "[Query applications](#)."

Application reports display reports organized by the list of applications in NTA. NTA provides many system-defined applications and NTA also supports user defined applications. For more information

about applications in NTA, see "[Managing applications](#)." This section describes the reports available for applications.

### Query applications

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application, or time range for the graphs and tables to customize the reports listed on the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and then select **Custom** from the list that is displayed.

2. Select **Application** from the **Query Type** list.

The page displays the report for Layer 4 through Layer 7 applications.

3. Click **Select** next to the **Application** field.

The **Query Applications** dialog box displays an empty **Application List**.

To select the applications you want to search for, you must first query the **Application List** as follows:

- a. In the **Query Applications** area of the dialog box, specify one or more of the following search criteria:
  - **Application**—Enter a partial or complete name for the applications for which you want to search.
  - **Pre-defined**—Select **Yes** to search for applications that are predefined; select **No** to filter for applications that are user defined; select **Not limited** to include system or predefined and user-defined applications.

- b. To display the full **Application List**, click **Query** without entering any search criteria.

- c. Click **Query**.

The query results are displayed in the **Application List** below the **Query Applications** area.

- d. Select the check boxes next to the applications you want to search.

- e. Click **OK** to add the applications to the filter.

The applications you selected are displayed in the **Application** field.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application report, click the icon  in the upper right corner of the application report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**.

Click the **Query** icon  in the query criteria area to set the time range for the traffic report for Layer 4 through Layer 7 applications.

4. Click **OK**.

The page displays the results of your query.

### Application List

The **Application List** provides a list of applications observed for all ASs in the selected BGP AS traffic analysis task or for a single AS in a task for the selected time range. This list includes the name of the application, an icon  for viewing the ports for all unknown applications, the total volume of traffic for the associated application, and the rate of traffic on all ASs generated by the associated

application. The application name in the **Application** field is a link to reports for the selected application.

**Figure 243 Application List**

| Application List                                        |                      |              |            |               |             |
|---------------------------------------------------------|----------------------|--------------|------------|---------------|-------------|
| Application ↕                                           | Unknown Applications | In Traffic ↕ | In Speed ↕ | Out Traffic ↕ | Out Speed ↕ |
| Telnet                                                  |                      | 18.27 KB     | 41.57 bps  | 15.68 KB      | 35.69 bps   |
| 1-1 of 1. Page 1 of 1.                                  |                      |              |            |               |             |
| <div>             « &lt; 1 &gt; » 50 ▼           </div> |                      |              |            |               |             |

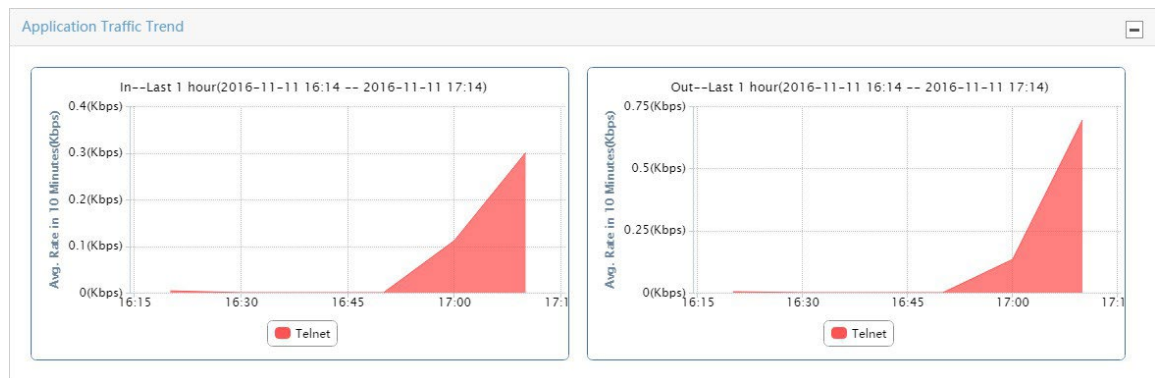
Select **8**, **15**, **50**, **100**, **200**, or **1000** from the lower right of the main pane to configure how many items per page you want to view.

Click the name of an application to view the report for the application. For more information about the report for each individual application, see "[Individual Application Reports](#)."

### Application Traffic Trend

The **Application Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. If more than one AS exists for the selected task, these statistics reflect traffic for all ASs configured in a task.

**Figure 244 Application Traffic Trend – In/Out**



## Individual Application Reports

NTA provides traffic trend statistics for the individual applications that were observed on the ASs for a selected task. Individual application reports include the **Application Traffic Trend** report that displays the average rate of traffic for the selected application. Individual application reports also include the **TopN Application Usage List** for source and destination hosts, which identifies which source and destination contributed the greatest volume of traffic for the selected application. Also included are reports for unknown TCP and UDP applications.

Unknown applications are those applications for which the Layer 4 TCP or UDP port number has not been assigned a name and is not included as an application in NTA. For more information on assigning names to TCP or UDP ports and adding them as applications to NTA, see "[Managing applications](#)."

To view individual application reports for a BGP AS task or for a single AS in a BGP AS task, click the name in the **Application** field of the **Application List** report for the application for which you want to view this report.

To view unknown application reports for a BGP AS traffic analysis task, click the icon  in the **Application** field of the **Application List** report for the application for which you want to view this report.

For more information about **Application List**, see "[Application List](#)."



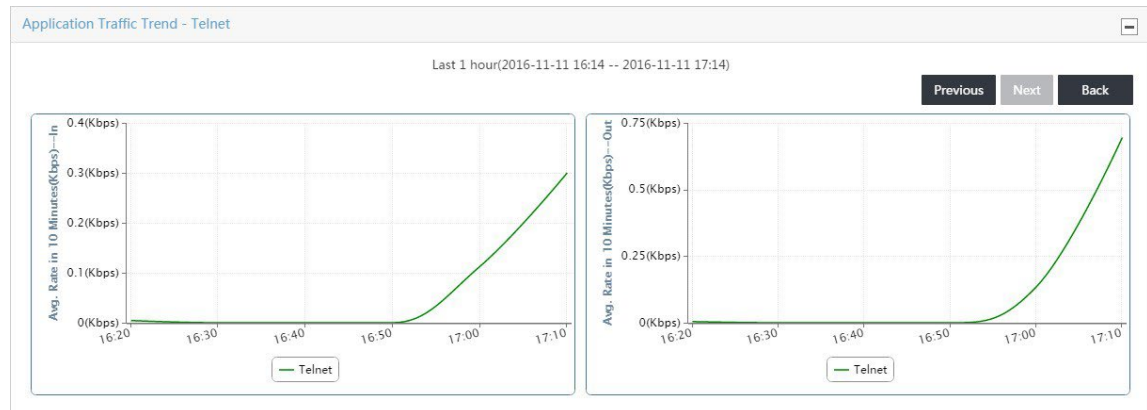
## Application Traffic Trend

The **Application Traffic Trend – In/Out** graph provides average rate of traffic for an individual application for all ASs in the selected traffic analysis task or for an individual AS in a task. If more than one AS exists for the selected task, this chart reflects traffic for all ASs configured in a task.

By default, the **Application Traffic Trend – In/Out** report graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Application** report page, click **Back**.

**Figure 245 Traffic Trend Report for the Telnet application**



## TopN Application Usage List

The **TopN Application Usage List** includes the **Source Host List – In/Out** and the **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 246 TopN Application Usage List-Telnet**

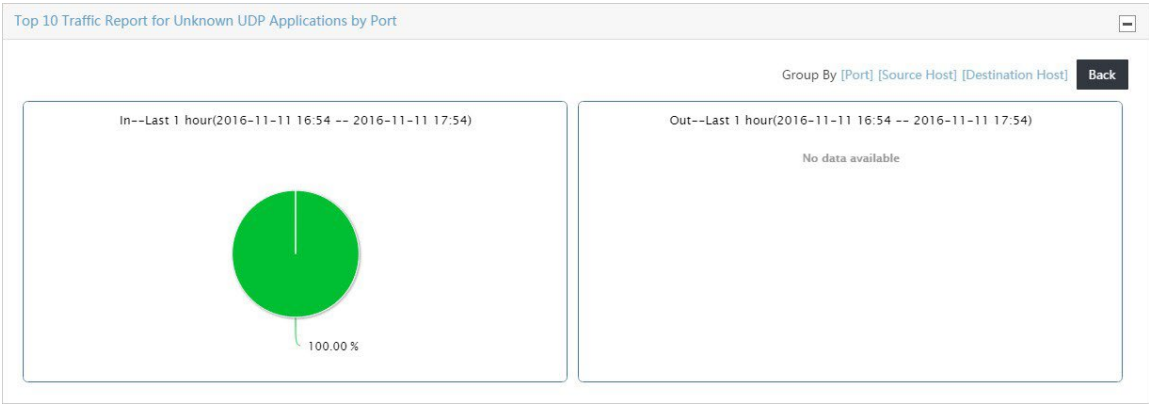
| Top 10 Application Usage List - Telnet                                                      |          |                                                                                             |                                                                                             |          |                                                                                               |
|---------------------------------------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------|
| Source Host List - In                                                                       |          |                                                                                             | Source Host List - Out                                                                      |          |                                                                                               |
| Source Host IP Address                                                                      | Traffic  | Percentage                                                                                  | Source Host IP Address                                                                      | Traffic  | Percentage                                                                                    |
|  3.1.1.2 | 30.55 KB | 100.00%  |  5.1.1.1 | 61.08 KB | 100.00%  |
| Destination Host List - In                                                                  |          |                                                                                             | Destination Host List - Out                                                                 |          |                                                                                               |
| Destination Host IP Address                                                                 | Traffic  | Percentage                                                                                  | Destination Host IP Address                                                                 | Traffic  | Percentage                                                                                    |
|  5.1.1.1 | 30.55 KB | 100.00%  |  3.1.1.2 | 61.08 KB | 100.00%  |

## TopN Traffic Report for Unknown TCP/UDP Applications by Port

The **TopN Traffic Report for Unknown TCP/UDP Applications by Port – In/Out** provides the distribution of traffic by TCP or UDP port number for all application traffic that cannot be attributed to an application or protocol for all ASs in the selected traffic analysis task for the selected time range. NTA enables you to change how the traffic is grouped.

1. From the **Group By** list in the upper right corner of the page, select **Port** to group by port.
2. From the **Group By** list, select **Source Host** to group by source host.
3. From the **Group By** list, select **Destination Host** to group by destination host.
4. Click **Back** to return to the main **Application** report page.

**Figure 247 TopN Traffic Report for Unknown TCP/UDP Applications by Port – In/Out**



**TopN Traffic List for Unknown TCP/UDP by Port**

The **TopN Traffic List for Unknown TCP/UDP Applications by Port** provides a list of the TopN unknown TCP or UDP applications measured by volume and rate of traffic observed on all ASs in the selected BGP AS traffic analysis task for the selected time range. This list includes the TCP or UDP port number, total volume of traffic for the associated source, rate of traffic, and the percentage of all observed traffic generated by the source. The port number is a link for navigating to individual reports for the selected port. The icon  in the **Define Application** field is a link for adding the selected port as a Layer 4 application to NTA. For more information on managing applications in NTA, see "[Managing applications](#)."

**Figure 248 TopN Traffic List for Unknown TCP/UDP Applications by Port**

| Top 10 Traffic List for Unknown UDP Applications by Port |          |           |                                                                                     |                     |
|----------------------------------------------------------|----------|-----------|-------------------------------------------------------------------------------------|---------------------|
| In                                                       |          |           |                                                                                     | Out                 |
| Port                                                     | Traffic  | Rate      | Define Application                                                                  | Percentage          |
| <a href="#">646</a>                                      | 43.57 KB | 99.15 bps |  | 100.00% <div></div> |
|                                                          |          |           |                                                                                     | No data available.  |

**Traffic Trend Report for Unknown TCP/UDP Applications by Port**

To view this report for a BGP AS traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **Traffic Trend** graph provides the average rate for an individual unknown application for all ASs in the selected traffic analysis task. If more than one AS exists for the selected task, this chart will reflect traffic for all ASs configured in a task. Click **Back** to return to the **Unknown Application Traffic Information** page.



Figure 249 Traffic Trend Report for Unknown TCP/UDP Applications by Port



TopN traffic Details List for Unknown TCP/UDP Applications by Port

To view this report for a BGP AS traffic analysis task, click the link in the **Port** field of the **Traffic Trend Report for Unknown Applications by Port** for the unknown TCP or UDP application whose report you want to view.

The **TopN Traffic Details List for Unknown TCP/UDP Applications by Port** displays the TopN source and destination host pairs, the volume of traffic sent and received between the source and destination hosts, the rate of traffic observed between the pair, and the percentage of all traffic observed for the source and destination hosts.

Figure 250 TopN Traffic Details List for Unknown TCP/UDP Applications by Port

| Top 10 Traffic Details List for Unknown UDP Applications by Port - 646 |                  |          |           |                     |
|------------------------------------------------------------------------|------------------|----------|-----------|---------------------|
| Source Host                                                            | Destination Host | Traffic  | Rate      | Percentage          |
| 4.1.1.2                                                                | 224.0.0.2        | 42.71 KB | 97.19 bps | 100.00% <div></div> |

Protocol reports

Protocol reports display traffic rate trend reports organized by the list of protocols predefined in NTA. Protocol reports for a BGP AS traffic analysis task include the **Protocol List**, which provides a list of protocols observed for all ASs in the selected BGP AS traffic analysis task or for an AS in a task. This report also provides drill-down capabilities for additional reports for the selected protocol. The **Protocol Traffic Trend** stacked area chart provides average inbound traffic rates for all protocols observed for all ASs in the selected traffic analysis task or for an AS in a task. Protocol reports also include traffic lists and trend reports for individual protocols.

As with all report types for a BGP AS traffic analysis task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a BGP AS traffic analysis task, click the **Application** tab to view application reports for the selected BGP AS traffic analysis task, and set **Query Type** to **Protocol** as described in "Query protocols."

For more information on protocols in NTA, see "Managing protocols." This section describes the reports available for protocols.

Query protocols

To view reports by protocol, you must configure the filter criteria for application reports. NTA enables you to change the filter criteria for protocol reports. You can change the default settings for query type, protocol, direction, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and then select **Custom** from the list that is displayed.
2. Select **Protocol** from the **Query Type** list.

The page will display the report for protocols.

3. Click **Select** next to the **Protocol** field.

The **Query Protocols** dialog box displays an empty **Protocol List**.

To select the protocols you want to search for, you must first query the **Protocol List** as follows:

- a. Enter one or more of the following search criteria in the **Query Protocols** area of the dialog box:
  - **Protocol**—Enter a partial or complete name for the protocols you want to search for in the **Protocol** field.
  - **Pre-defined**—To search for protocols that are predefined, select **Yes** from the list. To filter for protocols that are user defined, select **No** from the list. To include system or predefined and user-defined protocols, select **Not limited**.
- b. To display the full **Protocol List**, click **Query** without entering any search criteria.
- c. Click **Query**.

