



Monitoring Data

The Monitor tab provides options for viewing various types of monitored data. There are options for:

- [Viewing the Monitor Overview Charts, page 4-9](#)
- [Viewing Application Data, page 4-12](#)
- [Viewing Voice Data, page 4-19](#)
- [Monitoring Hosts Data, page 4-30](#)
- [Viewing Conversations Data, page 4-42](#)
- [Viewing VLAN Data, page 4-53](#)



Note VLAN data is not available on NM-NAM devices.

- [Viewing DiffServ Data, page 4-62](#)
- [Monitoring Response Time Data, page 4-78](#)
- [Viewing Port/Interface Statistics Data, page 4-85](#)

Overview of Data Collection and Data Sources

All statistics and monitoring data produced by the NAM are generated by various types of *collections*. A collection operates on a stream of packets and produces output based on the input stream. In most cases, a collection corresponds directly to MIB tables such as RMON or SMON.

The [Collection Definitions](#) table (Table 4-1) defines the different collection types.

Table 4-1 Collection Definitions

Collection	Definition	Corresponds
Host	Examines a stream of packets; produces a table of all network addresses observed in those packets (also known as the collection data). Each entry records the total number of packets and bytes sent and received by that host and the number of non-unicast packets sent by that host.	RMON2 nlHostTable (the actual implementation of the collection).
Protocol	Examines a stream of packets; produces a table of all protocols observed in those packets. Each entry indicates the number of packets and bytes observed for that protocol.	RMON protocolDistStatsTable (the actual implementation of the collection).
Capture	Examines a stream of packets; produces a table of actual packet data (the captureBufferEntries). Each entry contains an exact copy of the data observed in the packet.	RMON1 bufferTable, filterTable, and channelTable variables.
Voice (proprietary)	Examines a stream of packets; produces tables of data for IP telephony-related protocols: <ul style="list-style-type: none"> All IP phones observed in the packet stream. Individual calls observed in the packet stream. Statistics (such as jitter and packet loss) for each phone and call entry are recorded. The worst-quality calls that were observed (determined by several characteristics). 	—

The stream of packets on which a collection operates is called the *collection data source*. It might be different for each collection. The data produced by a collection is called the *collection data*.

**Note**

The collection data is usually in the form of SNMP tables (except in voice collections).

The NAM can support simultaneous combinations of different collections, each operating on different collection data sources.

- The number of potential simultaneous collections is limited only by CPU and memory resources.
- The collection data sources are limited by the SPAN sources. For more information on SPAN sources, see the [“Setting Up Data Sources” section on page 3-3](#).

Configuring Multiple Collections

You can configure multiple collections (such as host, conversation, protocol, ART, and voice) simultaneously on the NAM. Collections are always configured on separate data sources.

Associated with each collection is a specific collection data source that might or might not correspond directly with the SPAN/VACL traffic stream that was configured. Examples of collection data sources include:

- All packets in the SPAN/VACL traffic stream regardless of the port/VLAN or origin (ALL SPAN).
- All packets in the SPAN/VACL traffic stream on a specific VLAN (VLAN x).
- All packets in the SPAN/VACL traffic stream that were configured to arrive on a specific NAM data port (DATA PORT 1 or DATA PORT 2).

**Note**

These data sources are available only on the WS-SVC-NAM-2 model.

- NetFlow Data Export (NDE) records received by the NAM from either the local Supervisor engine module or other remote NDE sources (such as remote routers).

Individual collection instances process only those packets in the traffic streams that correspond to their configured data sources. For example, a host collection configured with a data source of VLAN 12 will not be populated with any received NDE flow records. Nor will it be populated with packets in the SPAN/VACL traffic stream that are not tagged for VLAN 12.

Similarly, a conversation collection configured with a data source specifying NDE records from a remote router will not be populated with any packets arriving in the SPAN/VACL traffic stream.

Scenario

You configured the SPAN/VACL traffic stream source to include VLANs 1, 2, and 3. You now want to start an application collection that counts the packets and bytes monitored for each application protocol.

You must specify a collection data source for this collection. The data source could be VLAN 1, VLAN 2, or VLAN 3, or any combination of the three.

If you configure the data source as VLAN 2, the collection generates statistics for those packets received on VLAN 2. However, if you were to specify VLAN 10 as the collection data source, even if VLAN 10 were a valid VLAN ID, the collection would never get populated with data because VLAN 10 was not configured as part of the SPAN/VACL traffic stream.



Note

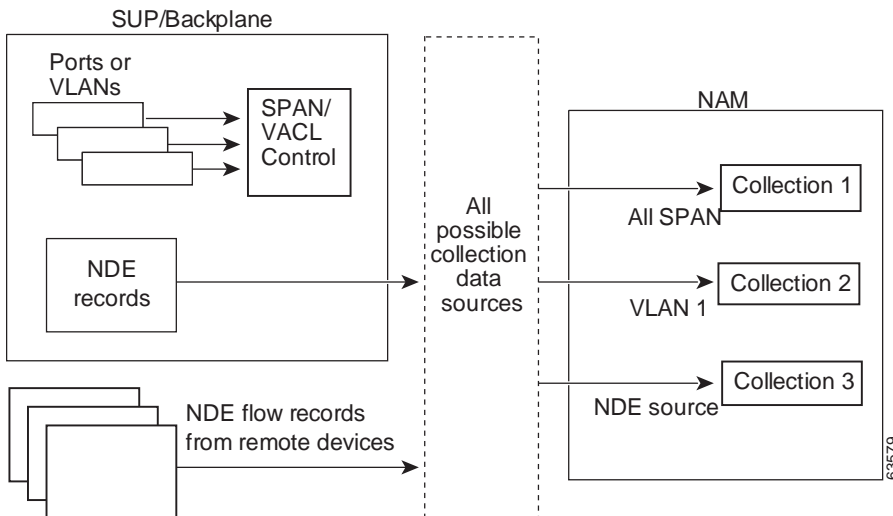
The SPAN/VACL traffic stream represents the aggregate sum of all traffic being sent to the NAM for monitoring as a result of SPAN or VACL configuration on the local Supervisor engine module. In addition to the SPAN/VACL traffic stream, one or more NDE traffic streams might be received from the local Supervisor engine module or remote switches and routers. The data source configured for a specific collection instance must correspond to traffic that appears on one of these traffic streams, or else the collection statistics will not get populated.

Each possible collection data source is represented as an ifEntry in the NAM ifTable (MIB-II). The [Data Collection Sources](#) table ([Table 4-2](#)) describes the valid collection data sources.

Table 4-2 Data Collection Sources

Collection Data Source	Limitations
All SPAN (aggregate SPAN/VACL traffic stream)	If no SPAN or VACL traffic sources are configured, the collection is not populated with data.
Specific VLAN ID	If the VLAN was not configured as part of the SPAN/VACL traffic stream, the collection is not populated with data.
NDE data source	The export parameters must be configured on the device that will export the records to the NAM; otherwise, the collection is not populated with data. Monitoring is limited to a subset of NAM collection types.

The [SPAN, VACL, NDE Traffic Streams and Collection Data Sources](#) illustration (Figure 4-1) shows the relationships between SPAN and NDE data sources and collection data sources.

Figure 4-1 SPAN, VACL, NDE Traffic Streams and Collection Data Sources

You can view real-time data from collections that were configured on the NAM. For more information on setting up collections on the NAM, see the [“Configuring Capture Settings”](#) section on page 6-2.

Protocol Auto Discovery

Traffic Analyzer can automatically discover up to 100 unknown protocols. The protocols are displayed according to the parent type and an identifier.

The [Auto-Discovered Protocol Types](#) table ([Table 4-3](#)) lists the type of protocols that can be automatically discovered and how they are displayed.

Table 4-3 Auto-Discovered Protocol Types

Protocol Type	Displays As...
Ether2	<i>ether2-ether-type number</i>
SNAP	<i>snap-ether-type number</i>
IP	<i>ip-protocol type number</i>
TCP	<i>tcp-port number</i>
UDP	<i>udp-port number</i>
SUNRPC	<i>sunrpc-program number</i>



Note

The automatically discovered protocols are not saved in NVRAM and are lost when the NAM is rebooted. To save an auto-discovered protocol, you can enter it manually into the Protocol Directory. For more information, see the [“Creating a Protocol”](#) section on page 3-39.

You can also clear the auto-discovered protocols without rebooting by entering the command `no monitor protocol auto-learned` in the NAM CLI.

NDE Flow Masks and V8 Aggregation Caches

Depending on the flow mask or aggregation configured at the device, some data fields might not be available in the NDE data structure. As a result, some windows will not display data for a NetFlow data source or will display specific conditions. The [Flow Mask and Aggregation Window Conditions](#) table ([Table 4-4](#)) lists the display conditions for the windows under the Monitor tab and the flow-mask or aggregation that causes them.

Table 4-4 Flow Mask and Aggregation Window Conditions

Flow Mask or Aggregation Cache	Window Conditions
Full flow mask	Supported in all windows.
Destination only flow mask	<ul style="list-style-type: none"> • Monitor>Apps displays “Others” only, and the detail pop-up window does not have data. • Monitor>Hosts displays 0.0.0.0 and the detail pop-up window does not have data. • Monitor>Conversations displays 0.0.0.0 for some hosts and the detail pop-up window does not have data.
Destination-Source flow mask	<ul style="list-style-type: none"> • Monitor>Apps displays “Others” only, and the detail pop-up window does not have data. • Monitor>Hosts has data, but the detail pop-up window does not. • Monitor>Conversations has data, but the detail pop-up window does not.
V8-Protocol-Port-Aggregation	<ul style="list-style-type: none"> • Monitor>Apps has data, and the detail pop-up window displays 0.0.0.0 only. • Monitor>Host displays 0.0.0.0 only. • Monitor>Conversations displays 0.0.0.0 to 0.0.0.0 only. • There is no data for custom NetFlow data sources that are set up for specific interfaces. • There is no DiffServ except TOS 0 and DSCP 0. • Setup>Data Sources>NetFlow Listening Mode detail pop-up window does not have interfaces information.