The query results are displayed in the **Protocol List** below the **Query Protocols** area.
- d. Select the check boxes next to the protocols for which you want to search.
- e. Click **OK** to add the protocols to the filter.

Click **Clear** to clear all selected protocols.

- **Start Time**—To autopopulate this field, click the **Calendar** icon . A pop-up calendar is displayed. Select the start date from the calendar. Adjust the hour value in the **Start Time** field.
- **End Time**—To autopopulate this field, click the **Calendar** icon . A pop-up calendar is displayed. Select the end date from the calendar. Adjust the hour value in the **End Time** field.

Additionally, to set the start time and end time for the protocol report, click the icon  in the upper right corner of the protocol report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the traffic report for protocols.

4. Click **OK**.

The page displays the results of your query.

### Protocol List

The **Protocol List** provides a list of the protocols observed for all ASs in the selected BGP AS traffic analysis task or for an AS in a task for the selected time range. This list includes the protocol name, total volume of traffic for the associated protocol, and the rate of traffic on all ASs generated by the associated protocol. The protocol name in the **Protocol** field is a link to reports for the selected protocol.

**Figure 251 Protocol List**

| Protocol List          |            |           |             |           |
|------------------------|------------|-----------|-------------|-----------|
| Protocol               | In Traffic | In Speed  | Out Traffic | Out Speed |
| ICMP                   | 1.42 MB    | 3.31 Kbps | 1.42 MB     | 3.31 Kbps |
| TCP                    | 25.98 KB   | 59.13 bps | 14.65 KB    | 33.34 bps |
| 1-2 of 2. Page 1 of 1. |            |           |             |           |

Select **8**, **15**, **50**, **100**, **200**, or **1000** from the lower right of the main pane to configure how many items per page you want to view.

Click the name of a protocol to see the report for the individual protocol. For more information about the reports for each individual protocol, see "[Individual protocol reports](#)."

### Protocol Traffic Trend

The **Protocol Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all protocols observed for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. If more than one AS exists for the selected task, these statistics reflect traffic for all ASs configured in a task.

**Figure 252 Protocol Traffic Trend – In/Out**



### Individual protocol reports

NTA provides traffic trend statistics for the individual protocol that were observed on the ASs for a selected task. Individual protocol reports include the **Protocol Traffic Trend** report that displays the average rate of traffic for the selected protocol. Individual protocol reports also include the **TopN Protocol Usage List** for source and destination hosts, which identifies which source and destination hosts contributed the greatest volume of traffic for the selected protocol.

To view individual protocol reports for a BGP AS task or for a single AS in a BGP AS task, click the name in the **Protocol** field of the **Protocol List** report for the protocol for which you want to view this report. For more information about **Protocol List**, see "[Protocol List](#)."

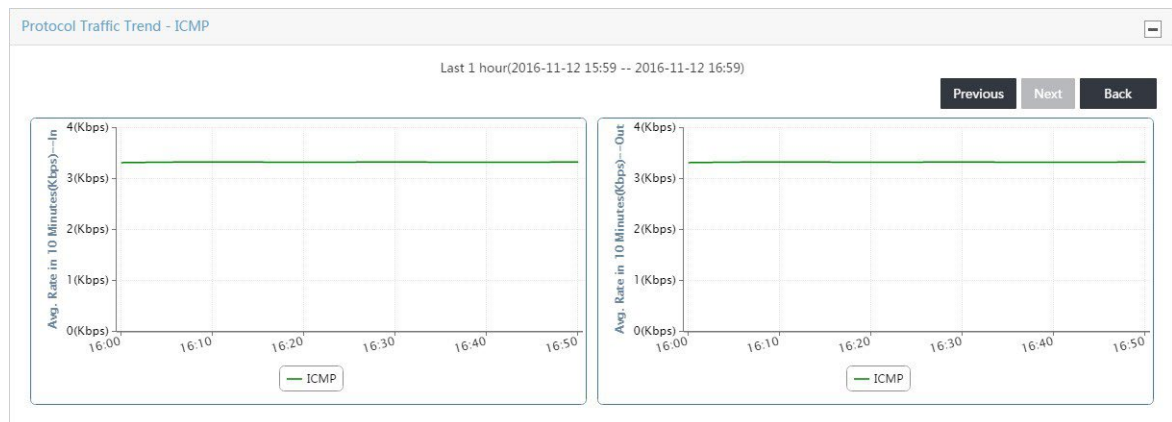
#### Protocol traffic trend

The **Protocol Traffic Trend – In/Out** graph provides average rate of traffic for an individual protocol for all ASs in the selected traffic analysis task or for a single AS in a task. If more than one AS exists for the selected task, this chart reflects traffic for all ASs configured in a task.

By default, the **Protocol Traffic Trend** graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Protocol** report page, click **Back**.

**Figure 253 Traffic Trend Report for an Individual Protocol – In/Out**



### TopN Protocol Usage List

The **TopN Protocol Usage List** includes the **Source Host List – In/Out** and the **Destination Host List – In/Out** lists.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for a single AS in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source. The host query icon  next to the **Source Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for a single AS in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 254 TopN Protocol Usage List**

| Top 10 Protocol Usage List - ICMP                                                           |         |                                                                                             |                                                                                             |         |                                                                                               |
|---------------------------------------------------------------------------------------------|---------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------------------------------------|
| Source Host List - In                                                                       |         |                                                                                             | Source Host List - Out                                                                      |         |                                                                                               |
| Source Host IP Address                                                                      | Traffic | Percentage                                                                                  | Source Host IP Address                                                                      | Traffic | Percentage                                                                                    |
|  3.1.1.2 | 1.42 MB | 100.00%  |  5.1.1.1 | 1.42 MB | 100.00%  |
| Destination Host List - In                                                                  |         |                                                                                             | Destination Host List - Out                                                                 |         |                                                                                               |
| Destination Host IP Address                                                                 | Traffic | Percentage                                                                                  | Destination Host IP Address                                                                 | Traffic | Percentage                                                                                    |
|  5.1.1.1 | 1.42 MB | 100.00%  |  3.1.1.2 | 1.42 MB | 100.00%  |

### Application category reports

Application category reports display traffic rate trend reports organized by the application categories in NTA. Application category reports for a BGP AS traffic analysis task have the **Application Category List**, which provides a list of the application categories observed for all ASs in the selected BGP AS traffic analysis task. This list has total volume of traffic for the associated application categories, rate of traffic, and the percentage of all observed traffic observed on all ASs generated by the associated application category. This report also provides capabilities for additional in-depth reports for the selected application category. The **Application Category Traffic Trend** stacked area chart provides average inbound/outbound traffic rates for all applications observed for all ASs in the selected traffic analysis task. Application category reports also have traffic lists and trend reports for the individual application categories.

As with all the report types for a BGP AS task, NTA also provides a query option for filtering reports based on criteria you define. To view the reports for a BGP AS task, click the **Application** tab to view application reports for the selected BGP AS traffic analysis task, and then set **Query Type** to **Application Category** as described in "[Query application categories](#)."

NTA provides many system-defined application categories and also supports user-defined application categories. For more information about application categories in NTA, see "[Managing application categories](#)." The introduction to application category reports also applies to individual AS traffic reports in BGP AS traffic analysis tasks.

### Query application categories

To view reports by application category, you must configure the filter criteria for application category reports.

NTA enables you to change the filter criteria for application reports. You can change the default settings for query type, application category, or time range for the graphs and tables to customize the reports displayed under the **Application** tab.

1. Click the icon  in the upper right corner of **Application Report**, and then select **Custom** from the list that is displayed.

2. Select **Application Category** from the **Query Type** list.  
The page will display the report for application categories.

3. Click **Select** next to the **Application Category** field.

The **Query Application Categories** dialog box displays an empty **Application Category List**.

To select the application categories you want to search for, you must first query the **Application Category List** as follows:

- a. Enter one or more of the following search criteria in the **Query Application Categories** area of the dialog box:
  - **Application Category**—Enter a partial or complete name for the application categories you want to search for in the **Application Category** field.
  - **Pre-defined**—To search for application categories that are predefined, select **Yes** from the list. To filter for application categories that are user defined, select **No** from the list. To include system or predefined and user-defined application categories, select **Not limited**.
- b. To display the full **Application Category List**, click **Query** without entering any search criteria.
- c. Click **Query**.  
The query results are displayed in the **Application Category List** below the **Query Application Categories** area.
- d. Click the boxes next to the application categories for which you want to search.
- e. Click **OK** to add the application categories you have selected to the filter.

The application categories you selected are displayed in the **Application Category** field.

Click **Clear**, located next to the **Application Category** field, to clear all selected application categories.

- **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
- **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.

Additionally, to set the start time and end time for the application category report, click the icon  in the upper right corner of the application category report. On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**,

**Last 30 days, Last 3 months, or Custom.** Click the **Query** icon  in the query criteria area to set the time range for the traffic report for application categories.

4. Click **OK**.

The page displays the results of your query.

### Application Category List

The **Application Category List** provides a list of the application categories observed for all ASs in the selected BGP AS traffic analysis task or for an AS in a task for the selected time range. This list includes the application category name, total volume of traffic for the associated application category, rate of traffic, and the percentage of traffic on all ASs generated by the associated application category. The application category name in the **Application Category** field is a link to reports for the selected application category.

**Figure 255 Application Category List**

| Application Category List  |              |            |               |             |
|----------------------------|--------------|------------|---------------|-------------|
| Application Category ↕     | In Traffic ↕ | In Speed ↕ | Out Traffic ↕ | Out Speed ↕ |
| Remote Management          | 23.95 KB     | 54.50 bps  | 12.04 KB      | 27.40 bps   |
| Other Application Category | 1.33 MB      | 3.10 Kbps  | 1.33 MB       | 3.10 Kbps   |
| 1-2 of 2. Page 1 of 1.     |              |            |               |             |

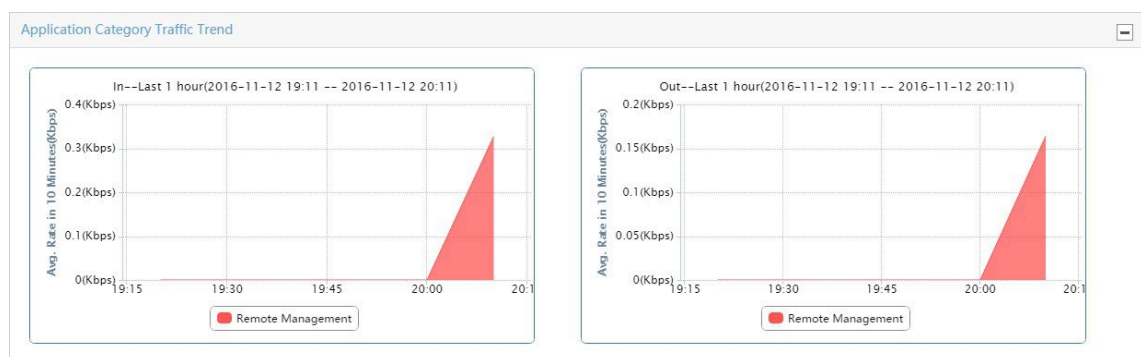
Select **8, 15, 50, 100, or 200** from the lower right of the main pane to configure how many items per page you want to view.

Click the name of an application category to view the report for the individual application category. For more information about the report for each individual application category, see "[Individual application category reports.](#)"

### Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** stacked area chart provides average inbound/outbound traffic rates for all application categories observed for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. If more than one AS exists for the selected task, these statistics reflect traffic for all ASs configured in a task.

**Figure 256 Application Category Traffic Trend**



## Individual application category reports

NTA provides traffic trend statistics for the individual application categories that were captured for the ASs for a selected task. Individual application categories reports include the **Application Category Traffic Trend** report that displays the average rate of traffic for the selected application category. Individual application category reports also include the **TopN Application Category Usage List** that identifies the TopN source and destination hosts.

To view individual application category reports for a BGP AS task or for a single AS in a task, click the name in the **Application Category** field of the **Application Category List** report for the application



category for which you want to view this report. For more information about **Application Category List**, see "[Application Category List](#)."

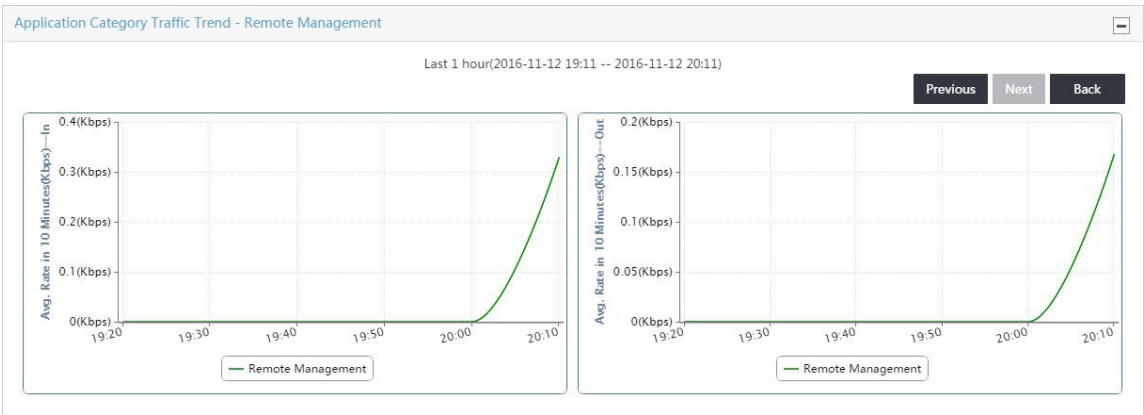
### Application Category Traffic Trend

The **Application Category Traffic Trend – In/Out** graph provides the average rate for an individual application category for all ASs in the selected traffic analysis task or for an AS in a task. If more than one AS exists for the selected task, this chart reflects traffic for all ASs configured in a task.

By default, this graph displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** in the upper right corner of the chart.
- To view data for a later period, click **Next** in the upper right corner of the chart.
- To return to the main **Application Category** report page, click **Back**.

**Figure 257 Traffic Trend Report for an Individual Application Category**



### TopN Application Category Usage List

The **TopN Application Category Usage List** includes **Source Host List – In/Out** and **Destination Host List – In/Out** for an individual application category for all ASs in the selected traffic analysis task or for an AS in a task.

The **Source Host List – In/Out** provides a list of the TopN source hosts measured by volume of traffic observed on all ASs in the selected traffic analysis task or an individual AS in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source.

The **Destination Host List – In/Out** provides a list of the TopN destination hosts measured by volume of traffic observed on all ASs in the selected traffic analysis task an individual AS in a task for the selected time range. This list includes the destination IP address, total volume of traffic for the associated destination, and the percentage of all observed traffic generated by the destination.

The host query icon  next to the **Source Host IP Address** and **Destination Host IP Address** is a link for initiating a host query and a link for navigating to the results of the query.

**Figure 258 TopN Application Category Usage List**

| Top 10 Application Category Usage List - Remote Management                                  |          |                                                                                             |                                                                                             |          |                                                                                               |
|---------------------------------------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------|
| Source Host List - In                                                                       |          |                                                                                             | Source Host List - Out                                                                      |          |                                                                                               |
| Source Host IP Address                                                                      | Traffic  | Percentage                                                                                  | Source Host IP Address                                                                      | Traffic  | Percentage                                                                                    |
|  3.1.1.2 | 24.15 KB | 100.00%  |  5.1.1.1 | 12.29 KB | 100.00%  |
| Destination Host List - In                                                                  |          |                                                                                             | Destination Host List - Out                                                                 |          |                                                                                               |
| Destination Host IP Address                                                                 | Traffic  | Percentage                                                                                  | Destination Host IP Address                                                                 | Traffic  | Percentage                                                                                    |
|  5.1.1.1 | 24.15 KB | 100.00%  |  3.1.1.2 | 12.29 KB | 100.00%  |



## Source reports

Source reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Source Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN source hosts for all ASs in the selected traffic analysis task or for an AS in a task. Both reports also include the **TopN Traffic List for Source Host**, which provides a list of the TopN source hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task. The pie chart contains a link for navigating to traffic reports for the selected host. The list also contains a link for navigating to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and the results of the host query. As with all report types for a BGP AS task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a BGP AS traffic analysis task, click the **Source** tab to view traffic reports for the selected BGP AS traffic analysis task. The introduction to source host reports also applies to individual ASs in BGP AS traffic analysis tasks.

### Query sources

NTA enables you to change the filter criteria for source reports. You can change the default settings for source host, or time range to customize the charts and lists displayed under the **Source** tab.

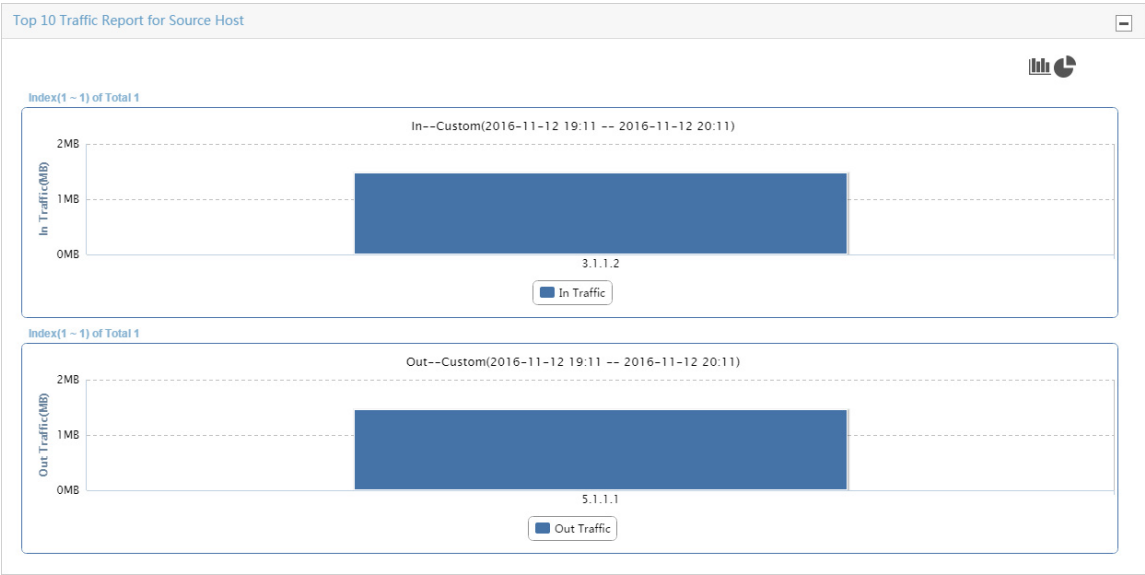
1. In the query criteria area in the upper right corner of the source report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the source report.
2. To customize the time range for the source report, select **Custom** from the list that is displayed in the query criteria area.
3. Specify one or more of the following query criteria:
  - **Source Host**—In the **Source Host** field, enter the IP address or address range. To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24  
Example of a valid IPv6 address:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.

### TopN Traffic Report for Source Host

The **TopN Traffic Report for Source Host** bar chart displays the TopN source hosts with the most inbound/outbound traffic in a certain period of time in a selected BGP AS traffic analysis task. Click a bar for a source host in the chart to view the traffic analysis report of the source host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of the TopN source hosts for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

**Figure 259 TopN Traffic Report for Source Host – In/Out**



**TopN Traffic List for Source Host**

The **TopN Traffic List for Source Host – In/Out** provides a list of the TopN source hosts measured by volume of inbound/outbound traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task for the selected time range. This list includes the source host IP address, total volume of traffic for the associated source host, total volume of traffic for the associated source, and the percentage of all observed traffic generated by the source host. The IP address is a link for navigating to reports for the selected source host. The host query icon  next to the source IP address is a link for initiating a host query and a link for navigating to the results of the host query.

**Figure 260 TopN Traffic List for Source Host – In/Out**



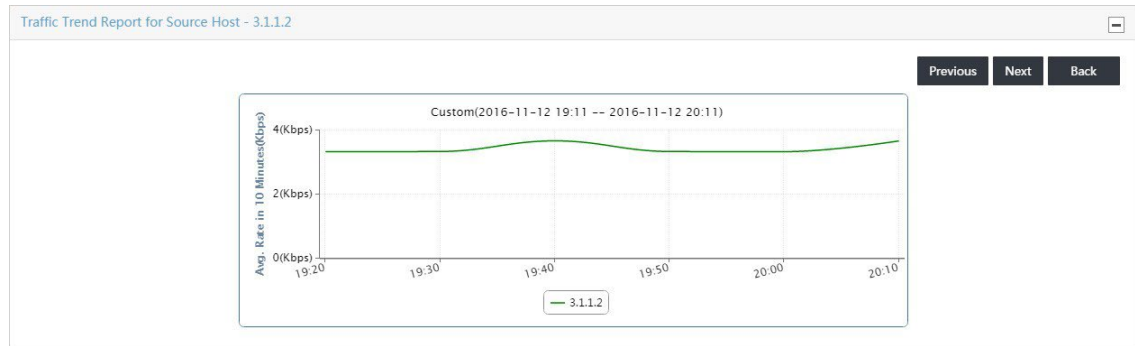
**Traffic Trend Report for Source Host**

To view this report for a BGP AS traffic analysis task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Trend Report for Source Host** line chart provides the average rate of traffic for the selected source host. By default, the **Traffic Trend Report for Source Host** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Source** host report page, click **Back**.

**Figure 261 Traffic Trend Report for Source Host**



## Traffic Details

To view this report for a BGP AS traffic analysis task, click the bar of the bar chart on the **TopN Traffic Report for Source Host** report for the source host whose statistics you want to view. Or, click the IP address for the source host whose statistics you want to view from the **TopN Traffic List for Source Host** list.

The **Traffic Details** for a source host table provides the following lists:

- The **TopN Destination Hosts Communicating with the Source Host** displays the TopN destination host IP addresses, the volume of traffic sent and received between this source and destination hosts, and the percentage of all traffic observed for this source and destination hosts.
- The **TopN Applications Communicating with the Source Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected source host, and the percentage of the associated application traffic observed for this source host.

**Figure 262 TopN Destination Hosts Communicating with the Source Host**

| Top 10 Destination Hosts Communicating with the Source Host |         |            |             | Top 10 Applications Communicating with the Source Host |          |                    |
|-------------------------------------------------------------|---------|------------|-------------|--------------------------------------------------------|----------|--------------------|
| Destination                                                 | Traffic | Percentage |             | Application Name                                       | Traffic  | Percentage         |
| 5.1.1.1                                                     | 1.47 MB | 100.00%    | <div></div> | ICMP Protocol Application                              | 1.45 MB  | 98.40% <div></div> |
|                                                             |         |            |             | Telnet                                                 | 24.15 KB | 1.60% <div></div>  |

## Destination reports

Destination reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Destination Host** pie chart. The pie chart displays the distribution of traffic generated by the TopN destination hosts for all ASs in the selected traffic analysis task or for an AS in a task. Both reports also include the **TopN Traffic List for Destination Host**, which provides a list of the TopN destination hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task. The pie chart contains a link for navigating to traffic reports for the selected host. The list also contains a link for navigating to reports for the selected destination host.

The host query icon  next to the destination IP address is a link for initiating a host query and the results of the host query. As with all report types for a BGP AS task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a BGP AS traffic analysis task, click the **Destination** tab to view traffic reports for the selected BGP AS traffic analysis task.

## Query destinations

NTA enables you to change the filter criteria for destination reports. You can change the default settings for destination host, or time range to customize the charts and lists displayed under the **Destination** tab.

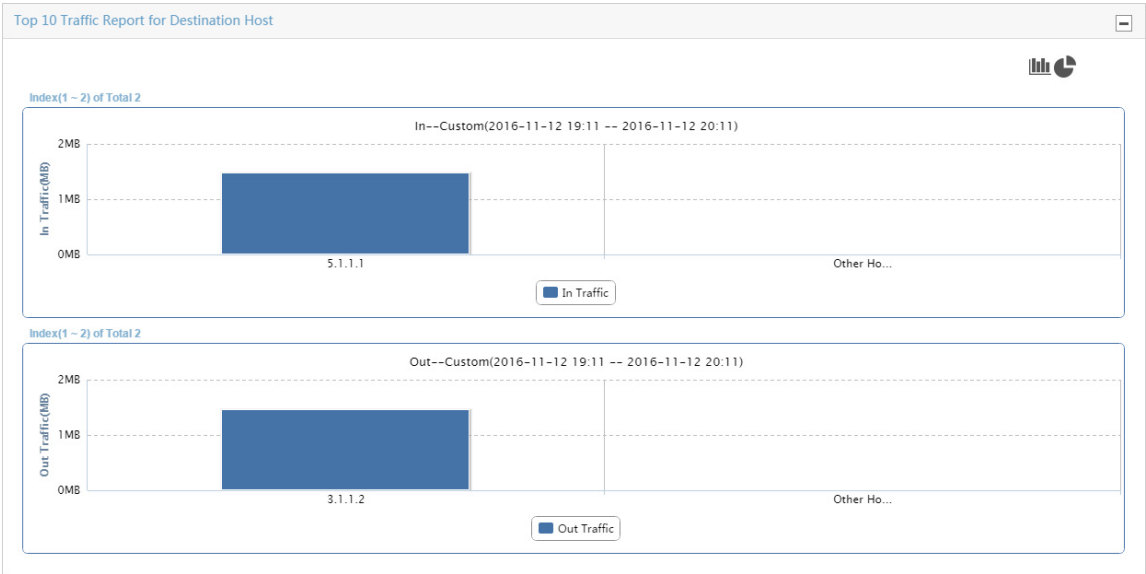
1. In the query criteria area in the upper right corner of the destination report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the destination report.
2. To customize the time range for the destination report, select **Custom** from the list that is displayed in the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Destination Host**—In the **Destination Host** field, enter the IP address or address range.
    - To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10
    - Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0
    - Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24
    - Example of a valid IPv6 address:  
a001:410:0:1::1
    - Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.

### TopN Traffic Report for Destination Host

The **TopN Traffic Report for Destination Host – In/Out** bar chart displays the TopN destination hosts with the most inbound/outbound traffic on all ASs in a certain period of time in a selected BGP AS traffic analysis task. Click a bar for a destination host in the chart to view the traffic analysis report of the destination host.

Click the pie chart icon  to change the bar chart to a pie chart. The pie chart displays the distribution of inbound/outbound traffic of TopN destination hosts for all ASs in the selected traffic analysis task for the selected time range. Each pie chart slice is a link for navigating to traffic reports for the selected host.

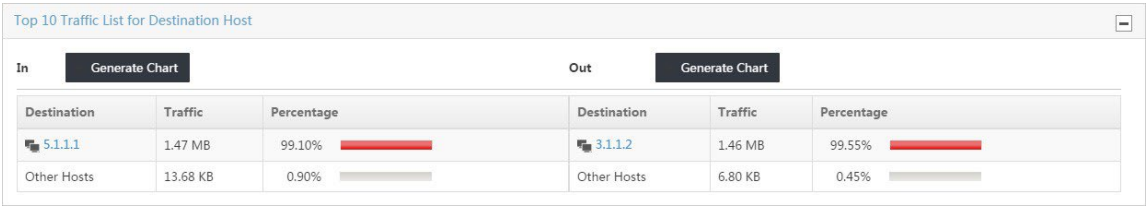
Figure 263 TopN Traffic Report for Destination Host – In/Out



TopN Traffic List for Destination Host

The **TopN Traffic List for Destination Host – In/Out** provides a list of the TopN destination hosts measured by volume of inbound/outbound traffic observed on all ASs in the selected BGP AS traffic analysis task for the selected time range. This list includes the host IP address, total volume of traffic generated by the associated destination host, and the percentage of all observed traffic generated by the destination host. The IP address is a link for navigating to reports for the selected destination host. The host query icon  next to the destination IP address is a link for initiating a host query and for navigating to the results of the host query.

Figure 264 TopN Traffic List for Destination Host – In/Out



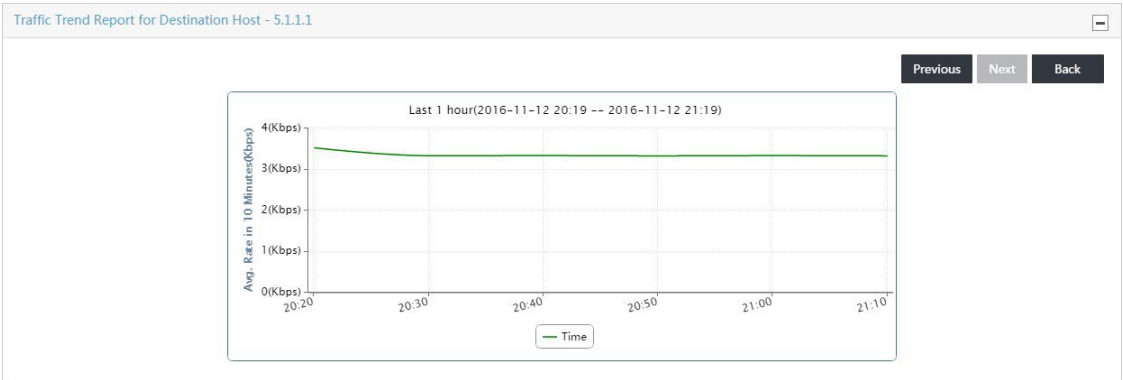
Traffic Trend Report for Destination Host

To view this report for a BGP AS traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the **TopN Traffic List for Destination Host** list.

The **Traffic Trend Report for Destination Host** line chart provides the average rate of traffic for the selected destination host. By default, the **Traffic Trend Report for Destination Host** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Destination** host report page, click **Back**.