Table 4-4 Flow Mask and Aggregation Window Conditions (continued)

Flow Mask or Aggregation Cache	Window Conditions
V8-Destination-Prefix-Aggregation	<ul style="list-style-type: none"> • Monitor>Apps displays “Others” only. • Monitor>Host displays data with subnets and 0.0.0.0. The detail pop-up window does not have data. • Monitor>Conversations displays data with 0.0.0.0 to subnets, and 0.0.0.0 to 0.0.0.0. The detail pop-up window does not have data. • There is no DiffServ except TOS 0 and DSCP 0. • There is support for NetFlow custom data sources that are set up for specific interfaces.
V8-Prefix-Aggregation	<ul style="list-style-type: none"> • Monitor>Apps displays “Others” only. • Monitor>Host displays data with subnets and 0.0.0.0. The detail pop-up window does not have data. • Monitor>Conversations displays data and 0.0.0.0 to 0.0.0.0. The detail pop-up window does not have data. • There is no DiffServ except TOS 0 and DSCP 0. • There is support for NetFlow custom data sources that are set up for specific interfaces.
V8-Source-Prefix-Aggregation	<ul style="list-style-type: none"> • Monitor>Apps displays “Others” only. • Monitor>Host displays data with subnets and 0.0.0.0. The detail pop-up window does not have data. • Monitor>Conversations displays data with subnets to 0.0.0.0, and 0.0.0.0 to 0.0.0.0. The detail pop-up window does not have data. • There is no DiffServ except TOS 0 and DSCP 0. • There is support for NetFlow custom data sources that are set up for specific interfaces.
V8-AS-Aggregation	Not supported.

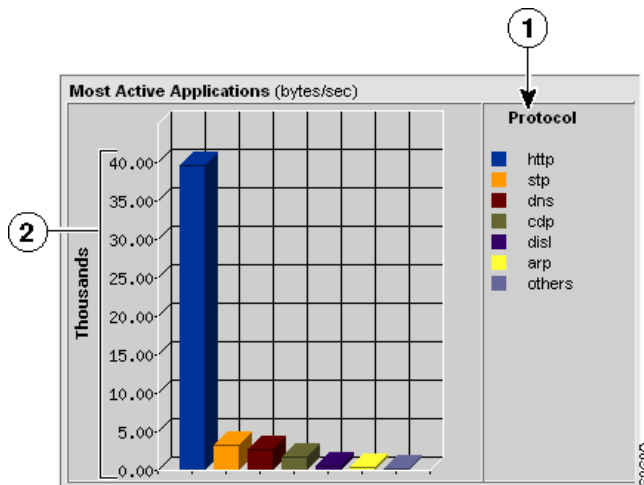
Viewing the Monitor Overview Charts

The Monitor Overview charts allow you to take a quick look, in graphical format, at the TopN protocol suites, active hosts, active applications, and application response times monitored on your network. To view the Monitor Overview charts, click the Monitor tab.

The following charts are displayed:

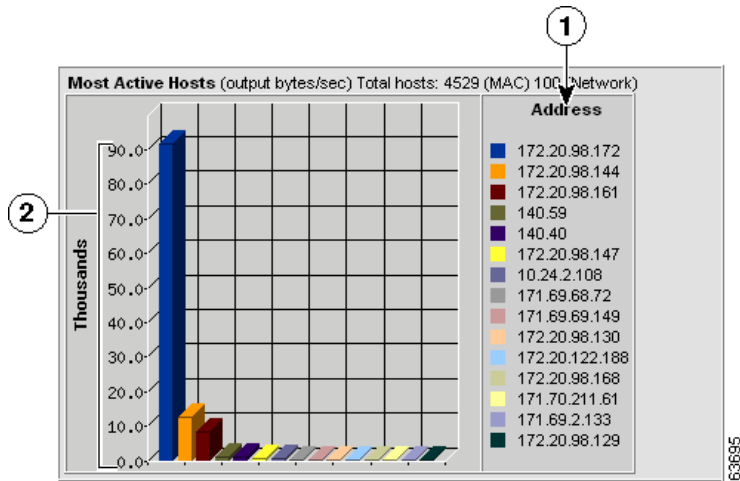
- [Most Active Applications Chart](#) (Figure 4-2)
- [Most Active Hosts Chart](#) (Figure 4-3)
- [Server Response Times Chart](#) (Figure 4-4)
- [Protocol Suites Chart](#) (Figure 4-5)

Figure 4-2 *Most Active Applications Chart*



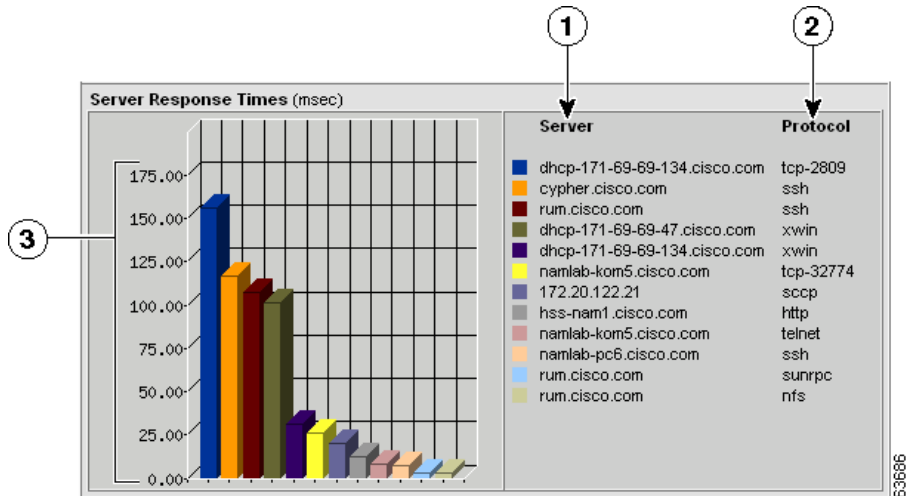
1	Top N protocols sorted by color.	2	Number of bytes collected per second for each protocol.
----------	----------------------------------	----------	---

Figure 4-3 Most Active Hosts Chart



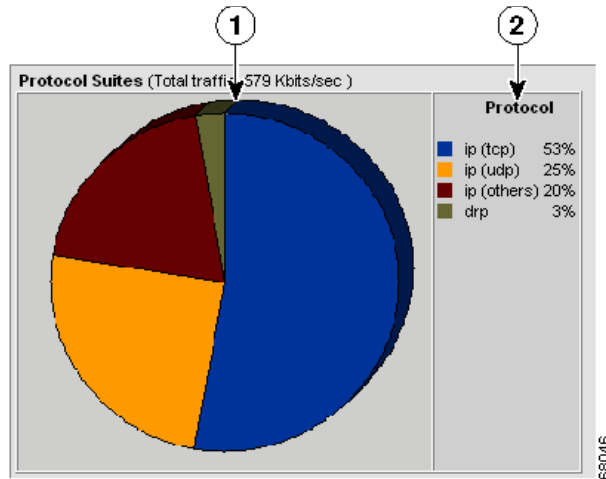
1 Top N network addresses sorted by color.	2 Number of bytes collected per second for each address.
--	--

Figure 4-4 Server Response Times Chart



1	Top N servers sorted by color.	3	Server response time.
2	Protocol used by the server.		

Figure 4-5 Protocol Suites Chart



1	Pie chart showing network protocol usage.	2	Top N network protocols.
---	---	---	--------------------------

Viewing Application Data

To view the distribution of packets and bytes based on the application protocol, click the Monitor tab, then click **Apps**. The Applications table is displayed with three radio buttons on top.

You can select a radio button for:

- [Viewing the Applications Current Rates Table, page 4-13](#)
- [Viewing the Top N Applications Chart, page 4-16](#)
- [Viewing the Applications Cumulative Data Table, page 4-17](#)

Viewing the Applications Current Rates Table

The Applications Current Rates table allows you to view the number of packets and bytes collected for each application protocol. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.



Note

Auto learned or user defined protocols are not listed in the table.

Step 1 Click the Current Rates table radio button.

The [Applications Current Rates Table](#) (Table 4-5) is displayed.

Table 4-5 Applications Current Rates Table

Field	Description
Protocol	Name of the application protocol.
Packets/s	Number of packets collected per second.
Bytes/s	Number of bytes collected per second.

Step 2 Select the data source to monitor from the Data Source list.

Step 3 To view data for a specific protocol, enter the protocol name in the Protocol text box, then click **Filter**.

Any matching protocols are displayed.



Tip

To view the full protocol name, move the cursor over the protocol name in the Protocol column of the Protocol Directory table.



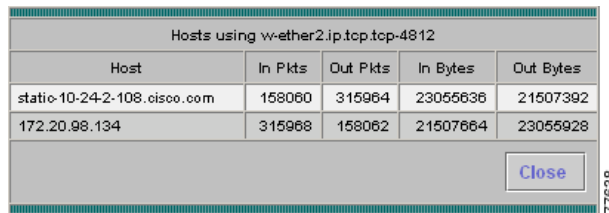
Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Displaying Details from the Applications Table

To view details for a specific application protocol, select the protocol and click Details, or click on the protocol name in the Protocol column. The [Application Protocol Detail Window](#) (Figure 4-6) is displayed, showing all network hosts using this protocol. The displayed data is specific to the selected data source.