Figure 265 Traffic Trend Report for Destination Host



Traffic Details

To view this report for a BGP AS traffic analysis task, click the pie chart slice on the **TopN Traffic Report for Destination Host** report for the destination host whose statistics you want to view. Or, click the IP address for the destination host whose statistics you want to view from the TopN Traffic List for **Destination Host** list.

The **Traffic Details** for a destination host table provides the following lists:

- The **TopN Source Hosts Communicating with the Destination Host** displays the TopN source host IP addresses, the volume of traffic sent and received between this destination host and the sources, and the percentage of all traffic observed for this destination host and the source hosts.
- The **TopN Applications Communicating with the Destination Host** displays the TopN applications, the volume of traffic attributed to the associated application for the selected destination host, and the percentage of the associated application traffic observed for this destination host.

Figure 266 Traffic Details

| Traffic Details                                             |         |            |                                                             |          |            |
|-------------------------------------------------------------|---------|------------|-------------------------------------------------------------|----------|------------|
| Top 10 Source Hosts Communicating with the Destination Host |         |            | Top 10 Applications Communicating with the Destination Host |          |            |
| Source                                                      | Traffic | Percentage | Application Name                                            | Traffic  | Percentage |
| 3.1.1.2                                                     | 1.44 MB | 100.00%    | ICMP Protocol Application                                   | 1.42 MB  | 99.00%     |
|                                                             |         |            | Telnet                                                      | 14.69 KB | 1.00%      |

Session reports

A session is a unique source and destination host pair. Session reports include inbound and outbound reports. Both reports include a **TopN Traffic Report for Session Host** pie chart. The pie chart displays the distribution of the traffic generated by the TopN session hosts for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. Both reports also include a **TopN Traffic List for Session Host**, which provides a list of the TopN session hosts measured by volume of traffic observed on all ASs in the selected BGP AS traffic analysis task or for an AS in a task. The pie chart contains a link for navigating to traffic reports for the selected session. The list also contains a link for navigating to reports for the selected session host. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and the results of the host query. As with all report types for a BGP AS task, NTA also provides a query option for filtering reports based on criteria you define.

To view the reports for a BGP AS traffic analysis task, click the **Session** tab to view traffic reports for the selected BGP AS traffic analysis task.

Query sessions

NTA enables you to change the filter criteria for session reports. You can change the default settings for source or destination session pair information, or time range to customize the charts and lists displayed under the **Session** tab.

1. In the query criteria area in the upper right corner of the session report, click the icon . On the list that is displayed, select **Last 1 hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 3 months**, or **Custom**. Click the **Query** icon  in the query criteria area to set the time range for the session report.
2. To customize the time range for the session report, select **Custom** from the list that is displayed in the query criteria area.
3. Specify one or more of the following query criteria:
  - o **Source Host**—In the **Source Host** field, enter the IP address or address range.  
To enter the IP address for a single host, enter the IP address using dotted decimal notation.  
Example of a valid IP address:  
10.153.89.10  
Example of a valid network/subnet mask in dotted decimal notation:  
10.153.89.0/255.255.255.0  
Example of a valid network/subnet mask using CIDR notation:  
10.153.89.0/24  
Example of a valid IPv6 address:  
a001:410:0:1::1  
Example of a valid IPv6 address and subnet mask using CIDR notation:  
a001:410:0:1::1/64
  - o **Destination Host**—Enter the IP address or address range in the **Destination Host** field. To enter the IP address for a single host, enter the IP address using dotted decimal notation.
  - o **Start Time**—Enter the start time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify a start time.
  - o **End Time**—Enter the end time of the time range, in YYYY-MM-DD hh:mm format. Or, click the **Calendar** icon  next to the input box to manually specify an end time.
4. Click **OK**.  
The page displays the results of your query.

### TopN Traffic Report for Session Host

The **TopN Traffic Report for Session Host – In/Out** pie chart displays the distribution of inbound and outbound traffic for TopN source and destination session pairs for all ASs in the selected traffic analysis task or for an AS in a task for the selected time range. Each pie chart slice is a link to traffic reports for the select source and destination session pair.



Figure 267 TopN Traffic Report by Session Host – In/Out



**TopN Traffic List for Session Host**

The **TopN Traffic List for Session Host – In/Out** provides a list of the TopN session source and destination pairs measured by volume of inbound/outbound traffic observed on all ASs in the selected BGP AS traffic analysis task for the selected time range. This list includes the source and destination host IP addresses, total volume of traffic generated by the source and destination session pair, and the percentage of all observed traffic generated between the source and destination session pair. The icon  in the **Details** field is a link for viewing reports for the selected session or source/destination pair. The host query icon  next to the **Source Host** and **Destination Host** IP address fields is a link for initiating a host query and a link for navigating to the results of the host query.

Figure 268 TopN Traffic Report for Session Host – In/Out

| In                                                                                          |                                                                                             |         |                                |                                                                                     |                                                                                     | Out                                                                                         |                                                                                             |         |                                |                                                                                       |                                                                                       |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------|--------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------|--------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Generate Chart                                                                              |                                                                                             |         |                                |                                                                                     |                                                                                     | Generate Chart                                                                              |                                                                                             |         |                                |                                                                                       |                                                                                       |
| Source Host                                                                                 | Destination Host                                                                            | Traffic | Percentage                     | Details                                                                             | Topology                                                                            | Source Host                                                                                 | Destination Host                                                                            | Traffic | Percentage                     | Details                                                                               | Topology                                                                              |
|  3.1.1.2 |  5.1.1.1 | 1.42 MB | 100.00% <div><div></div></div> |  |  |  5.1.1.1 |  3.1.1.2 | 1.42 MB | 100.00% <div><div></div></div> |  |  |

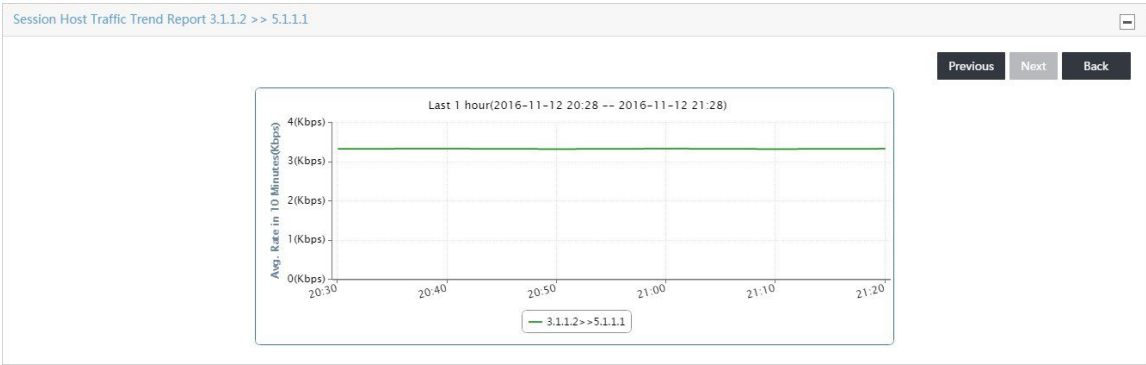
**Session Host Traffic Trend Report**

To view this report for a BGP AS traffic analysis task or for an AS in a task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **Session Host Traffic Trend Report** line chart provides the average rate of traffic for the source and destination host pair. By default, the **Session Host Traffic Trend Report** chart displays statistics for the previous hour.

- To view data for an earlier period, click **Previous** located in the upper right corner of the chart.
- To view data for a later period, click **Next** located in the upper right corner of the chart.
- To return to the main **Session** report page, click **Back**.

Figure 269 Session Host Traffic Trend Report



### TopN Applications for Session Host

To view this report for a BGP AS traffic analysis task or for an AS in a task, click the pie chart slice on the **TopN Traffic Report for Session Host** report for the session pair whose statistics you want to view. Or, click the **Details** icon  on the **TopN Traffic List for Session Host**.

The **TopN Applications for Session Host** displays the TopN applications observed for the selected session pair, the volume of traffic sent and received between this session pair, and the percentage of all traffic observed for the session pair.

Figure 270 TopN Applications for Session Host

Top 10 Applications for Session Host 3.1.1.2 >> 5.1.1.1

| Application Category      | Traffic | Percentage                                                                                  |
|---------------------------|---------|---------------------------------------------------------------------------------------------|
| ICMP Protocol Application | 1.42 MB | 99.98%  |
| Telnet                    | 0.26 KB | 0.02%   |

### Session host topology

In the **TopN Traffic List for Session Host** list, click the **Topology** icon  for a session host to view the topology between the source and destination hosts.

# Performing traffic log audits in NTA

Traffic log auditing in NTA provides the ability to generate source, destination, and session traffic reports based on the NTA data capture from the data source you select. NTA supports traffic log auditing for one interface on a device or for the selected data sources for an existing interface, probe, or VPN task. To use the traffic log auditing feature, devices, probes, and interface, probe, or VPN tasks must already exist in NTA prior to the execution of a traffic log audit. This chapter describes the process of configuring NTA to support traffic log auditing and provides instructions for executing a traffic log capture and viewing the reports generated by them.

## Configuring NTA for traffic log auditing

Traffic log auditing leverages the traffic packets captured by the interfaces of devices, VPNs, and probes that have been added to NTA and configured in traffic analysis tasks. Therefore, performing a traffic log audit for viewing source, destination, or session statistics requires pre-audit configuration of NTA. This section explains how to configure NTA before using the traffic log auditing feature.

## Adding data sources to NTA

Before using the NTA traffic log auditing feature to view source, destination, and session traffic statistics for a selected data source, you must first add the data source to NTA. Then, you must create a traffic analysis task for the interface, probe, or VPN to make the interface, probe, or VPN available as a data source for traffic log audits. This section describes adding devices, probes, and VPNs as data sources.

### Adding a device

The traffic log auditing feature enables you to use the interfaces of devices as data sources in NTA. To use a device interface in a traffic log audit, you must first add the device to NTA. For information on adding a device to NTA, see "[Device management](#)," specifically "[Adding an NTA data source device](#)."

You must also configure the device to forward NetStream, NetFlow, or sFlow traffic to the NTA server. See the vendor documentation for information on configuring a router or switch to enable NetStream, NetFlow, or sFlow data to a collector. For more information on configuring the NTA server as a collector, see "[Managing NTA servers](#)."

After you have added a device to NTA, select the device or probe in the NTA server configuration.

### Adding a probe

You can use the probes that have been configured in traffic analysis tasks as a data source for traffic log auditing. A probe in NTA is a server running probe server software that converts traffic it receives through mirroring into network flow records that NTA can process. To add a probe to NTA, see "[Probe management](#)," specifically "[Adding a probe](#)."

You must also install the probe application program on a dedicated server and configure it to receive traffic mirrored from the ports which whose statistics you want to view.

You must configure the router or switch to mirror traffic from one or more ports to the port to which the probe server is connected. If you are using a tap kit, you must also install the tap kit inline into the link being monitored. See the vendor documentation for information on configuring a router or switch to enable NetStream, NetFlow, or sFlow data to a collector, or for information on installing tap kits. For more information on configuring the NTA server to receive network flows from a probe server, see "[Managing NTA servers](#)."

After you have added a probe to NTA, you select a probe in the NTA server configuration, see "[Selecting the device or probe](#)."

## Adding a VPN

You can also use the VPNs that have been configured in traffic analysis tasks as a data source for traffic log auditing. To add a VPN to NTA, you must first add the device to which the VPN belongs. For instructions, see "[Device management](#)," specifically "[Adding an NTA data source device](#)."

You must also configure the device to forward NetStream, NetFlow, or sFlow traffic to the NTA server. See the vendor documentation for information on configuring a router or switch to enable NetStream, NetFlow, or sFlow data to a collector. For more information on configuring the NTA server as a collector, see "[Managing NTA servers](#)."

After you have added a device to NTA, you select the device or probe in the NTA server configuration, see "[Selecting the device or probe](#)."

## Selecting the device or probe

After you have added a device that includes the interface or VPN for which you want to capture a traffic audit log, you select the device or probe in the NTA server configuration.

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.  
NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.
3. Click the **Modify** icon  for the NTA server you want to modify.
4. To enable the processing of network flow data from a device in NTA, select the check box next to the device name in the **Traffic Analysis—Device Information** area.  
To disable the processing of network flow data from a device in NTA, clear the check box next to the device name.
5. To add a device that is not displayed in the **Device Information** list, see "[Device management](#)" in NTA data source management.
6. To enable the processing of network flow data from a probe (probe server) in NTA, select the check box next to the probe name in the **Traffic Analysis—Probe Information** area.  
To disable the processing of network flow data from a probe in NTA, clear the check box next to the device name.
7. To add a probe that is not displayed on the **Probe Information** list, see "[Managing NTA data sources](#)," specifically "[Probe management](#)."

---

### **IMPORTANT:**

Every device and probe selected on the **Server Configuration** page consumes a license. If you do not have enough licenses to add a device or probe, then you must clear a device or probe before adding a new one. If the device or probe you clear is already configured for an interface, VPN or probe traffic analysis task, you must remove it from the task before selecting a new device or probe on the **Server Configuration** page. For example, if you want to modify an interface task, see "[Modifying an interface traffic analysis task](#)."

---

8. Click **Deploy** to accept and deploy the NTA server configuration changes.

After you have selected a device or probe in NTA, you must create a traffic analysis task if the data source you want to use is an interface, probe, or VPN.

- For information on creating an interface traffic analysis task, see "[Managing interface traffic analysis tasks](#)," specifically "[Adding an interface traffic analysis task](#)."
- For information on creating a probe traffic analysis task, see "[Managing probe traffic analysis tasks](#)," specifically "[Adding a probe traffic analysis task](#)."
- For information on adding a VPN task to NTA, see "[Managing VPN traffic analysis tasks](#)," specifically "[Adding a VPN traffic analysis task](#)."

# Configuring the aggregation policy

NTA enables you to define the granularity that is used to process the network flow records. The standard aggregation policy summarizes data at five-minute intervals; the rough aggregation policy summarizes data at 20-minute intervals.

1. Select **Service > Traffic Analysis and Audit > Settings**.
2. Click the **Server Management** link.  
NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.
3. Click the **Modify** icon  for the NTA server you want to modify.
4. From the **Traffic Analysis Log Aggregation Policy** list, select the aggregation policy you want to apply to all log files processed by this NTA server. Options are:
  - o **No Aggregation (Best Report Timeliness)**—This option does not aggregate data and is suitable for environments with high requirements on report timeliness. This aggregation mode requires much disk space because several logs will be generated.
  - o **Aggregation (Standard)**—This option aggregates data at five-minute intervals and is suitable for environments with an average number of logs generated. It requires less disk space than No Aggregation mode and more disk space than Aggregation (Rough Granularity) mode.
  - o **Aggregation (Rough Granularity)**—This option aggregates data at 20-minute intervals and is suitable for environments with a small number of logs generated. It requires the least amount of disk space.
5. Click **Deploy** to accept and deploy the NTA server configuration changes.