Figure 4-6 Application Protocol Detail Window



Hosts using w-ether2.ip.tcp.tcp-4812				
Host	In Pkts	Out Pkts	In Bytes	Out Bytes
static-10-24-2-108.cisco.com	158060	315964	23055636	21507392
172.20.98.134	315968	158062	21507664	23055928

The Applications Protocol Detail Window displays the following information.

Table 4-6 Application Protocol Detail Table

Field	Description
Description	Full name and description of the protocol.
Host	The hostname of the computer using the application protocol.
In Pkts	Number of packets the host received for the specified protocol.
Out Pkts	Number of packets the host transmitted for the specified protocol.
In Bytes	Number of bytes the host received for the specified protocol.
Out Bytes	Number of bytes the host transmitted for the specified protocol.

Capturing Application Protocol Data from the Application Table

You can capture data for a specific application protocol directly from the Application table.

Select the protocol from the table, then click **Capture**. The Packet Browser is displayed. For more information on viewing packets using the Packet Browser, see the “[Viewing Protocol Decode Information](#)” section on page 6-12.

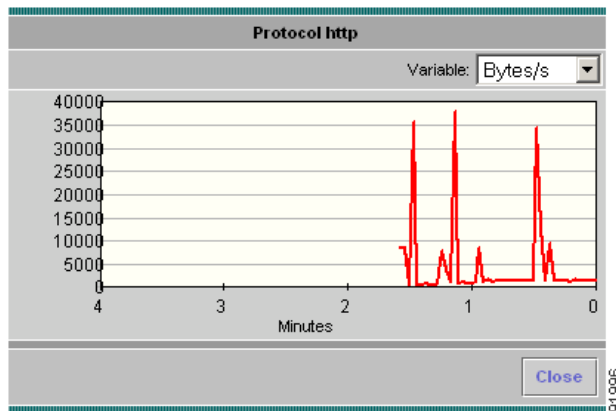
If a capture is already running, a message window is displayed. Click **Yes** to stop the current capture or **No** to disregard your selection.

Viewing Real-Time Data from the Application Table

You can view real-time data in a graphical format for a specific application protocol.

Select the protocol from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-7](#)) is displayed.

Figure 4-7 Real-Time Graph



Viewing Reports from the Applications Table

You can view reports directly from the Applications table. Select the application protocol for which to view a report, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, one will be created based on the selected application and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

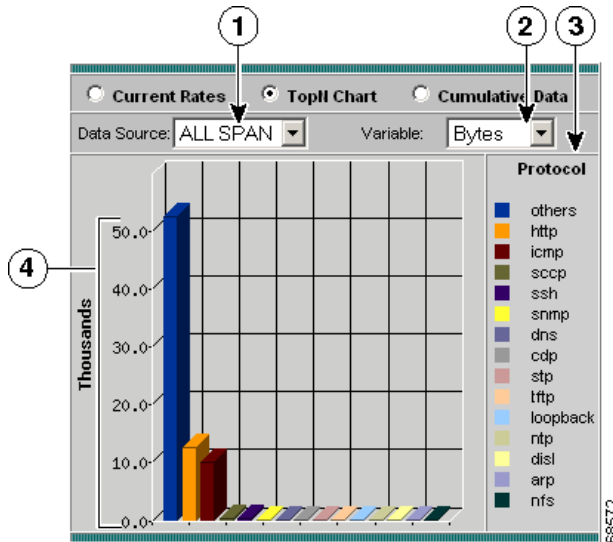
Viewing the Top N Applications Chart

The TopN Applications Chart allows you to view the number of packets and bytes collected for the Top N application protocols in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 Click the TopN Chart radio button.

The [TopN Applications Chart](#) (Figure 4-8) is displayed.

Figure 4-8 TopN Applications Chart



1	Data Source list.	3	Top N application protocols.
2	Variable list.	4	Number of bytes or packets collected per second on each Top N protocol.

- Step 2** Select the data source to monitor from the Data Source list.
- Step 3** Select one of the following from the Variable list:
- Packets—Displays the number of packets per second monitored.
 - Bytes—Displays the number of bytes per second monitored.

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To view the full protocol name, move the cursor over the protocol name.

Viewing the Applications Cumulative Data Table

The Applications Cumulative Data Table allows you to view the number of packets and bytes collected for each application protocol. The data displayed is the total number of packets and bytes collected since the collection was created or since the NAM was restarted.

- Step 1** Click the Cumulative Data radio button.

The [Applications Cumulative Data Table](#) (Table 4-7) is displayed.

Table 4-7 Applications Cumulative Data Table

Field	Description
Protocol Name	Name of the monitored protocol.
Packets	Total number of packets collected over the last time interval.
Bytes	Total number of bytes collected over the last time interval.

- Step 2** Select the data source to be monitored from the Data Source list.

- Step 3** To refresh the table, click **Refresh**.
- Step 4** To view data for a specific protocol, enter the protocol name in the Protocol text box, then click **Filter**.
- Any matching protocols are displayed.



Tip

To view the full encapsulated protocol name, move the cursor over the protocol name in the Protocol column of the Protocol Directory table.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Displaying Details from the Applications Table

To view details for a specific application protocol, click on the protocol name in the Protocol column. The Protocol Detail Window (Figure 4-9) is displayed.

Figure 4-9 Protocol Detail Window

Hosts using w-ether2.ip.tcp.tcp-4812				
Host	In Pkts	Out Pkts	In Bytes	Out Bytes
static-10-24-2-108.cisco.com	158060	315964	23055636	21507392
172.20.98.134	315968	168062	21507664	23055928

The Protocol Detail Window displays the following information:

Table 4-8 Protocol Detail Table

Field	Description
Host	The hostname of the computer using the application protocol.
In Pkts	Number of packets the host received for the specified protocol.

Table 4-8 Protocol Detail Table (continued)

Field	Description
Out Pkts	Number of packets the host transmitted for the specified protocol.
In Bytes	Number of bytes the host received for the specified protocol.
Out Bytes	Number of bytes the host transmitted for the specified protocol.

Viewing Voice Data

You can use the NAM Traffic Analyzer to view troubleshooting data collected from any enabled voice protocols on the NAM. This allows you to identify potential problems with your voice network.

There are menu items for:

- [Viewing the Voice Protocol Overview, page 4-19](#)
- [Viewing Known Phones, page 4-21](#)
- [Viewing Active Calls, page 4-28](#)

Viewing the Voice Protocol Overview

The Aggregate Statistics table contains basic troubleshooting information for the voice protocols implemented in your network.

Step 1 Click the Monitor tab.

Step 2 Click **Voice**.

The [Aggregate Statistics Table \(Table 4-9\)](#) is displayed.

Table 4-9 Aggregate Statistics Table

Field	Description
Protocol	Name of the voice protocol.
Calls Monitored	Number of calls monitored.
Avg Pkt Loss (%)	Average packet loss for all calls.
Avg Jitter (ms)	Average jitter for all calls.
Worst Pkt Loss (%)	Worst packet loss percentage monitored.
Worst Jitter (ms)	Worst jitter monitored.

Displaying Protocol Details From the Aggregate Statistics Table

To view the voice protocol details window, select the radio button of the protocol name and click **Details**, or click the protocol name.

The [Worst Quality Calls Tables](#) (Table 4-10) are displayed:

- Packet Loss - Worst Quality Calls Table—Displays the TopN worst calls based on packet loss.
- Jitter - Worst Quality Calls Table—Displays the TopN worst calls based on jitter

To clear the information in the tables, click **Clear**.

Table 4-10 Worst Quality Calls Tables

Field	Description
Caller Number	Number of the caller phone.
Called Number	Number of the called phone.
Caller	Alias name or MGCP endpoint ID of the calling party phone.
Called	Alias name or MGCP endpoint ID of the called party phone.

Table 4-10 Worst Quality Calls Tables (continued)

Field	Description
Time of Call	Time the call was placed.
Caller IP Address	IP address of the caller.
Called IP Address	IP address of the called phone.
% Packet Loss	Percentage of packets lost on the call.
Jitter	Amount of jitter on the call.

Viewing Known Phones

You can view basic and detailed information on all known monitored phones in your network.

If you are using MGCP gateways in your network, the MGCP endpoint and endpoint IDs represent the ports of the MGCP gateway that are used to establish connections with the specified call.

-
- Step 1** Click the Monitor tab.
- Step 2** Click **Voice**.
The Aggregate Statistics table is displayed.
- Step 3** In the contents, click **Known Phones**.
The [Phones Table](#) (Table 4-11) is displayed.

Table 4-11 Phones Table

Field	Description
Phone	Phone number or MGCP endpoint.
IP Address	IP address of the phone.
Name	Alias name or MGCP endpoint ID of the phone.
Calls Monitored	Number of calls monitored and percentage of total calls.
Avg Pkt Loss %	Average packets loss on the phone.
Avg Jitter	Average jitter on the phone (in milliseconds).

- Step 4** Select the protocol variable to filter from the list.
- Step 5** Enter the variable to filter in the text box, then click **Filter**.
The specified variable is displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.

Displaying Phone Details From the Known Phones Table

To view details for a specific phone, click on the phone number in the Phone column of the Phones table. The [Phone Details](#), [Aggregate Statistics](#), and [Last N Calls](#) tables ([Table 4-12](#) through [Table 4-14](#)) are displayed.

Table 4-12 Phone Details

Field	Description
Phone	Phone number.
Name	The alias name or MGCP endpoint ID of the phone.
IP Address	IP address of the phone.
Switch Port	Physical interface switch port that the phone is attached to.
Protocol	The protocol that the phone is learned from.

Table 4-13 Aggregate Statistics

Field	Description
Calls Monitored	Number of calls monitored since Call Monitoring was last enabled.
Average Packet Loss (%)	Average percent packet loss over all monitored calls.
Average Jitter (msec)	Average jitter over all monitored calls.

Table 4-13 Aggregate Statistics (continued)

Field	Description
Worst Packet Loss (%)	Worst percent packet loss from all monitored calls.
Worst Jitter (msec)	Worse amount of jitter from all monitored calls.

Table 4-14 Last N Calls

Field	Description
Caller Number	Phone number of the caller.
Called Number	Phone number of the called phone.
Caller	Alias name or MGCP endpoint ID of the calling party.
Called	Alias name or MGCP endpoint ID of the called party.
Time of Call	Time the call was established.
Caller IP Address	IP address of the connected caller.
Called IP Address	IP address of the called party.
% Pkt Loss	Percentage of packets lost on the call.
Jitter (msec)	Jitter on the call. For SCCP, the jitter value is reported by the phone. For H.323, it is the average inter-arrival jitter calculated as the sum of all detected RTCP receiver reports inter-arrival jitter, divided by the number of detected RTCP receiver reports.

Displaying Call Details From the Last N Calls Table

To view the details of a specific call from the Last N Calls Table, select the radio button, then click **Details**.

For phones using SCCP, the [SCCP Call Detail Table \(Table 4-15\)](#) is displayed.

For phones using H.323, the [H.323 Call Detail Table \(Table 4-16\)](#) is displayed.

For phones using MGCP, the [MGCP Call Detail Table \(Table 4-17\)](#) is displayed.



Note The title of the SCCP Call Detail Table shows whether the data is collected from the calling or called party.

Table 4-15 *SCCP Call Detail Table*

Field	Description
Number	Phone numbers of the calling and called parties.
IP Address	IP addresses of the calling and called parties.
Call Reference	The call reference field in the call setup messages.
Owner	Alias name of the calling and called party phones.
Call State	Current state of the call—setup, hold, connect, or ended.
RTP Port	Port that the phone is listening on for the call.
Line Instance	Line of the call (line 1, line 2, etc.).
Conference ID	The conference field in the call setup messages.
Pass Thru Party ID	Internal field used by Call Manager to correlate call set-up messages.
RTP Sampling Period	Period (in msec) at which an RTP frame is sampled for transmission.
Payload Type	The codec of the RTP stream.
RTP Pre Value	Initial sequence-number value of the RTP stream.
Silence Sup	Indicates whether silence suppression is on or off.
Max Frames per Pkt	The maximum number of RTP frames in an RTP packet.
G.723 Bit Rate	Bit rate in kilobits per second for G.723 payload types (codec).
Start Time	Day, date, and time the call was started.
End Time	Day, date, and time the call was ended.
Packets Sent	Number of packets sent during the call.
Packets Received	Number of packets received during the call.
Octets Sent	Number of octets sent during the call.
Octets Received	Number of octets received during the call.
Packet Loss (%)	Percentage of packets lost during the call.

Table 4-15 SCCP Call Detail Table (continued)

Field	Description
Jitter (msec)	Amount of jitter monitored during the call.
Switch Port	Physical interface switch port that the phone is attached to.

Table 4-16 H.323 Call Detail Table

Field	Description
Number	Phone numbers of the calling and called parties.
Q.931 IP Address	For the calling party, the source IP address of the Q.931 setup message. For the called party, the source IP address of the Q.931 connect message.
Q.931 Port	Port that the phone is using to send Q.931 messages.
Alias	Alias name of the calling and called phones.
Call State	State of the call—setup, connect, or ended.
Call Status	Good—Jitter and/or packet loss do not pass threshold values. Acceptable—Jitter and/or packet loss pass threshold values but are within 10% of exceeding the values. Bad—Jitter and/or packet loss exceed the threshold values by more than 10%.
Call Reference	The call reference field in the call setup messages.
Call Id	The call ID field in the call setup messages.
Conference Id	The conference ID field in the call setup messages.
Conference Goal	The conference action of the caller—Create, Invite, or Join.
Fast Start	True or false. Indicates if the call used faststart sequence to set-up the call.
Tunneling	True or false. Indicates if the call used tunneling to set-up the medium (RTP) channel.
Call Type	The type of call—Point-to-Point, N-to-One, or One-to-N.
Product Id	The product string in the call setup message for the calling and called parties.
Version Id	The version of the product for the calling and called parties.
Session Id	The session number of the media (RTP) channel for the calling and called parties.

Table 4-16 H.323 Call Detail Table (continued)

Field	Description
Logical Channel Number	The logical channel number value of the media (RTP) channel for the calling and called parties.
H.245 IP Address	The IP address where the calling and called parties send H.245 messages to negotiate.
H.245 Port	The port where the calling and called parties send H.245 messages to negotiate.
RTP IP Address	IP address where the calling and called parties send the RTP packets.
RTP Port	Port where the calling and called parties send the RTP packets.
Codec	The encoding or decoding method used to convert analog signals to digital.
RTCP IP Address	IP address where the RTCP report is sent to.
RTCP Port	Port where the RTCP report is sent to.
Start Time	Day, date, and time the call started.
End Time	Day, date, and time the call ended.
Synch Source	Synchronization source value that represents the calling and called party in RTP packets.
Packets Sent	The cumulative number of packets sent on the call, as reported in the last RTCP sender report.
Octets Sent	The cumulative number of octets sent on the call, as reported in the last RTCP sender report.
Packets Lost	The cumulative number of packets lost on the call, as reported in the last RTCP sender report.
Average Packet Loss (%)	The average fraction loss calculated as the sum of fraction loss reported in detected RTCP receiver reports, divided by the number of detected RTCP receiver reports.
Average Jitter (msec)	The average inter-arrival jitter calculated as the sum of all detected RTCP receiver reports inter-arrival jitter, divided by the number of detected RTCP receiver reports.

**Note**

Because of the nature of the MGCP protocol, calls that were monitored by the NAM might have the caller and called party information reversed.

Table 4-17 MGCP Call Detail Table

Field	Description
Name	Alias name or MGCP endpoint ID. Note This information might appear in a separate Q.931 table above the MGCP Call Detail table.
Phone Number	Phone number of the calling and called parties. Note This information might appear in a separate Q.931 table above the MGCP Call Detail table.
Phone Number Confidence	Because of the nature of the protocol, the phone number is sometimes detected with errors. <ul style="list-style-type: none"> • High—The detection of the phone number is not likely to have a mistake. • Low—The detection of the phone number is subject to error due to the nature of the MGCP protocol. Note This information might appear in a separate Q.931 table above the MGCP Call Detail table.
RTP Address	Receiving RTP address of the calling and called parties.
Endpoint ID	MGCP endpoint ID of the calling and called parties.
Agent Address	IP address of the MGCP call agent.
Gateway Address	Network address of the MGCP gateway.
Call State	Setup—The call is setting up. Connected—The call is fully established. Ended—The call has ended.
Call ID	MGCP identification number of the call.
RTP Port	Receiving RTP port of the calling and called parties.
Connection ID	MGCP connection identification number of the call.
RTP Sampling Period	Period at which the RTP packet is sampled for transmission.
Silence Sup	On—Silence suppression option for the call is turned on. Off—Silence suppression option for the call is turned off.
Codec	Codec of the RTP streams.
Start Time	Time the call is fully established.

Table 4-17 MGCP Call Detail Table (continued)

Field	Description
End Time	Time the call ended.
Packet Sent	Number of RTP packets sent by the calling and called parties as reported in MGCP connection parameters.
Packets Received	Number of RTP packets received by the calling and called parties as reported in connection parameters.
Octets Sent	Number of RTP octets sent between the calling and called parties as reported in MGCP connection parameters.
Octets Received	Number of RTP octets received between the calling and called parties as reported in MGCP connection parameters.
Packet Loss (%)	Calculated percent loss based on the number of packet loss as reported in MGCP connection parameters.
Jitter	Jitter of the call as reported in MGCP connection parameters.

Viewing Active Calls

The Active Calls table displays information for all calls currently being monitored.

-
- Step 1** Click the Monitor tab.
- Step 2** Click **Voice**.
The Aggregate Statistics table is displayed.
- Step 3** In the contents, click **Active Calls**.
The [Active Calls Table](#) (Table 4-18) is displayed.

Table 4-18 Active Calls Table

Field	Description
Caller Number	Number of the phone placing the call.
Called Number	Number of the phone receiving the call.

Table 4-18 Active Calls Table (continued)

Field	Description
Caller	Alias name or MGCP endpoint ID of the calling party phone.
Called	Alias name or MGCP endpoint ID of the called party phone.
Time of Call	Time the call was placed.
Caller IP Address	IP address of the phone making the call.
Called IP Address	IP address of the phone receiving the call.

- Step 4** Select the protocol variable to filter from the list.
- Step 5** Enter the variable to filter in the text box, then click **Filter**.
The specified variable is displayed.
- Step 6** To clear the Active Calls table, click **Clear**.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Displaying Call Details From the Active Calls Table

To display details of a specific call from the Active Calls table, click the phone number in the Caller Number column. The Active Call Detail window is displayed.

For phones using SCCP, the [SCCP Call Detail Table \(Table 4-15\)](#) is shown.

For phones using H.323, the [H.323 Call Detail Table \(Table 4-16\)](#) is shown.

For phones using MGCP, the [MGCP Call Detail Table \(Table 4-17\)](#) is shown.