## Creating an interface, probe, or VPN traffic analysis task

A traffic analysis task ties network flow records to data analysis and reporting. NTA will not capture log data for a traffic log audit if the data source has not been added to a traffic analysis task. Administrators must create traffic analysis tasks that define which data sources configured in NTA will become available for traffic log auditing. This section explains how to create traffic analysis tasks so that interfaces, probes, and VPNs are available for traffic log audits.

### Adding an interface traffic analysis task

Adding an interface traffic analysis task makes the device and its interfaces available as a data source configuration option for a traffic log audit. For more information on adding an interface task to NTA, see "[Managing interface traffic analysis tasks](#)," specifically "[Adding an interface traffic analysis task](#)."

### Adding a probe traffic analysis task

Adding a probe traffic analysis task makes the probes available as a data source configuration option for a traffic log audit. For more information on adding a probe task to NTA, see "[Managing probe traffic analysis tasks](#)," specifically "[Adding a probe traffic analysis task](#)."

### Adding a VPN traffic analysis task

Adding a VPN traffic analysis task makes VPNs available as a data source configuration option for a traffic log audit. For more information on adding a VPN task to NTA, see "[Managing VPN traffic analysis tasks](#)," specifically "[Adding a VPN traffic analysis task](#)."

After completing these configuration steps, you can perform a traffic log audit. For information on how to perform an audit, see "[Performing a traffic log audit](#)."

# Performing a traffic log audit

A traffic log audit enables you to view source, destination, and session traffic statistics for the last hour for the selected interface, probe, or VPN. This section explains how to configure NTA to perform a traffic log audit. The first step is to capture the NTA server flux log.

To initiate a traffic log audit:

1. Select **Service > Traffic Analysis and Audit > Settings** from the top navigation bar.
2. Click the **Server Management** link.  
NTA displays all servers in the **Server List** in the main pane of the **Server Management** page.
3. Click the **Capture Flux Log** icon  for the NTA server for which you want to capture a flux log.
4. When prompted, click **OK** to capture the flux log.  
The results of the Capture Flux Log request are displayed at the top of the **Server Management** page. Review the results to ensure that NTA is configured properly to capture the flux log. It may take several minutes before the captured data becomes available for viewing.
5. To configure and view the captured data, click the **Traffic Log Audit** icon  in the left navigation tree under **Traffic Analysis and Audit**.  
The **Audit Conditions** page is displayed.
6. To select the device interface, probe, or VPN whose statistics you want to view, click **Select** next to the **Audit Items** field.

The **Select Audit Item** dialog box is displayed.

All devices that have been added to NTA, selected on the NTA server configuration page, and added to traffic analysis tasks are displayed. All interface, probe, and VPN traffic analysis tasks are also displayed.

- a. Click the **Expand** icon  next to a device name to view all interfaces for that device.
- b. Click the **Expand** icon  next to a task group heading to view all tasks for the task type.
- c. Select an interface on the device, or a specific interface/probe/VPN traffic analysis task.
- d. Click **OK**.

If the interface, probe, or VPN for which you want to perform a traffic log audit is not displayed, it is likely because the device or probe has not been added to NTA, selected as a data source device for the NTA server you are using, or has not been selected as a data source for an interface, probe, or VPN traffic analysis task. For more information on configuring NTA for a traffic log audit, see "[Configuring NTA for traffic log auditing](#)."

NTA autopopulates the **Start Time** and **End Time** fields with the maximum time range permitted for a traffic log audit.

7. To change the start time range, click the **Calendar** icon  next to the **Start Time** field. A pop-up calendar is displayed. Select the start date from the calendar. Adjust the hour value in the **Start Time** field.
8. To change the end time range, click the **Calendar** icon  next to the **End Time** field. A pop-up calendar is displayed. Select the end date from the calendar. Adjust the hour value in the **End Time** field.
9. Filter the traffic log audit results based on your configuration of the filter parameters. To instruct NTA to filter based on all filter conditions you define, select **Meet all following conditions** from the **Custom Query** list. To instruct NTA to meet one or more of the conditions you define, select **Meet any of the following conditions** from the **Custom Query** list.

- To filter the traffic log audit results by source host, enter the IP address of the source host in the **Source Host** field.
  - To filter the traffic log audit results by destination host, enter the IP address of the destination host in the **Destination Host** field.
  - To filter the traffic log audit results by source port, enter the source port in the **Source Port** field.
  - To filter the traffic log audit results by destination port, enter the destination port in the **Destination Port** field.
  - To filter the traffic log audit results by Layer 4 IP protocol, select **TCP** or **UDP** from the **Protocol** list.
10. Click **Audit** to display the source, destination, and session reports generated by the audit. The page displays the source, destination, and session reports generated by the audit.

## Viewing traffic log audit reports

Traffic log audits generate three types of reports:

- **Source host reports** display statistical information for all unique source host IP addresses discovered during the log capture.
- **Destination host reports** display statistical information for all unique destination host IP addresses discovered during the log capture.
- **Session reports** display statistical information for all unique source and destination pairs discovered during the log capture.

You must initiate a flux log capture on your NTA server and submit your audit conditions configuration before NTA will update the **Audit Conditions** page to display the traffic log audit results. For more information on these steps, see "[Performing a traffic log audit.](#)"

## Source host reports

Source host reports organize, by source host IP address, the statistical information captured during the traffic log audit. Source host reports include a list of all source host IP addresses discovered during the capture and detailed information for a single host.

### Source Host List

The **Source Host List** contains a list of all unique source IP addresses identified in the flux log. The list contains statistical information about each host, including the total volume of traffic and packets and the percentage of traffic generated by the source host. It also contains links to more detailed reports for the associated host, including the **Host Query** page and the **Source Host Details List**.

To view the **Source Host List**, click the **Source** tab under the **Audit Conditions** area of the **Traffic Log Audit** page that is generated after you have initiated a flux log capture and submitted your audit conditions configuration. (For more information on these steps, see "[Performing a traffic log audit.](#)") NTA displays all source hosts that it has identified in the flux capture log.

#### Source Host List contents

-  **Query Hosts**—This icon is a link to the **Query Hosts** page that contains historical information for the associated source host.
- **Source Host**—This field contains the IP address of the source host. The field is a link to the NTA **Source Host Details Report** page for detailed information on the associated source host. For more information on this feature, see "[Source Host Details list.](#)"
- **Traffic**—This field contains the total volume of traffic generated by the associated source host for the traffic log audit time range.



- **Packet**—This field contains the total number of IP packets generated by the associated source host for the traffic log audit time range.
- **Packet Length**—This field contains the average length of the data package.
- **Percentage**—This field contains the percentage of traffic generated by the associated source host.

If the **Source Host List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Source Host List**.
- Click the **Last Page** icon  to page forward to the end of the **Source Host List**.
- Click the **Previous Page** icon  to page backward in the **Source Host List**.
- Click the **First Page** icon  to page backward to the front of the **Source Host List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the Source Host List to configure how many items per page you want to display.
- For lists that have more than one page, click a number on the lower right of the main pane to go to that page.
- To change the order of columns in this list, click **Custom** in the upper left corner of the **Source Host List**. The **Column List** dialog box is displayed.
  - To move a column up or left in the table, select the column, and then click the **Move Up** icon .
  - To move a column down or to the right in the table, select the column, and then click the **Move Down** icon .

You can sort the **Source Host List** by all fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Source Host Details list

The **Source Host Details List** contains a list of all unique destination IP addresses for the selected source host captured in the flux log. The list contains statistical information about each destination host, including the total volume of traffic and packets observed between the selected source host and the associated destination host. It also contains the source and destination ports and links to **Query Hosts** reports for the associated destination host.

To view the **Source Host Details List**, click the **Source** tab under the **Audit Conditions** area of the **Traffic Log Audit** page that is generated after you have initiated a flux log capture and submitted your audit conditions configuration. (For more information on these steps, see "[Performing a traffic log audit](#).") Click the IP address in the **Source Host** field. NTA displays all destination hosts that it has identified for the selected source host in the flux capture log.

### Source Host Details List contents

- **Start Time**—This field contains the timestamp for the start of the network flow for the selected source host and destination host.
- **End Time**—This field contains the timestamp for the end of the network flow for the selected source host and destination host.
- **Destination Host**—This field contains the IP address of the destination host. It is a link to the **Query Hosts** page for historical information on the selected destination host.
- **Protocol**—This field identifies the Layer 4 IP protocol used in the flow: TCP or UDP.
- **Source Port**—This field identifies the Layer 4 source port number for the flow. For more information on the port, click the port number in this field.

- **Destination Port**—This field identifies the Layer 4 destination port number for the flow. For more information on the port, click the port number in this field.
- **Traffic**—This field contains the total volume of traffic generated by the associated source host for the traffic log audit time range.
- **Packet**—This field contains the total number of IP packets generated by the associated source host for the traffic log audit time range.
- **Packet Length**—This field contains the average length of the data package.

If the **Source Host Details List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Source Host Details List**.
- Click the **Last Page** icon  to page forward to the end of the **Source Host Details List**.
- Click the **Previous Page** icon  to page backward in the **Source Host Details List**.
- Click the **First Page** icon  to page backward to the front of the **Source Host Details List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Source Host Details List** to configure how many items per page you want to display.
- For a **Source Host Details List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To change the order columns in this list, click **Custom** in the upper left corner of the **Source Host Details List**. The **Column List** dialog box opens.
  - To move a column up or to the left in the table, select the column, and then click the **Move Up** icon .
  - To move a column down or to the right in the table, select the column, and then click the **Move Down** icon .

You can sort the **Source Host Details List** by all fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Destination host reports

Destination host reports organize, by destination host IP address, the statistical information captured during the traffic log audit. Destination host reports include a list of all destination host IP addresses discovered during the capture and detailed reports for a single host.

### Destination Host List

The **Destination Host List** contains a list of all unique destination IP addresses identified in the flux log. The list contains statistical information about each host, including the total volume of traffic and packets and the percentage of traffic generated by the destination host. It also contains links to more detailed reports for the associated host, including the **Query Hosts** page and the **Destination Host Details List**.

To view the **Destination Host List**, click the **Destination** tab under the **Audit Conditions** area of the **Traffic Log Audit** page that is generated after you have initiated a flux log capture and submitted your audit conditions configuration. (For more information on these steps, see "[Performing a traffic log audit](#).") NTA displays all destination hosts that it has identified in the flux capture log.

### Destination Host List contents

- **Query Hosts** —This icon is a link to the **Query Hosts** page that contains historical information for the associated destination host.
- **Destination Host**—This field contains the IP address of the destination host. The field is a link to the NTA **Destination Host Details Report** page for detailed information on the associated destination host. For more information on this feature, see "[Destination Host Details list](#)."
- **Traffic**—This field contains the total volume of traffic generated by the associated destination host for the traffic log audit time range.
- **Packet**—This field contains the total number of IP packets generated by the associated destination host for the traffic log audit time range.
- **Packet Length**—This field contains the average length of the data package.
- **Percentage**—This field contains the percentage of traffic generated by the associated destination host.

If the **Destination Host List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Destination Host List**.
- Click the **Last Page** icon  to page forward to the end of the **Destination Host List**.
- Click the **Previous Page** icon  to page backward in the **Destination Host List**.
- Click the **First Page** icon  to page backward to the front of the **Destination Host List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Application List** to configure how many items per page you want to display
- For a **Destination Host List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To change the order columns in this list, click **Custom** in the upper left corner of the **Destination Host List**. The **Column List** dialog box opens.
  - To move a column up or to the left in the table, select the column, and then click the **Move Up** icon .
  - To move a column down or to the right in the table, select the column, and then click the **Move Down** icon .

You can sort the **Destination Host List** by all fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Destination Host Details list

The **Destination Host Details List** contains a list of all unique destination IP addresses for the selected destination host captured in the flux log. The list contains statistical information about each destination host, including the total volume of traffic and packets observed between the selected destination host and the associated source host. It also contains the source and destination ports and links to **Query Hosts** reports for the associated destination host.

To view the **Destination Host Details List**, click the **Destination** tab under the **Audit Conditions** area of the **Traffic Log Audit** page that is generated after you have initiated a flux log capture and submitted your audit conditions configuration. (For more information on these steps, see "[Performing a traffic log audit](#).") Click the IP address in the **Destination Host** field. NTA displays all destination hosts that it has identified for the selected destination host in the flux capture log.

### Destination Host Details List contents

- **Start Time**—This field contains the timestamp for the start of the network flow for the selected source host and destination host.

- **End Time**—This field contains the timestamp for the end of the network flow for the selected source host and destination host.
- **Source Host**—This field contains the IP address of the source host. The field is a link to the **Query Hosts** page for historical information on the selected destination host.
- **Protocol**—This field identifies the Layer 4 IP protocol used in the flow: TCP or UDP.
- **Source Port**—This field identifies the Layer 4 source port number for the flow. For more information on the port, click the port number in this field.
- **Destination Port**—This field identifies the Layer 4 destination port number for the flow. For more information on the port, click the port number in this field.
- **Traffic**—This field contains the total volume of traffic generated by the associated destination host for the traffic log audit time range.
- **Packet**—This field contains the total number of IP packets generated by the associated destination host for the traffic log audit time range.
- **Packet Length**—This field contains the average length of the data package.

If the **Destination Host Details List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Destination Host Details List**.
- Click the **Last Page** icon  to page forward to the end of the **Destination Host Details List**.
- Click the **Previous Page** icon  to page backward in the **Destination Host Details List**.
- Click the **First Page** icon  to page backward to the front of the **Destination Host Details List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Destination Host Details List** to configure how many items per page you want to display
- For a **Destination Host Details List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To change the order columns in this list, click **Custom** in the upper left corner of the **Destination Host Details List**. The **Column List** dialog box opens.
  - To move a column up or to the left in the table, select the column, and then click the **Move Up** icon .
  - To move a column down or to the right in the table, select the column, and then click the **Move Down** icon .

You can sort the **Destination Host Details List** by all fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

## Session reports

Session reports organize, by session source and destination IP address pairs, the statistical information captured during the traffic log audit. Session reports include a list of all session source and destination IP addresses discovered during the capture and historical details for both source and destination hosts.

## Session List

The **Session List** contains a list of all unique source and destination IP address pairs identified in the flux log. The list contains statistical information about each pair, including the total volume of traffic and packets, protocol used, and packet length generated by the session. It also contains links to the **Query Hosts** page.

To view the **Session List**, click the **Session** tab under the **Audit Conditions** area of the **Traffic Log Audit** page that is generated after you have initiated a flux log capture and submitted your audit conditions configuration. (For more information on these steps, see "[Performing a traffic log audit](#).") NTA displays all sessions that it has identified in the flux capture log.