Monitoring Hosts Data

You can view results from any active hosts collections in the RMON1 and RMON2 host tables on the NAM.

Step 1 Click the Monitor tab.

Step 2 Click **Hosts**.

The Network Hosts table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the Network Hosts Current Rates Table, page 4-31](#)
- [Viewing the Network Hosts Top N Chart, page 4-35](#)
- [Viewing the Network Hosts Cumulative Data Table, page 4-36](#)

Step 3 To view the data based on the host MAC addresses, click **MAC Stations** in the contents.



Note MAC statistics are not available on NM-NAM devices.

The Mac Stations table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the MAC Stations Current Rates Table, page 4-37](#)
 - [Viewing the MAC Stations Top N Chart, page 4-39](#)
 - [Viewing the MAC Stations Cumulative Data Table, page 4-40](#)
-

Viewing the Network Hosts Current Rates Table

The Network Current Rates table allows you to view the various data collected for each host. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 In the contents, click **Network Hosts**.

Step 2 Click the Current Rates radio button.

The [Network Hosts Current Rates Table](#) (Table 4-19) is displayed.

Table 4-19 Network Hosts Current Rates Table

Field	Description
Address	Network address of the host.
Via	Protocol being monitored.
In Packets/s	Number of input packets collected per second.
Out Packets/s	Number of output packets collected per second.
In Bytes/s	Number of input bytes collected per second.
Out Bytes/s	Number of output bytes collected per second.
Non Unicast/s	Number of non unicast broadcast packets collected per second.

Step 3 Select a data source to monitor from the Data Source list.

Step 4 Enter an address to filter in the Address text box, then click **Filter**.

The specified address is displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.



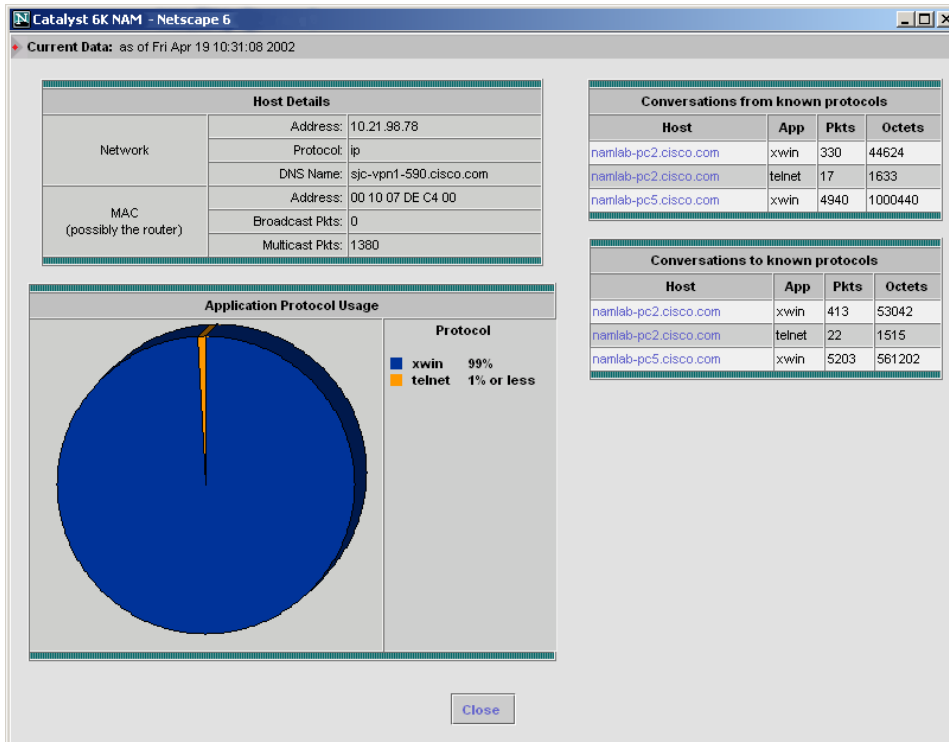
Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Network Host Details

To view details for a specific host, click on the address in the Address column of the Network Hosts table. The [Network Hosts Detail Window](#) (Figure 4-10) is displayed.

Figure 4-10 Network Hosts Detail Window



77644

- Host Details—Displays detailed information for the host.
- Application Protocol Usage Chart—Displays the application protocol usage for the host in graphical format.
- Conversations From Known Protocols—Displays known conversations and statistics *from* the specified host to other hosts on the network using known protocols.
- Conversations To Known Protocols—Displays known conversations and statistics *to* the specified host from other hosts on the network using known protocols.

**Note**

To view the full protocol name, move the cursor over the protocol name in the Application Protocol Usage chart.

Capturing Network Host Data from the Network Host Table

You can capture data for a specific host directly from the Network Host table.

Select the host from the table, then click **Capture**. The Packet Browser is displayed. For more information on viewing packets using the Packet Browser, see the [“Viewing Protocol Decode Information” section on page 6-12](#).

If a capture is already running, a message window is displayed. Click **Yes** to stop the current capture or **No** to disregard your selection.

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-17](#).

**Note**

The Capture button is disabled for NetFlow-based data sources.

Viewing Real-Time Traffic Statistics from the Hosts Table

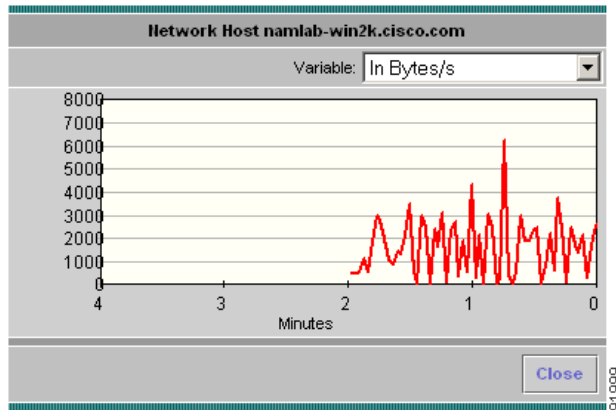
You can view real-time traffic statistics in a graphical format for a specific host.

Select the host from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-11](#)) is displayed.



Note The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-11 Real-Time Graph



Viewing Reports from the Network Hosts Table

You can view reports directly from the Network Hosts table. Select the host for which to view a report, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected host and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the Network Hosts Top N Chart

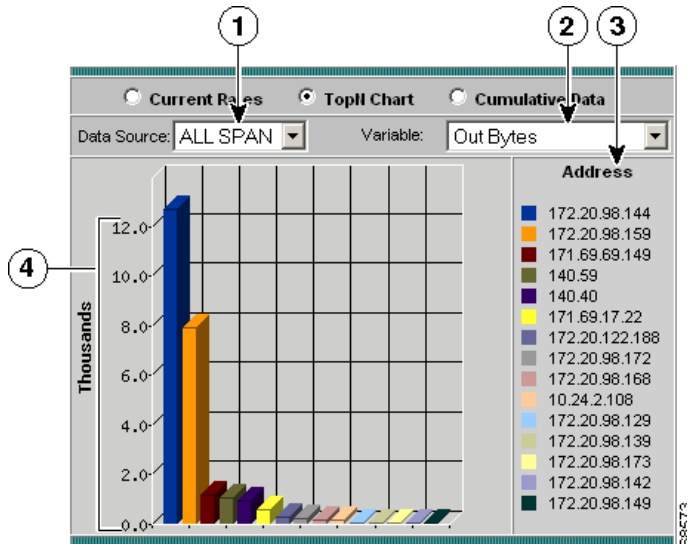
The Network Hosts Top N Chart allows you to view various data for the TopN hosts in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the “[Setting Global Preferences for All Users](#)” section on page 3-55.

Step 1 In the contents, click **Network Hosts**.

Step 2 Click the TopN Chart radio button.

The [Top N Network Hosts Chart](#) (Figure 4-12) is displayed.

Figure 4-12 Top N Network Hosts Chart



1	Data Source list.	3	Top N network host addresses.
2	Variable list.	4	Number of packets/bytes input/output per second for each Top N host.

- Step 3** Select the data source to monitor from the Data Source list.
- Step 4** Select one of the following from the Sort Option list:
- In Pkts—Displays the number of input packets.
 - Out Pkts—Displays the number of output packets.
 - In Bytes—Displays the number of input bytes.
 - Out Bytes—Displays the number of output bytes.
 - Non Unicast Pkts—Displays the number of non-unicast packets.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the Network Hosts Cumulative Data Table

The Network Hosts Cumulative Data Table allows you to view various data collected for each host. The information displayed represents the total data collected since the collection was created or since the NAM was restarted.

Step 1 In the contents, click **Network Hosts**.

Step 2 Click the Cumulative Data radio button.

The [Network Hosts Cumulative Data Table](#) (Table 4-20) is displayed.

Table 4-20 Network Hosts Cumulative Data Table

Field	Description
Address	Network address of the host.
Via	Protocol being monitored.
In Pkts	Total number of input packets over the last interval.
Out Pkts	Total number of output packets over the last interval.
In Bytes	Total number of input bytes over the last interval.

Table 4-20 Network Hosts Cumulative Data Table (continued)

Field	Description
Out Bytes	Total number of output bytes over the last interval.
Non Unicast	Total number of non-unicast broadcast packets over the last interval.

Step 3 Select a data source to monitor from the Data Source list.

Step 4 To view data for a specific address, enter the address in the Address text box, then click **Filter**.

Any matching addresses are displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the MAC Stations Current Rates Table



Note

This section does not apply to NM-NAM devices.

The MAC Stations Current Rates table allows you to view the various data collected for each host. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55](#).

- Step 1** In the contents, click **MAC Stations**.
- Step 2** Click the Current Rates Table radio button.
The **MAC Stations Table** (Table 4-21) is displayed.

Table 4-21 MAC Stations Table

Field	Description
Address	MAC address of the host.
In Packets/s	Number of packets received by the host per second.
Out Packets/s	Number of packets sent by the host per second.
In Bytes/s	Number of bytes received by the host per second.
Out Bytes/s	Number of bytes sent by the host per second.
Broadcasts/s	Number of broadcasts sent by the host per second.
Multicasts/s	Number of multicasts sent by the host per second.

- Step 3** Select a data source to monitor from the Data Source list.
- Step 4** Enter an address to filter in the Address text box, then click **Filter**.
The specified address is displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.



Tip To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the MAC Stations Top N Chart



Note

This section does not apply to NM-NAM devices.

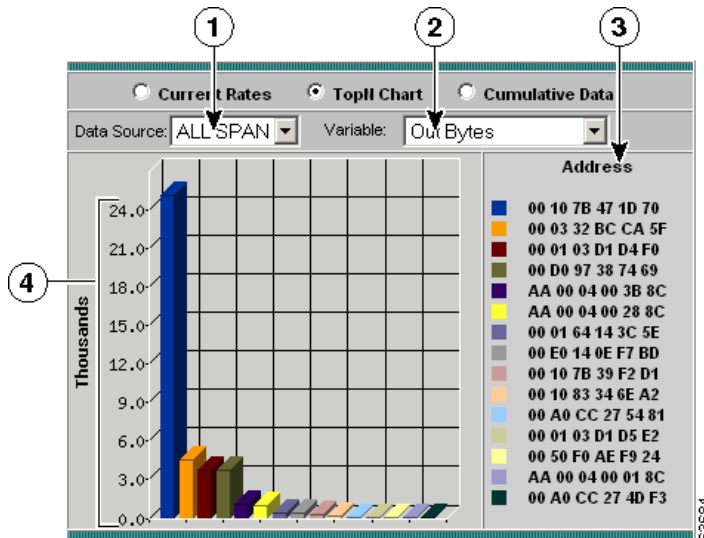
The MAC Stations Top N chart allows you to view the various data collected for each host in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 In the contents, click **MAC Stations**.

Step 2 Click the TopN Chart radio button.

The **Top N MAC Stations Chart** (Figure 4-13) is displayed.

Figure 4-13 Top N MAC Stations Chart



1	Data Source list.	3	Top N MAC host addresses.
2	Variable list.	4	Number of packets/bytes input/output per second for each Top N host.

Step 3 Select the data source to monitor from the Data Source list.

Step 4 Select one of the following from the Sort Option list:

- In Packets—Displays the number of input packets per second.
- Out Packets—Displays the number of output packets per second.
- In Bytes—Displays the number of input bytes per second.
- Out Packets—Displays the number of input bytes per second.
- Broadcast Packets—Sorts the addresses based on the number of broadcast packets per second.
- Multicast Packets—Sorts the addresses based on the number of multicast packets per second.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the MAC Stations Cumulative Data Table



Note

This section does not apply to NM-NAM devices.

The MAC Stations Cumulative Data Table allows you to view the various data collected for each host. The information displayed represents the total data collected since the collection was created or since the NAM was restarted.

Step 1 In the contents, click **MAC Stations**.

Step 2 Click the Cumulative Data radio button.

The [MAC Stations Cumulative Data Table](#) (Table 4-21) is displayed.

Table 4-22 *MAC Stations Cumulative Data Table*

Field	Description
Address	MAC address of the host.
In Packets	Total number of packets received by the host over the last time interval.
Out Packets	Total number of packets sent by the host over the last time interval.
In Bytes	Total number of bytes received by the host over the last time interval.
Out Bytes	Total number of bytes sent by the host over the last time interval.
Broadcasts	Total number of broadcasts sent by the host over the last time interval.
Multicasts	Total number of multicasts sent by the host.

Step 3 Select a data source to monitor from the Data Source list.

Step 4 Enter an address to filter in the Address text box, then click **Filter**.

The specified address is displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Conversations Data

You can view conversations data collected on the NAM. Conversations data represents the number of packets and bytes collected between two hosts.

Step 1 Click the Monitor tab.

Step 2 Click **Conversations**.

The Network Hosts Conversations table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the Network Host Conversations Current Rates Table, page 4-42](#)
- [Viewing the Network Host Conversations Top N Chart, page 4-46](#)
- [Viewing the Network Host Conversations Cumulative Data Table, page 4-48](#)

Step 3 To view the conversations data based on the MAC addresses, click **MAC Stations** in the contents.



Note MAC statistics are not available on NM-NAM devices.

The MAC Station Conversations table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the MAC Station Conversations Current Rates Table, page 4-49](#)
 - [Viewing the MAC Conversations Top N Chart, page 4-50](#)
 - [Viewing the MAC Station Conversations Cumulative Data Table, page 4-52](#)
-

Viewing the Network Host Conversations Current Rates Table

The Network Host Conversations Current Rates table allows you to view the number of packets and bytes collected for each host conversation. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

- Step 1** In the contents, click **Network Hosts**.
- Step 2** Click the Current Rates Table radio button.
- The [Network Host Conversations Current Rates Table \(Table 4-23\)](#) is displayed.

Table 4-23 Network Host Conversations Current Rates Table

Field	Description
Source	Source address of the conversation.
Via	Network layer protocol over which the hosts are conversing.
Destination	Destination address of the conversation.
Packets/s	Number of packets collected per second for the conversation over the last interval.
Bytes/s	Number of bytes collected per second for the conversation. over the last interval.

- Step 3** Select the data source to be monitored from the Data Source list.
- Step 4** To view data for a specific source or destination, select Source, Destination, or Source or Destination from the list.
- Step 5** Enter the address in the text box, then click **Filter**.
- Any matching source or destination addresses are displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.



Tip To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Network Host Conversation Details

To view conversation details for a specific network conversation, click the network address in the Source or Destination column. The following tables are displayed:

- Host Details—Displays detailed information for the source or destination host.
- Application Protocol Usage Chart—Displays the application protocol usage for the source of destination host in graphical format.
- Conversations From Known Protocols—Displays known conversations and statistics from the specified host to other hosts on the network using known protocols.
- Conversations To Known Protocols—Displays known conversations and statistics to the specified host from other hosts on the network using known protocols.

**Note**

To view the full protocol name, move the cursor over the protocol name in the Application Protocol Usage chart.

Capturing Network Host Conversation Data from the Network Host Conversations Table

You can capture data for a specific network host conversation directly from the Network Host Conversations table.

Select the conversation from the table, then click **Capture**. The Packet Browser is displayed. For more information on viewing packets using the Packet Browser, see the [“Viewing Protocol Decode Information”](#) section on page 6-12.

If a capture is already running, a message window is displayed. Click **Yes** to stop the current capture or **No** to disregard your selection.

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters”](#) section on page 6-17.



Note The Capture button is disabled for NetFlow-based data sources.

Viewing Real-Time Traffic Statistics from the Network Host Conversations Table

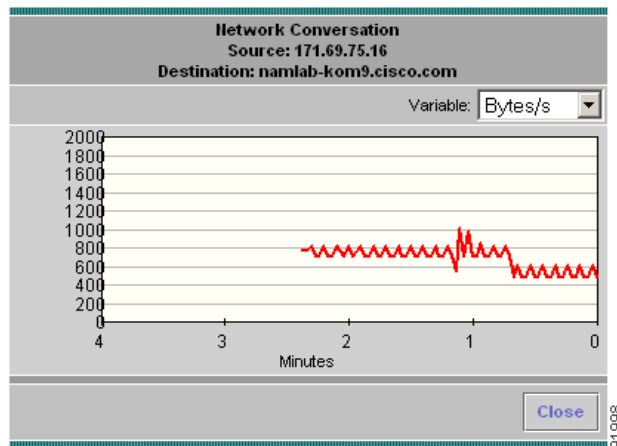
You can view real-time traffic statistics in a graphical format for a specific host conversation.

Select the conversation from the table, then click **Real-Time**. The Real-Time Graph (Figure 4-11) is displayed.



Note The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-14 Real-Time Graph



Viewing Reports from the Network Host Conversations Table

You can view reports directly from the Network Hosts Conversations table. Select the conversation you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected host and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the Network Host Conversations Top N Chart

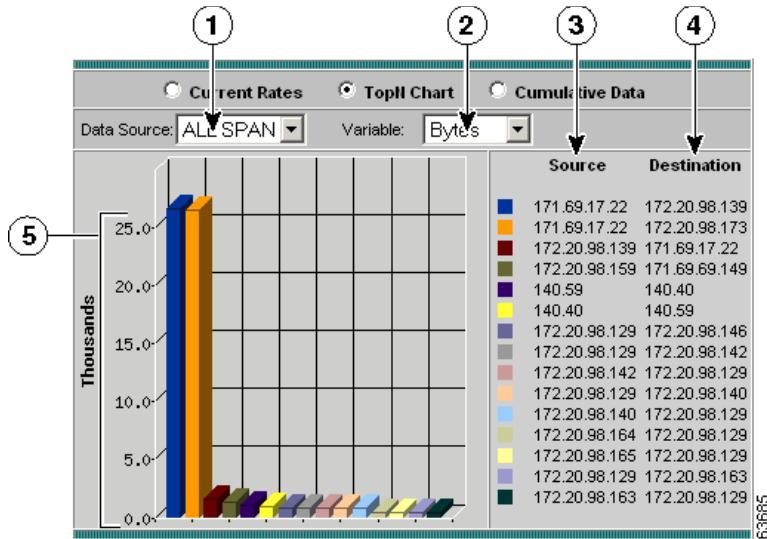
The Top N Network Host Conversations Chart allows you to view the number of packets and bytes collected for the Top N network host conversations in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55.](#)

Step 1 In the contents, click **Network Hosts**.