### Session List contents

- **Start Time**—This field contains the timestamp for the start of the network flow for the selected source and destination host pair.
- **End Time**—This field contains the timestamp for the end of the network flow for the selected source and destination host pair.
- **Source Host** —This field contains the IP address of the session's source host. The field is a link to the **Query Hosts** page that contains historical information for the associated source host.
- **Destination Host** —This field contains the IP address of the session's destination host. The field is a link to the **Query Hosts** page that contains historical information for the associated destination host.
- **Protocol**—This field identifies the Layer 4 protocol used in the association: TCP or UDP.
- **Source Port**—This field identifies the Layer 4 source port number for the flow. For more information on the port, click the port number in this field.
- **Destination Port**—This field identifies the Layer 4 destination port number for the flow. For more information on the port, click the port number in this field.
- **Traffic**—This field contains the total volume of traffic generated by the associated destination host for the traffic log audit time range.
- **Packet**—This field contains the total number of IP packets generated by the associated session for the traffic log audit time range.
- **Packet Length**—This field contains the average length of the data package.

If the **Session List** contains enough entries, the following navigational aids are displayed:

- Click the **Next Page** icon  to page forward in the **Session List**.
- Click the **Last Page** icon  to page forward to the end of the **Session List**.
- Click the **Previous Page** icon  to page backward in the **Session List**.
- Click the **First Page** icon  to page backward to the front of the **Session List**.
- Select **8**, **15**, **50**, **100**, or **200** from the list at the lower right of the **Session List** to configure how many items per page you want to display
- For a **Session List** that has more than one page, click a number on the lower right of the main pane to go to that page.
- To change the order columns in this list, click **Custom** in the upper left corner of the **Session List**. The **Column List** dialog box opens.
  - To move a column up or to the left in the table, select the column, and then click the **Move Up** icon .

- o To move a column down or to the right in the table, select the column, and then click the **Move Down** icon .

You can sort the **Session List** by all fields. Click the column label to sort the list by the selected field. The column label allows you to toggle between the sort options specific to each field.

# NTA reports

The NTA report function is implemented through the report module of the INC platform. All reporting is template driven, meaning that reports are generated from system or user-defined templates. NTA provides the following templates:

- Device Interfaces Traffic Summary Report V2.
- Device Interfaces Application Summary Report V2.
- Interface Task Application TopN Report V2.
- Interface Task Destination Host TopN Report V2.
- Interface Task Session TopN Report V2.
- Interface Task Source Host TopN Report V2.
- Single Interface Traffic Summary Report V2.

INC offers various reporting options. From the **Report** tab, you can quickly and easily access NTA's template-driven reports on the device interface traffic and device interface applications. You can view and export realtime reports and scheduled reports. For instructions on viewing realtime reports and scheduled reports,

The NTA report function provides scheduled reports. You can schedule NTA reports to run daily, weekly, monthly, quarterly, semi-annually, or annually. You can define the start dates of data collection for scheduled reports, and the end dates and times for the corresponding scheduled report tasks. You configure the report formats with options for Adobe Acrobat PDF, XLS, CSV, DOCX, RTF, XLSX, PPTX, HTML, or JRXML. You can include email recipients for all scheduled reports. A description of each report template follows.

- **Device Interfaces Traffic Summary Report V2**—Provides traffic statistics for the interfaces of the specified device managed by NTA. The report shows the summary traffic statistics for all interfaces of a device to which the operator has access. To view the report, set the following parameters:
  - **Device Name**—Select the device for which a report will be generated. You can set only one device.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.
- **Device Application Summary Report V2**—Provides application statistics for the specified devices managed by NTA. The report shows the summary application statistics for a device to which the operator has access. To view the report, set the following parameters:
  - **Device Name**—Select the device for which a report will be generated. You can set only one device.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.
- **Interface Task Application TopN Report V2**—Provides traffic statistics for TopN applications, protocols, or application types of an interface traffic analysis task. To view the report, set the following parameters:
  - **Interface Task**—Select the interface task for which a report will be generated. You can set only one interface task.
  - **Query Type**—Select the traffic type. Options are **Application**, **Protocol**, and **Application Type**.
  - **TopN**—Select the number of traffic entries for applications, protocols, or application types you want to display. Options are **10**, **20**, **50**, and **100**.
  - **Begin Time**—Set the start time for the time range in a data collection period.



- **End Time**—Set the end time for the time range in a data collection period.
- **Interface Task Destination Host TopN Report V2**—Provides traffic statistics for TopN destination hosts of an interface traffic analysis task. To view the report, set the following parameters:
  - **Interface Task**—Select the interface task for which a report will be generated. You can set only one interface task.
  - **TopN**—Select the number of traffic entries for destination hosts you want to display. Options are **10**, **20**, **50**, and **100**.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.
- **Interface Task Session TopN Report V2**—Provides traffic statistics for TopN sessions of an interface traffic analysis task. To view the report, set the following parameters:
  - **Interface Task**—Select the interface task for which a report will be generated. You can set only one interface task.
  - **TopN**—Select the number of traffic entries for sessions you want to display. Options are **10**, **20**, **50**, and **100**.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.
- **Interface Task Source Host TopN Report V2**—Provides traffic statistics for TopN source hosts of an interface traffic analysis task. To view the report, set the following parameters:
  - **Interface Task**—Select the interface task for which a report will be generated. You can set only one interface task.
  - **TopN**—Select the number of traffic entries for source hosts you want to display. Options are **10**, **20**, **50**, and **100**.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.
- **Single Interface Traffic Summary Report V2**—Provides traffic statistics for the specified interface of a device managed by NTA. The report shows the summary traffic statistics for the specified interface of a device to which the operator has access. To view the report, set the following parameters:
  - **Interface Name**—Select the interface for which a report will be generated. You can set only one interface.
  - **Begin Time**—Set the start time for the time range in a data collection period.
  - **End Time**—Set the end time for the time range in a data collection period.

# NTA widgets

NTA provides various widgets, including dashboard widgets and home page widgets.

The HTML5-based dashboard widgets function of INC displays multiple monitoring tasks simultaneously on a high-resolution screen. NTA provides the following dashboard widgets:

- Traffic Trend for Interface NTA Task (Last 1 Hour)
- Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)
- Traffic Trend for Probe NTA Task (Last 1 Hour)
- Traffic Trend for Application NTA Task (Last 1 Hour)
- Traffic Trend for Host NTA Task (Last 1 Hour)
- Traffic Trend for VPN NTA Task (Last 1 Hour)
- Application Traffic Trend for Interface NTA Task

The home page customization function of INC allows an operator to customize a home page. The operator can customize different home page widgets after logging in to the INC home page. This function facilitates viewing various monitoring information. NTA provides the following home page widgets:

- TopN Application for Interface NTA Task (Last 1 Hour)
- TopN Application for VLAN/VXLAN NTA Task (Last 1 Hour)
- TopN Application for Probe NTA Task (Last 1 Hour)
- TopN Application for Host NTA Task (Last 1 Hour)
- TopN Application for VPN NTA Task (Last 1 Hour)
- Traffic Trend for Application NTA Task (Last 1 Hour)
- Traffic Trend for Host NTA Task (Last 1 Hour)
- Traffic Trend for Interface NTA Task (Last 1 Hour)
- Traffic Trend for Probe NTA Task (Last 1 Hour)
- Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)
- Traffic Trend for VPN NTA Task (Last 1 Hour)
- Application Traffic for Host NTA Task (Last 1 Hour)
- TopN Session List (Last 1 Hour)

## Dashboard widgets

Dashboard widgets provided by NTA include:

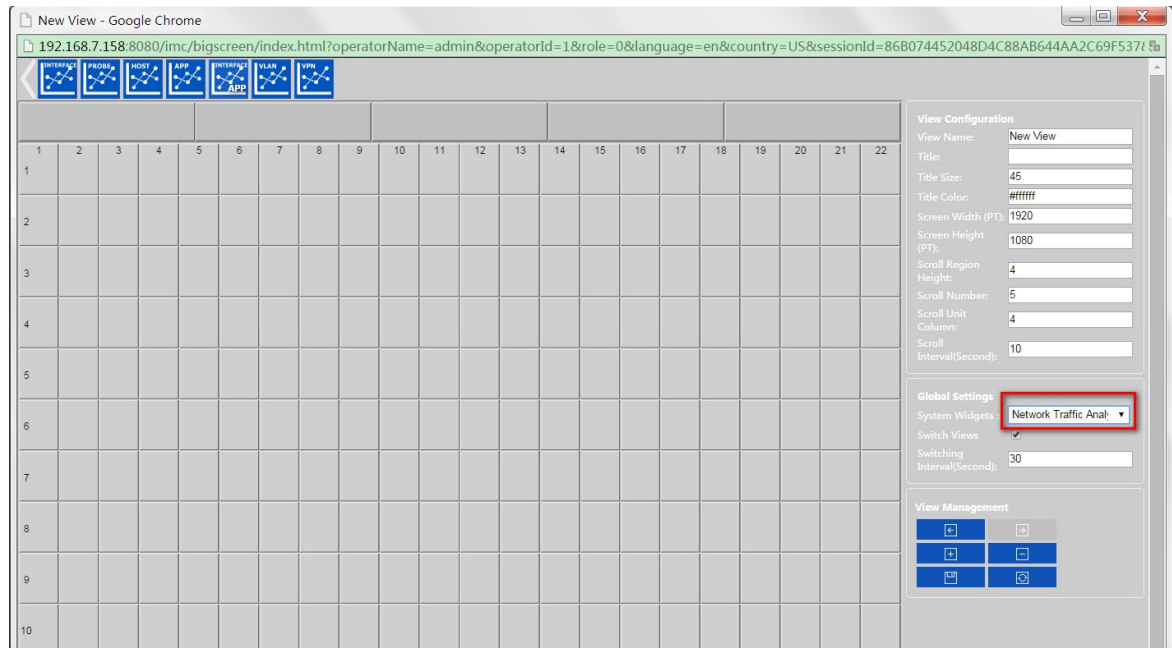
- Traffic Trend for Interface NTA Task (Last 1 Hour)
- Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)
- Traffic Trend for Probe NTA Task (Last 1 Hour)
- Traffic Trend for Application NTA Task (Last 1 Hour)
- Traffic Trend for Host NTA Task (Last 1 Hour)
- Traffic Trend for VPN NTA Task (Last 1 Hour)
- Application Traffic Trend for Interface NTA Task

To view widgets by using the dashboard widgets function, the administrator should configure the display content and layout of the dashboard widgets first.

# Configuring the dashboard display

1. Click the  icon in the top navigation bar.
2. Select **Dashboard > Configuration**.
3. In the **Global Settings** area of the right pane, select **Network Traffic Analyzer** from the **System Widgets** list.

Figure 271 Dashboard configuration page



4. Select a dashboard widget provided by NTA on the widget bar menu at the top of the page, and drag it to the configuration area.
5. Drag the display boxes of the widget to configure the layout of the page.
6. Right-click the widget in the configuration area. Click **Configure Parameters** in the shortcut menu.  
The **Configure Parameters** window opens.
7. Configure the parameters. Different widgets have different parameters. For more information, see "[Configuring dashboard widget parameters](#)."
8. Click **OK**.

## Configuring dashboard widget parameters

Each NTA dashboard widget has different parameters. The **Traffic Trend for Interface NTA Task (Last 1 Hour)**, **Traffic Trend for Host NTA Task (Last 1 Hour)**, and **Traffic Trend for VPN NTA Task (Last 1 Hour)** widgets have the same parameters. The **Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)**, **Traffic Trend for Probe NTA Task (Last 1 Hour)**, and **Traffic Trend for Application NTA Task (Last 1 Hour)** widgets have the same parameters.

Parameters for the **Traffic Trend for Interface/Host/VPN NTA Task (Last 1 Hour)** widget include:

- **Direction**—Specifies the direction of the traffic, and displays only statistics of the specified direction. Options are **In**, **Out**, and **Unlimited**.
- **Task**—Specifies the selected tasks, and displays only statistics about the selected tasks.

Parameters for the **Application Traffic Trend for Interface NTA Task** widget include:

- **Direction**—Specifies the direction of the traffic, and displays only statistics of the specified direction. Options are **In**, **Out**, and **Unlimited**.
- **TopN**—Displays statistics for the topN applications with the highest traffic volumes. Options are 3, 5, and 10.
- **Task**—Specifies the selected task, and displays only statistics about the selected task.

For the **Traffic Trend for VLAN/VXLAN/Probe/Application NTA Task (Last 1 Hour)** widget, you only need to select tasks and do not need to specify a direction.

For the **Traffic Trend for Probe NTA Task (Last 1 Hour)** and **Traffic Trend for Application NTA Task (Last 1 Hour)** widgets, the direction is ignored in the collection of statistics.

For the **Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)** widget, the direction is specified when the VLAN/VXLAN traffic analysis task is created.



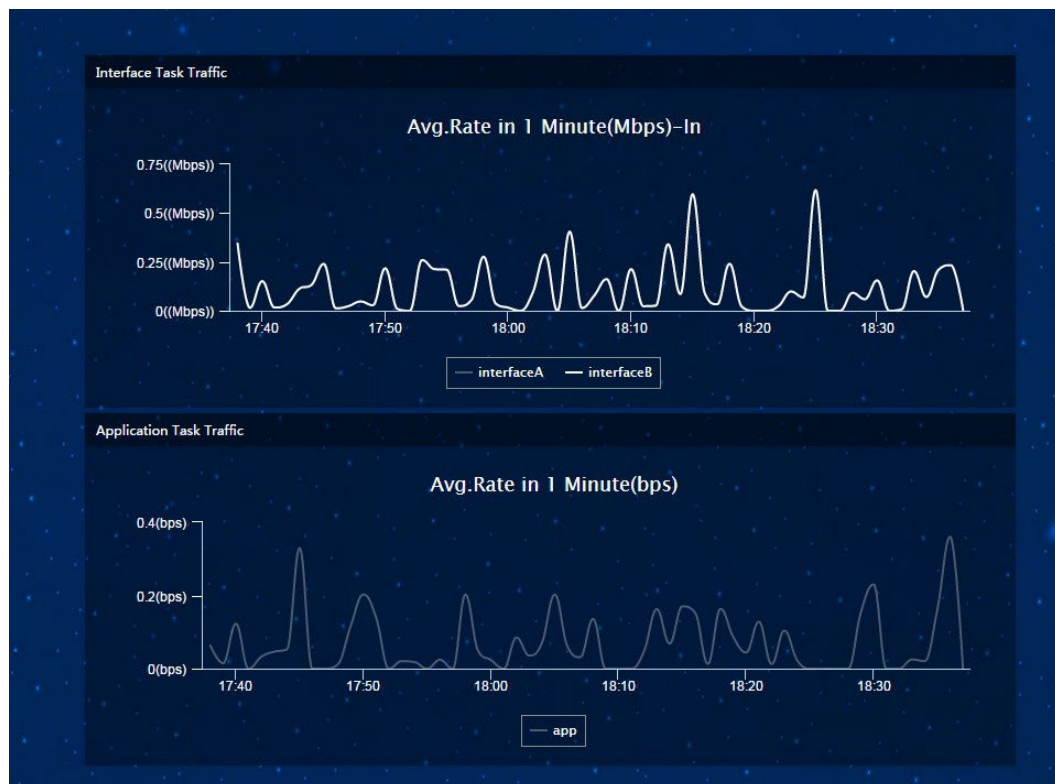
**TIP:**

For NTA widgets for which the direction needs to be specified, if you select **Not Limited**, the widget needs two curves to display information. Increase the height of the display area on the screen so you can see the curves clearly.