Step 2 Click the TopN Chart radio button.

The [Top N Network Host Conversations Chart](#)([Figure 4-15](#)) is displayed.

Figure 4-15 Top N Network Host Conversations Chart



1	Data Source list.	4	Top N destination network addresses.
2	Variable list.	5	Number of packets or bytes collected per second.
3	Top N source network addresses.		

Step 3 Select the data source to be monitored from the Data Source list.

Step 4 Select one of the following from the Variable list:

- Packets—Sorts the addresses based on the number of packets.
- Bytes—Sorts the addresses based on the number of bytes.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the Network Host Conversations Cumulative Data Table

The Network Host Conversations Cumulative Data Table allows you to view the number of packets and bytes collected for each host conversation. The data displayed is the total number of packets and bytes collected since the collection was created or since the NAM was restarted.

Step 1 In the contents, click **Network Hosts**.

Step 2 Click the Cumulative Data radio button.

The [Network Host Conversations Cumulative Data Table](#) (Table 4-24) is displayed.

Table 4-24 Network Host Conversations Cumulative Data Table

Field	Description
Source	Source address of the conversation.
Via	Network layer protocol over which the hosts are conversing.
Destination	Destination address of the conversation.
Packets	Total number of packets collected over the last time interval for the conversation.
Bytes	Total number of bytes collected over the last time interval for the conversation.

Step 3 Select a data source to monitor from the Data Source list.

Step 4 Enter an address to filter in the Address text box, then click **Filter**.

The specified address is displayed.

Step 5 To refresh the table, click **Refresh**.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Network Host Conversation Details

To view conversation details for a specific network conversation, click the network address in the Source or Destination column. The following tables are displayed:

- Host Details—Displays detailed information for the source or destination host.
- Application Protocol Usage Chart—Displays the application protocol usage for the source or destination host in graphical format.
- Conversations From Known Protocols—Displays known conversations and statistics from the specified host to other hosts on the network using known protocols.
- Conversations To Known Protocols—Displays known conversations and statistics to the specified host from other hosts on the network using known protocols.

Viewing the MAC Station Conversations Current Rates Table



Note

This section does not apply to NM-NAM devices.

The MAC Station Conversations Current Rates table allows you to view the number of packets and bytes collected for each host conversation. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 In the contents, click **MAC Stations**.

Step 2 Click the Current Rates Table radio button.

The [MAC Station Conversations Current Rates Table](#) (Table 4-25) is displayed.

Table 4-25 MAC Station Conversations Current Rates Table

Field	Description
Source	Source MAC address of the conversation.
Destination	Destination MAC address of the conversation.
Packets/s	Number of packets collected per second for the conversation over the last interval.
Bytes/s	Number of bytes collected per second for the conversation. over the last interval.
Errors/s	Number of errors collected per second for the conversation. over the last interval.

Step 3 Select the data source to be monitored from the Data Source list.

Step 4 To view data for a specific address, enter the full or partial MAC address in the Address text box, then click **Filter**.

Any matching addresses are displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the MAC Conversations Top N Chart



Note

This section does not apply to NM-NAM devices.

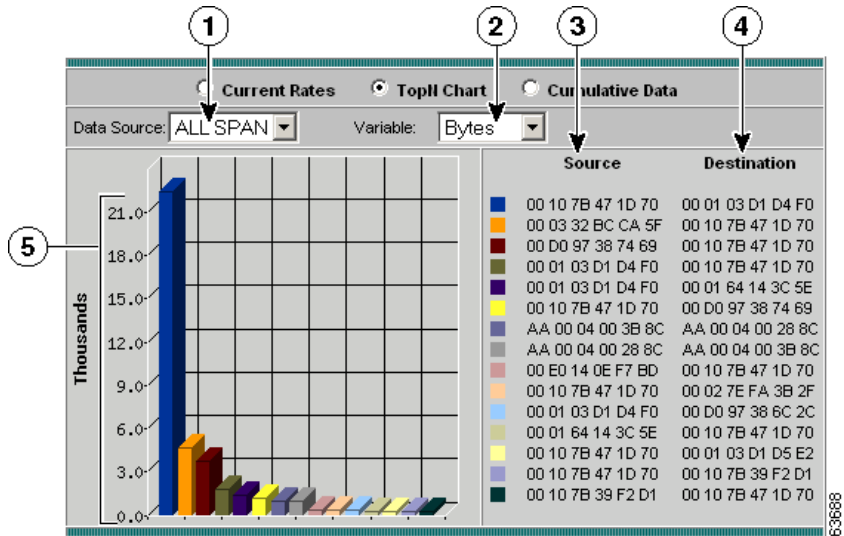
The Top N MAC Station Conversations Chart allows you to view the number of packets and bytes collected for the Top N MAC station conversations in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 In the contents, click **MAC Stations**.

Step 2 Click the TopN Chart radio button.

The **Top N MAC Station Conversations Chart** (Figure 4-16) is displayed.

Figure 4-16 Top N MAC Station Conversations Chart



1	Data Source list.	4	Top N destination MAC addresses.
2	Variable list.	5	Number of packets, bytes, or errors collected per second.
3	Top N source MAC addresses.		

- Step 3** Select the data source to be monitored from the Data Source list.
- Step 4** Select one of the following from the Variable list:
- Packets—Displays the number of packets.
 - Bytes—Displays the number of bytes.
 - Errors—Displays the number of errors.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the MAC Station Conversations Cumulative Data Table

**Note**

This section does not apply to NM-NAM devices.

The MAC Station Conversations Cumulative Data Table allows you to view the number of packets and bytes collected for each MAC station conversation. The data displayed is the total number of packets and bytes collected since the collection was created or since the NAM was restarted.

Step 1 In the contents, click **MAC Stations**.

Step 2 Click the Cumulative Data radio button.

The [MAC Station Conversations Cumulative Data Table](#) (Table 4-26) is displayed.

Table 4-26 *MAC Station Conversations Cumulative Data Table*

Field	Description
Source	Source MAC address of the conversation.
Destination	Destination MAC address of the conversation.
Pkts	Total number of packets collected over the last time interval for the conversation.

Table 4-26 MAC Station Conversations Cumulative Data Table (continued)

Field	Description
Bytes	Total number of bytes collected over the last time interval for the conversation.
Errors	Total number of errors collected over the last time interval for the conversation.

- Step 3** Select the data source from the Data Source list.
- Step 4** Enter an address to filter in the Address text box, then click **Filter**.
The specified address is displayed.
- Step 5** To refresh the table, click **Refresh**.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing VLAN Data

**Note**

This section does not apply to NM-NAM devices.

You can view VLAN traffic statistics or VLAN priority (COS) statistics collected on the NAM. Supervisor engine module collections are done independent of any collections done on the NAM.

**Note**

Supervisor engine module-based collections require Supervisor II engine module or later on your switch.

Step 1 Click the Monitor tab.

Step 2 Click **VLAN**.

The VLAN Traffic Statistics table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the VLAN Traffic Statistics Current Rates Table, page 4-54.](#)
- [Viewing the VLAN Traffic Statistics Top N Chart, page 4-56.](#)
- [Viewing VLAN Traffic Statistics Cumulative Data Table, page 4-57.](#)

Step 3 To view the VLAN data based on VLAN priority (COS) statistics, click **VLAN Priority (COS) Statistics** in the contents.

The VLAN Priority (COS) Statistics table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the VLAN Priority \(COS\) Statistics Current Rates Table, page 4-58.](#)
 - [Viewing the VLAN Priority \(COS\) Statistics Top N Chart, page 4-59.](#)
 - [Viewing the VLAN Priority \(COS\) Statistics Cumulative Data Table, page 4-61.](#)
-

Viewing the VLAN Traffic Statistics Current Rates Table



Note

This section does not apply to NM-NAM devices.

The VLAN Traffic Statistics Current Rates table allows you to view various data collected for each VLAN ID. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55.](#)

To view the VLAN Traffic Statistics Current Rates table, click the Current Rates radio button.

The [VLAN Traffic Statistics Table \(Table 4-27\)](#) is displayed.

Table 4-27 VLAN Traffic Statistics Table

Field	Description
VLAN ID	VLAN ID number.
Packets/s	Number of packets collected per second over the last time interval.
Bytes/s	Number of bytes collected per second over the last time interval.
Non-Unicast Packets/s	Number of non-unicast packets collected per second over the last time interval.
Non-Unicast Bytes/s	Number of non-unicast bytes collected per second over the last time interval.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Reports from the VLAN Traffic Statistics Table

You can view reports directly from the VLAN Traffic Statistics table. Select the VLAN ID you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected VLAN and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the VLAN Traffic Statistics Top N Chart



Note

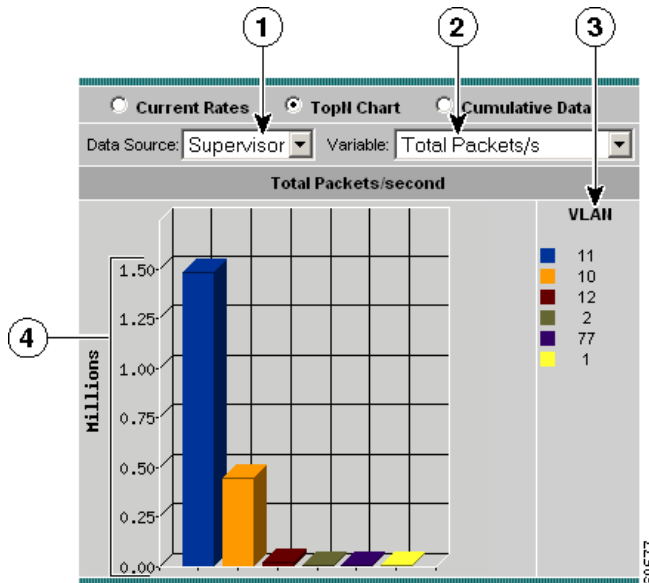
This section does not apply to NM-NAM devices.