## Viewing the display effect

After completing the configuration, you can view the configuration effect by using the dashboard function. [Figure 272](#) shows the display effect of the **Traffic Trend for Interface NTA Task (Last 1 Hour)** and **Traffic Trend for Application NTA Task (Last 1 Hour)** widgets. Move the mouse pointer to the curves to see the specific values.

**Figure 272 Dashboard widgets display**



# Home page widgets

The home page widgets that NTA provide include:

- TopN Application for Interface NTA Task (Last 1 Hour)
- TopN Application for VLAN/VXLAN NTA Task (Last 1 Hour)
- TopN Application for Probe NTA Task (Last 1 Hour)
- TopN Application for Host NTA Task (Last 1 Hour)
- TopN Application for VPN NTA Task (Last 1 Hour)
- Traffic Trend for Interface NTA Task (Last 1 Hour)
- Traffic Trend for Probe NTA Task (Last 1 Hour)
- Traffic Trend for VLAN/VXLAN NTA Task (Last 1 Hour)
- Traffic Trend for Application NTA Task (Last 1 Hour)
- Traffic Trend for Host NTA Task (Last 1 Hour)
- Traffic Trend for VPN NTA Task (Last 1 Hour)
- Application Traffic for Host NTA Task (Last 1 Hour)
- TopN Session List (Last 1 Hour)

When using home page widgets, after choosing the layout scheme on the home page, the administrator can just add and configure NTA home page widgets without too many layout operations. For more information about customizing home page widgets,

## Configuring home page widget parameters

The parameters for different NTA home page widgets are not the same.

### TopN Application for Interface/VLAN/VXLAN/Probe/Host/VPN NTA Task (Last 1 Hour)

Move the mouse pointer to the title bar at the upper right of each widget. Click the **Setting** icon  in the popup menu. Click **Parameter Settings** in the menu to open the parameter configuration window.

For the TopN Application for Interface/VLAN/VXLAN/Probe/Host/VPN NTA Task (Last 1 Hour) widgets, the home page widget parameters that can be configured include:

- **Direction**—Specifies the direction of the traffic. Only statistics of the specified direction are displayed. Options are **In**, **Out**, and **Not Limited**.
- **Task**—Specifies the selected tasks. Only statistics about the selected tasks are displayed. Select the boxes next to the task names on the task list to select one or more tasks.

For the TopN Application for VLAN/VXLAN/Probe NTA Task (Last 1 Hour) widget, the direction does not need to be specified. After the configuration is completed, the INC home page displays the content that needs to be monitored in a pie chart.

### Traffic Trend for Interface/VLAN/VXLAN/Application/Probe/Host/VPN NTA Task (Last 1 Hour)

Move the mouse pointer to the title bar at the upper right of each widget. Click the **Setting** icon  in the popup menu. Click **Parameter Settings** in the menu to open the parameter configuration window.

For the Traffic Trend for Interface/VLAN/VXLAN/Application/Probe/Host/VPN NTA Task (Last 1 Hour) widgets, the home page widget parameters that can be configured include:

- **Direction**—Specifies the direction of the traffic. Only statistics of the specified direction are displayed. Options are **In**, **Out**, and **Not Limited**.
- **Task**—Specifies the selected tasks. Only statistics about the selected tasks are displayed. Select the boxes next to the task names on the task list to select one or more tasks.

For the TopN Application for VLAN/VXLAN/Probe/Application NTA Task (Last 1 Hour) widget, the direction does not need to be specified. After the configuration is completed, the INC home page displays the content that needs to be monitored in a line chart.

### Application Traffic for Host NTA Task (Last 1 Hour)

Move the mouse pointer to the title bar at the upper right of the **Application Traffic for Host NTA Task (Last 1 Hour)** widget. Click the **Setting** icon  in the popup menu. Click **Parameter Settings** in the menu to open the parameter configuration window.

Parameters that need to be configured include:

- **Direction**—Specifies the traffic direction in the host traffic analysis task. Only statistics of the specified direction are displayed. Options are **In**, **Out**, and **Not Limited**.
- **Application**—Specifies the applications in the host traffic analysis task. Only statistics of the specified applications are displayed. Click the plus sign (+) next to the application text box to display the **Query Applications** dialog box. To select applications:
  - a. Enter the complete or part of the application name in the **Application** text box.
  - b. Click **Search** to search for the application.
  - c. Select the boxes on the application list to select applications.
  - d. Click **OK**.

To remove a selected application, highlight the application name and click the minus sign (-).

- **NTA Task List**—Specifies the selected host traffic analysis tasks. Only statistics about the selected tasks are displayed. Select the boxes on the task list to select one or more.

After the configuration is completed, the INC home page displays the content that needs to be monitored in a list.

### TopN Session List (Last 1 Hour)

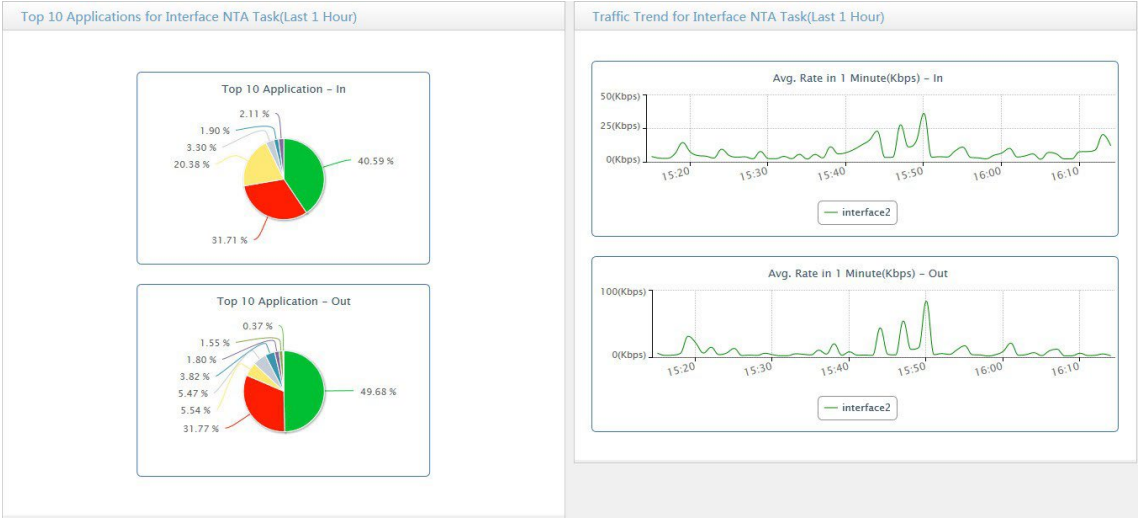
Move the mouse pointer to the title bar at the upper right of home page widgets of the **TopN Session List (Last 1 Hour)** widget. Click the **Setting** icon  in the popup menu. Click **Parameter Settings** in the menu to open the parameter configuration window.

- **Query Time**—Specifies the time range of the data that the widget displays.
- **Server**—Specifies a NTA server to count the number of host sessions.
- **Direction**—Specifies the direction in which the host sessions are counted. Options are **In**, **Out**, and **Not Limited**.
- **Top N**—Shows information about the TopN hosts by the number of sessions.

## Viewing the display effect

After the configuration is completed, the administrator can view the configuration effect on the customized home page. [Figure 273](#) shows the display effect of the **TopN Application for Interface NTA Task (Last 1 Hour)** and **Traffic Trend for Interface NTA Task (Last 1 Hour)** widgets.

Figure 273 Customized Home Page





# Analyzing traffic between virtual machines

Virtual machines running on the same physical server can provide different types of services to network users concurrently. Each virtual machine has a unique IP/MAC address, so all traffic passing through the devices can be captured by the device supporting NetStream v5/v9, NetFlow v5/v9, or sFlow v5, and sent to NTA for processing and analysis. However, because traffic between virtual machines is forwarded internally by the vSwitches of the physical server without passing through the devices, traffic cannot be captured and forwarded to NTA for processing and analysis.

To collect and analyze traffic between virtual machines, you create a virtual machine on the physical server and deploy a probe server on the virtual machine. This chapter describes how to deploy the probe server on a VMware virtual machine to collect and analyze traffic between virtual machines. By default, the probe server deployed on a VMware virtual machine does not receive traffic between virtual machines. To enable the probe server to capture traffic between virtual machines, you must modify the settings of the virtual machine's network adapter.

To use NTA to analyze traffic between VMware virtual machines:

1. Deploy a probe on the virtual machines.

In NTA, a probe is a probe server, which is an application that runs on a dedicated server. A probe server acts as a network flow generator that transmits network flow data to the NTA server that acts as a flow collector. Probe servers receive information forwarded to it from network devices. NTA retrieves data from probe servers when the probe server is added to the NTA server as a probe. Operators use probe servers when the devices in their network cannot generate NetStream, NetFlow, or sFlow data. For instructions on deploying a probe on virtual machines, see ["Deploying a probe on a virtual machine."](#)

2. Configure the virtual machine's network adapters.

A virtual machine with a probe deployed needs two network adapters, one for collecting data and the other for sending data to the NTA server. The two network adapters are added to different port groups. To enable the probe to collect and analyze traffic between virtual machines, you must add the network adapters to the correct port groups. By default, the probe deployed on a virtual machine cannot receive packets transmitted between virtual machines. You must configure the port group on which the network adapter for collecting traffic resides to operate in promiscuous mode; then, all virtual machine network adapters in the port group operate in promiscuous mode. A probe can capture data packets between virtual machines only when the network adapters operate in promiscuous mode. For instructions on how to modify the network configuration of a port group, see ["Setting the network configuration for a virtual machine network adapter."](#)

In promiscuous mode, a virtual machine network adapter listens to all packets. In non-promiscuous mode, it can listen only to traffic on its own MAC address. By default, virtual machine network adapters are in non-promiscuous mode.

3. Add the probe to NTA.

After you deploy a probe and modify port group configurations, you must configure the NTA server to receive and process the network flow records from the probe. Use the **Probe Management** feature in the **Settings** area to add probes to NTA. For more information on using **Probe Management** to configure NTA to receive network flow data records from probe servers, see ["Probe management."](#)

After a probe server has been added to an NTA server as a probe, and the probe has been selected on the **Server Management** page, the NTA server is ready to begin processing data from the probe server/probe. Probe traffic analysis tasks instruct NTA to begin processing probe server data based on the task configuration. For more information on selecting a probe in the NTA server configuration, see ["Managing NTA servers,"](#) specifically ["Modifying an NTA server configuration."](#)

4. Configure probe traffic analysis tasks.

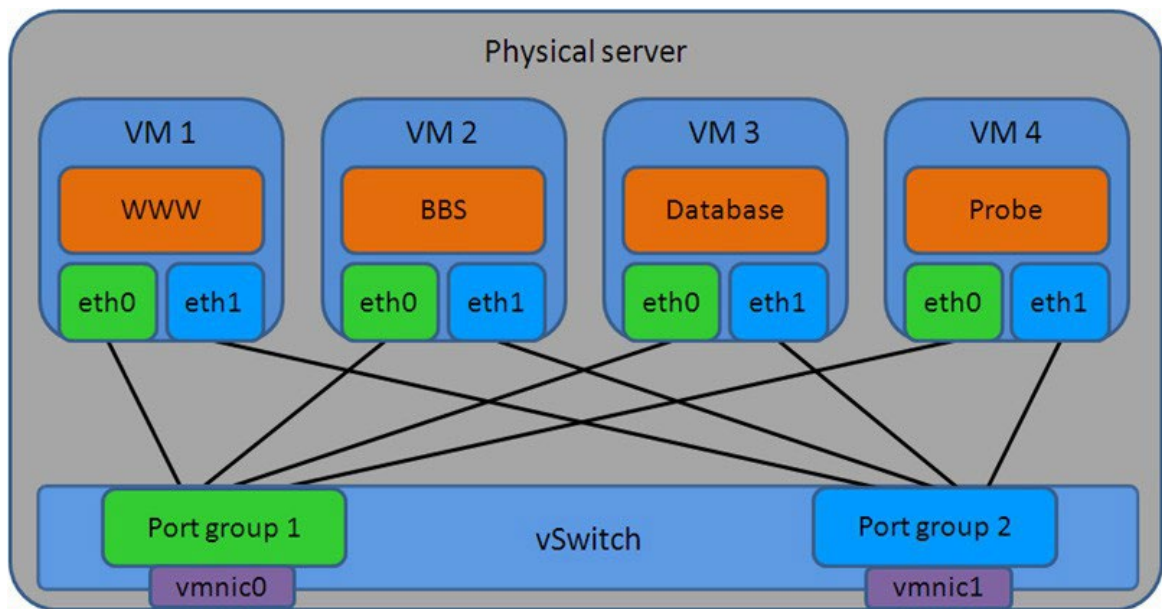
Probe traffic analysis tasks analyze network flow data for the probes you specify. NTA parses all network flow data and provides statistical views of traffic received by the probes configured in a probe traffic analysis task. For example, NTA provides source and destination host information reporting by probe, displaying traffic for source or destination hosts that sent or received traffic from the locations where the probes were deployed. For instructions on how to configure probe traffic analysis tasks, see ["Probe monitoring."](#)

## Deploying a probe on a virtual machine

The network shown in [Figure 274](#) provides four virtual machines: WWW, BBS, Database, and Probe. WWW and BBS are web servers, Database is a database server, and Probe is a probe server. Network adapter eth0 for virtual machines WWW, BBS, and Database provides external services and is added to port group 1. Network adapter eth1 is used for network management and is added to port group 2. Probe adds network adapter eth0 to port group 1 and network adapter eth1 to port group 2.

After you configure port group 1 to operate in promiscuous mode, network adapter eth0 for Probe can capture the network traffic transmitted between users and the WWW/BBS server, and can capture the network traffic transmitted between the WWW or BBS server and the database server. Probe can use network adapter eth1 to send the collected traffic to the NTA server.

**Figure 274 Deploying a probe on a virtual machine**



To deploy a probe on a virtual machine:

1. On a physical server, use the **New Virtual Machine** wizard to create virtual machines. The virtual machines must meet the hardware requirements in [Table 1](#) and the software requirements in [Table 2](#).

**Table 1 Server hardware requirements**

| Item | Requirements                                                                                                                                                                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU  | <p><b>Type:</b> Intel x86</p> <p><b>Frequency:</b> 3.0 GHz</p> <p><b>Number of processors:</b> 1 or 2</p> <p><b>NOTE:</b></p> <p>To process traffic lower than 300 Mb/s, use one single-core CPU. To process traffic</p> |

| Item                 | Requirements                                                         |
|----------------------|----------------------------------------------------------------------|
|                      | higher than 300 Mb/s, use two single-core CPUs or one dual-core CPU. |
| Memory               | 2 GB                                                                 |
| Hard disk drive      | 80 GB                                                                |
| Network adapter card | <b>Type:</b> Built-in Gigabit NIC<br><b>Number of cards:</b> 2       |

**Table 2 Server software requirements**

| Item             | Requirements                                                                                                                                                                                                                                                     |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating system | <ul style="list-style-type: none"> <li>Red Hat Enterprise Linux Server 5.0 (32-bit)</li> <li>Red Hat Enterprise Linux Server 5.5 (32-bit)</li> <li>Red Hat Enterprise Linux Server 6.1 (64-bit)</li> <li>Red Hat Enterprise Linux Server 6.4 (64-bit)</li> </ul> |

2. Install Linux operating system on the newly created virtual machine.
3. Install the probe program on the virtual machine with Linux installed.  
For instructions on how to install the probe,

## Setting the network configuration for a virtual machine network adapter

Setting the network configuration for a virtual machine network adapter involves the following tasks:

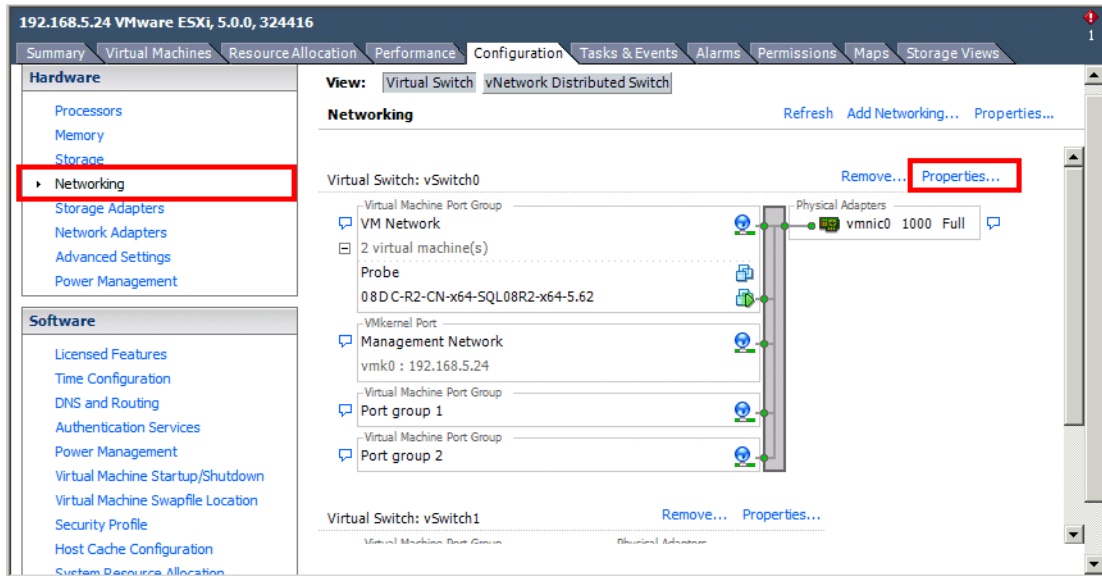
- Adding the virtual machine network adapter to the correct port group.
- Setting promiscuous mode for the port group on which the network adapter for collecting traffic for the probe resides.

[Figure 275](#) shows a network for deploying a probe on a virtual machine. You must add network adapter eth0 of Probe to port group 1, and add network adapter eth1 of Probe to port group 2. Port group 1 is a service network through which the web server and database server provide external services. Port group 2 is a network for managing all virtual servers. To enable the probe to collect all traffic in the network, configure port group 1 to operate in promiscuous mode.

To set the network configuration for a virtual machine network adapter:

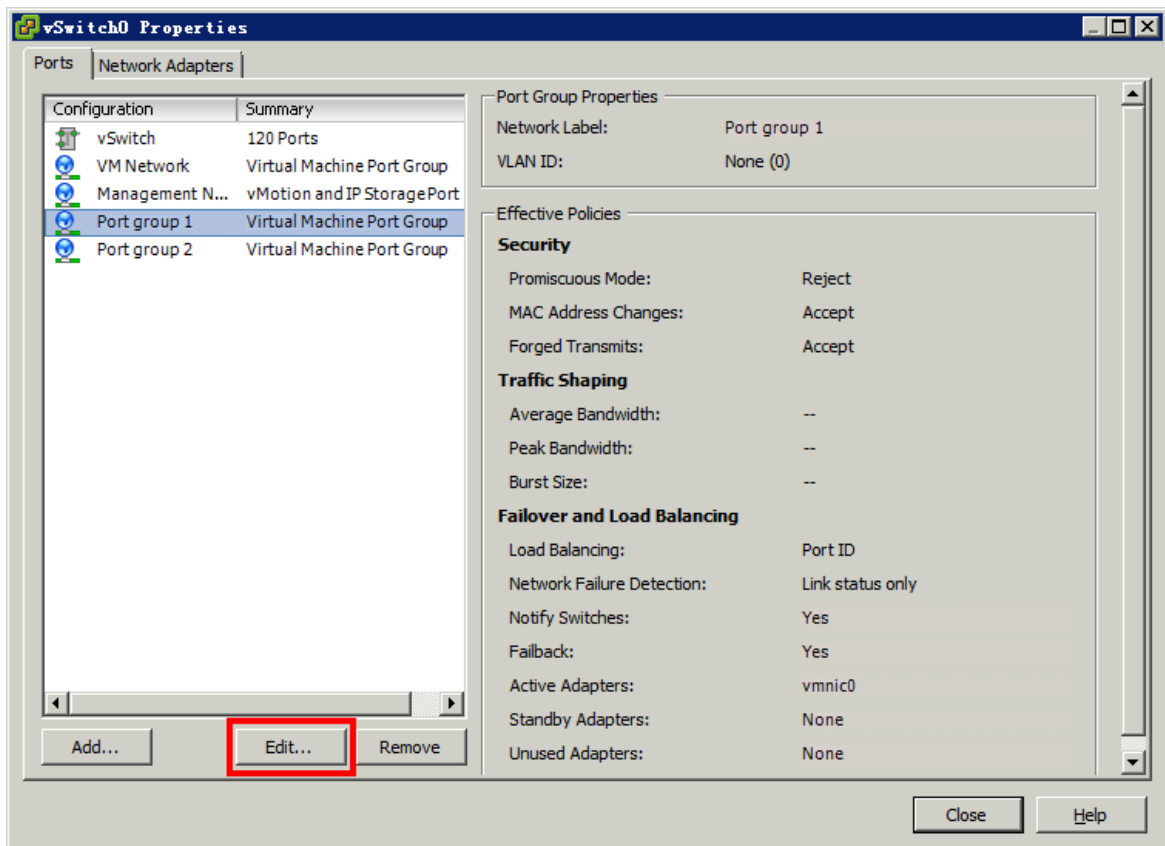
1. Log in to the **VMware vSphere Client**, and then select the host from the inventory panel.
2. Click the **Configuration** tab, and then click **Networking**, as shown in [Figure 275](#).
3. Find the vSwitch to edit and click **Properties** for that vSwitch.  
The **vSwitch Properties** dialog box opens.

Figure 275 Opening the vSwitch Properties dialog box



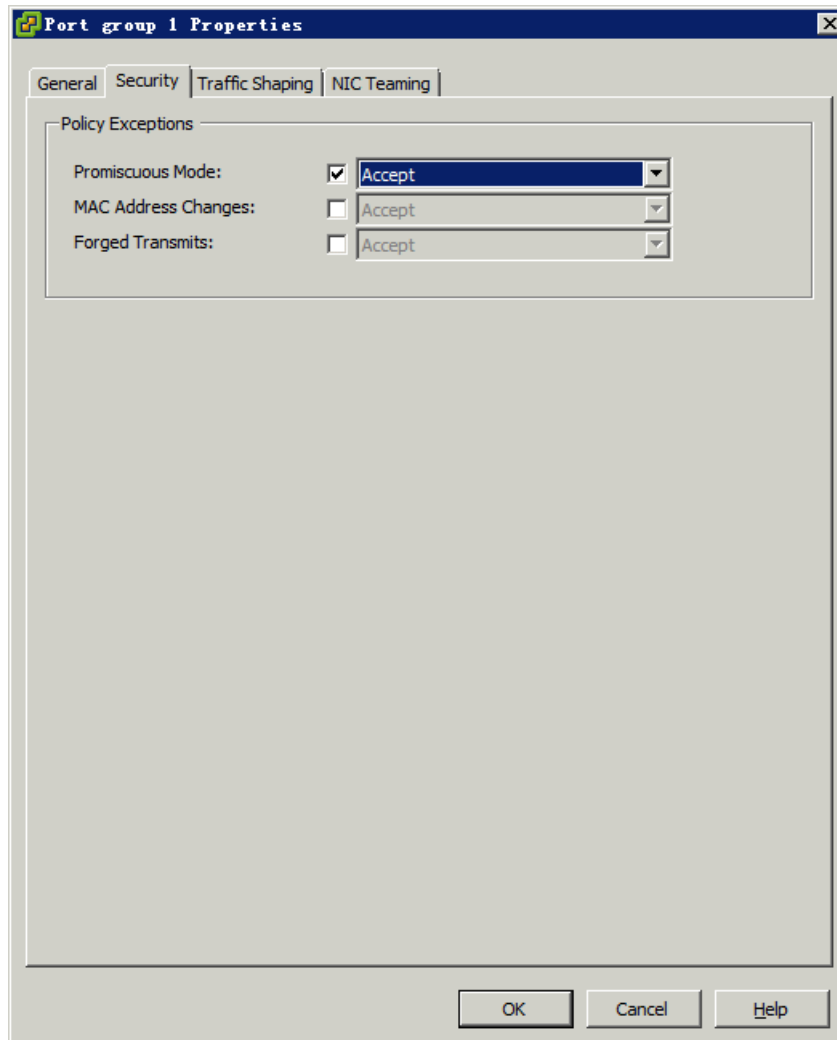
4. Click the **Ports** tab, as shown in Figure 276.
5. Select the port group 1 and click **Edit**. The port group properties dialog box opens.

Figure 276 vSwitch Properties dialog box



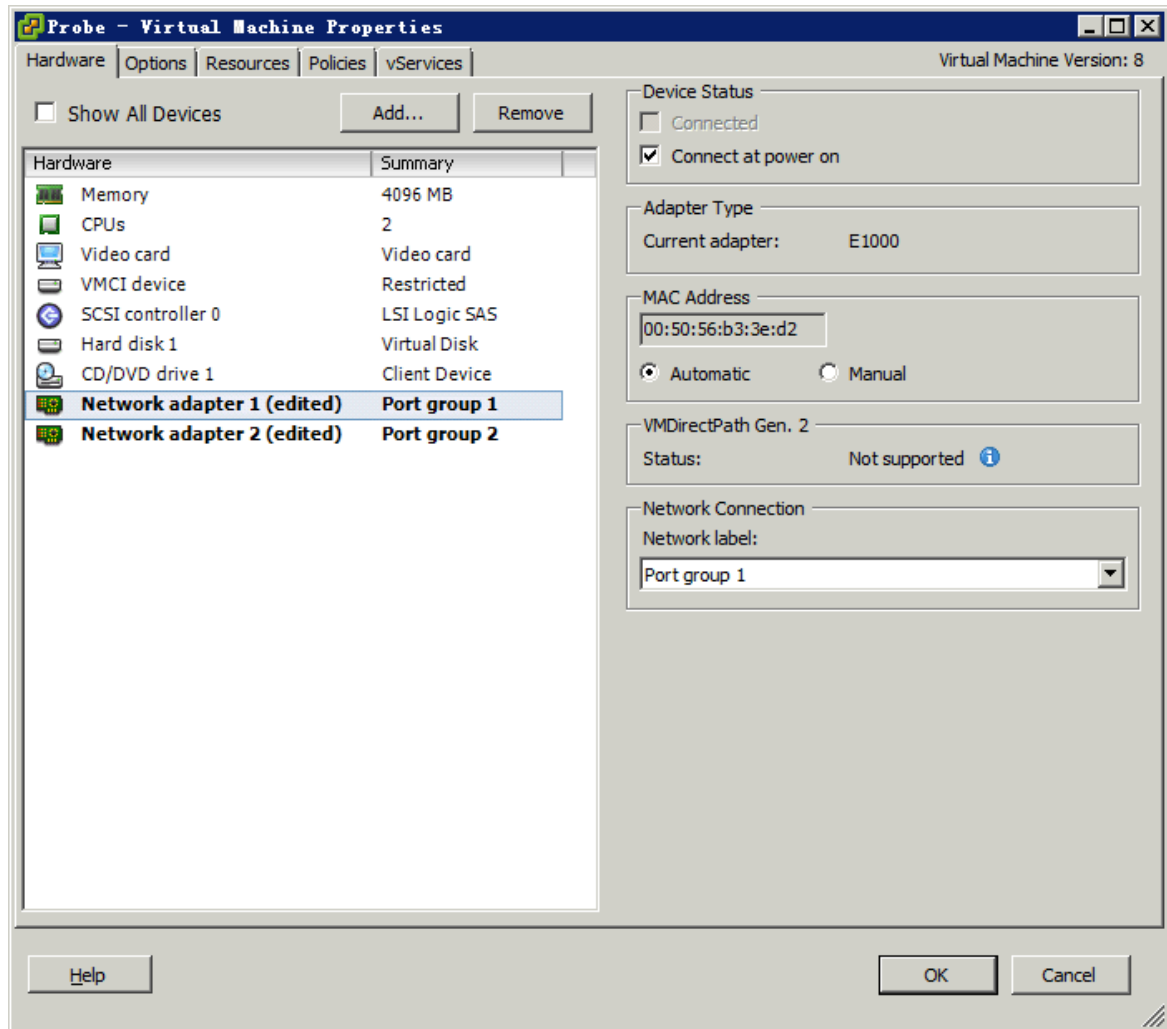
6. Click the **Security** tab in port group properties dialog box, as shown in Figure 277.
7. Click the box next to the **Promiscuous Mode** and select **Accept** from the list.

Figure 277 Port group properties dialog box



8. Click **OK**. All network adapters in port group 1 are configured to operate in promiscuous mode.
9. Select the virtual machine with the probe installed from the inventory panel and click **Edit Settings**. The **Virtual Machine Properties** dialog box opens.
10. Click the **Hardware** tab as shown in [Figure 278](#).
11. Click **Network adapter 1**, and then select **Port group 1** from the **Network label** list for Network adapter 1 (eth0).  
A port group is uniquely identified by the network label.
12. Click **Network adapter 2**, and then select **Port group 2** from the **Network label** list for Network adapter 2 (eth1).

**Figure 278 Setting a port group for a virtual machine network adapter**



**13.** Click **OK** to add virtual machine network adapters to correct port groups.