The Top N VLAN Traffic Statistics Chart allows you to view the various data collected for the top N VLAN IDs in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 Click the TopN Chart radio button.

The [Top N VLAN Traffic Statistics Chart](#) (Figure 4-17) is displayed.

Figure 4-17 Top N VLAN Traffic Statistics Chart



1	Data source list.	3	Top N VLAN IDs.
2	Variable list.	4	Number of packets/bytes collected per second.

Step 2 Select the data source from the Data Source list.

Step 3 Select one of the following from the Variable list:

- Total Packets—Displays the number of total packets.
- Total Bytes—Displays the number of total bytes.
- Non-unicast Packets—Displays the number of non-unicast packets.
- Non-unicast Bytes—Displays the number of non-unicast bytes.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing VLAN Traffic Statistics Cumulative Data Table



Note

This section does not apply to NM-NAM devices.

The VLAN Traffic Statistics Cumulative Data table allows you to view various data collected for each VLAN ID. The information displayed represents the total data collected since the collection was created or since the NAM was restarted.

To view the VLAN Traffic Statistics Cumulative Data table, click the Cumulative Data Table radio button.

The [VLAN Traffic Statistics Cumulative Data Table \(Table 4-28\)](#) is displayed.

Table 4-28 VLAN Traffic Statistics Cumulative Data Table

Field	Description
VLAN ID	VLAN ID number.
Packets	Total number of packets collected over the last time interval.
Bytes	Total number of bytes collected over the last time interval.
Non-Unicast Packets	Total number of non-unicast packets collected over the last time interval.
Non-Unicast Bytes	Total number of non-unicast bytes collected over the last time interval.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the VLAN Priority (COS) Statistics Current Rates Table

**Note**

This section does not apply to NM-NAM devices.

The VLAN Priority (COS) Statistics Current Rates table allows you to view user priority distributions per data source. The displayed information represents the data collected each second during the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55](#).

Step 1 In the contents, click **Priority (COS) Statistics**.

The [VLAN Priority \(COS\) Statistics Current Rates Table \(Table 4-29\)](#) is displayed.

Table 4-29 VLAN Priority (COS) Statistics Current Rates Table

Field	Description
Priority	Value of the three bit user priority field encoded in the Tag Control Information field.
Packets/s	Number of packets collected on this priority level. Data is the rate per second over the last time interval.
Bytes/s	Number of bytes collected on this priority level. Data is the rate per second over the last time interval.

Step 2 Select the data source to monitor from the Data Source list.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the VLAN Priority (COS) Statistics Top N Chart



Note

This section does not apply to NM-NAM devices.

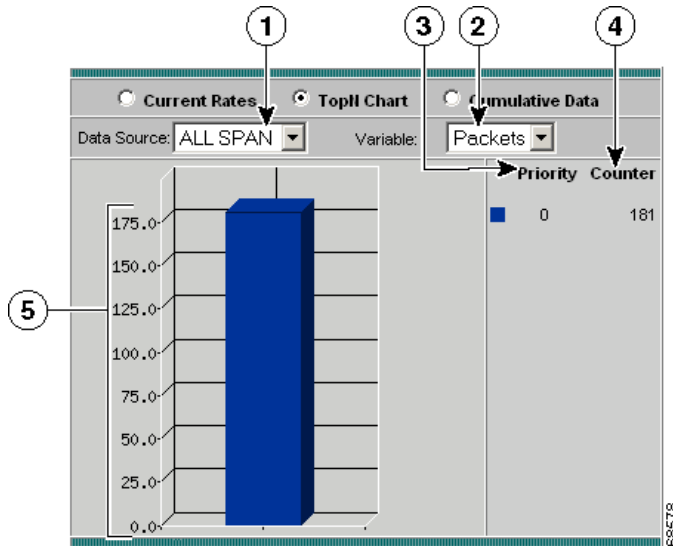
The Top N VLAN Priority (COS) Statistics Chart allows you to view user priority distributions per data source in a graphical format. The information displayed represents the data collected *per second* over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55](#).

Step 1 In the contents, click **Priority (COS) Statistics**.

Step 2 Click the TopN Chart radio button.

The **Top N VLAN Priorities (COS) Statistics Chart**(Figure 4-18) is displayed.

Figure 4-18 Top N VLAN Priorities (COS) Statistics Chart



1	Data Source list.	4	VLAN counter.
2	Variable list.	5	Number of packets/bytes collected per second.
3	Top N VLAN priorities.		

Step 3 Select the data source to be monitored from the Data Source list.

Step 4 Select one of the following from the Variable list:

- Packets—Displays the number of packets.
- Bytes—Displays the number of bytes.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the VLAN Priority (COS) Statistics Cumulative Data Table

**Note**

This section does not apply to NM-NAM devices.

The VLAN Priority (COS) Statistics Cumulative Data table allows you to view user priority distributions per data source. The information displayed represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 In the contents, click **Priority (COS) Statistics**.

Step 2 Click the Cumulative Data radio button.

The [VLAN Priority \(COS\) Statistics Cumulative Data Table](#) (Table 4-30) is displayed.

Table 4-30 *VLAN Priority (COS) Statistics Cumulative Data Table*

Field	Description
Priority	Value of the three bit user priority field encoded in the Tag Control Information field.
Packets	Total number of packets collected on this priority level.
Bytes	Total number of bytes collected on this priority level.

Step 3 Select the data source to monitor from the Data Source list.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing DiffServ Data

You can view the distribution of packets and bytes based on the Differential Services (DiffServ) data collected on the NAM.

**Note**

DiffServ data is not available for local NetFlow devices. This is applicable to WS-X6380-NAM, WS-SVC-NAM-1, and WS-SVC-NAM-2 devices.

Step 1 Click the Monitor tab.

Step 2 Click **DiffServ**.

The DiffServ Traffic Statistics table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the DiffServ Traffic Statistics Current Rates Table, page 4-63.](#)
- [Viewing the DiffServ Traffic Top N Chart, page 4-65.](#)
- [Viewing the DiffServ Traffic Statistics Cumulative Data Table, page 4-66.](#)

Step 3 To view the DiffServ data based on the application statistics, click **Application Stats** in the contents.

The DiffServ Applications Statistics table is displayed with three radio buttons above it. You can select a radio button for:

- [Viewing the DiffServ Application Statistics Current Rates Table, page 4-67.](#)
- [Viewing the DiffServ Application Statistics Top N Chart.](#)
- [Viewing the DiffServ Application Statistics Cumulative Data Table, page 4-71.](#)

Step 4 To view the DiffServ data based on the host statistics, click **Host Stats** in the contents.

The DiffServ Host Statistics table is displayed with three radio buttons above it.

You can select a radio button for:

- [Viewing the DiffServ Host Statistics Current Rates Table, page 4-72.](#)
- [Viewing the DiffServ Host Statistics Top N Chart, page 4-75.](#)
- [Viewing the DiffServ Host Statistics Cumulative Data Table, page 4-77.](#)

Viewing the DiffServ Traffic Statistics Current Rates Table

Step 1 In the contents, click **Traffic Stats**.

Step 2 Click the Current Rates Table radio button.

The [DiffServ Traffic Statistics Current Rates Table \(Table 4-31\)](#) is displayed.

Table 4-31 DiffServ Traffic Statistics Current Rates Table

Field	Description
Aggregation Group	Name of the aggregation group.
Packets/s	Total packets collected per second over the last interval.
Bytes/s	Total bytes collected per second over the last interval.

Step 3 Select the data source and profile to monitor from the Data Source-Profile list.

Step 4 Enter the aggregation group to filter in the Aggregation text box, then click **Filter**.
The specified aggregation group is displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing Real-Time Traffic Statistics from the DiffServ Traffic Statistics Table

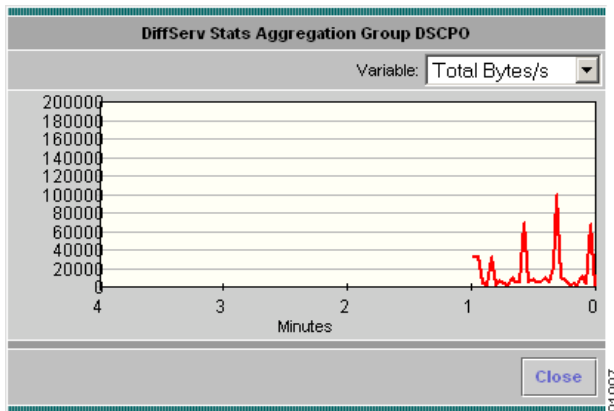
You can view real-time traffic statistics in a graphical format for a specific aggregation group in the DiffServ Traffic Statistics table.

Select the aggregation group from the table, then click **Real-Time**. The Real-Time Graph (Figure 4-11) is displayed.

**Note**

The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-19 Real-Time Graph



Viewing Reports from the DiffServ Traffic Statistics Table

You can view reports directly from the DiffServ Traffic Statistics table. Select the aggregation group you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

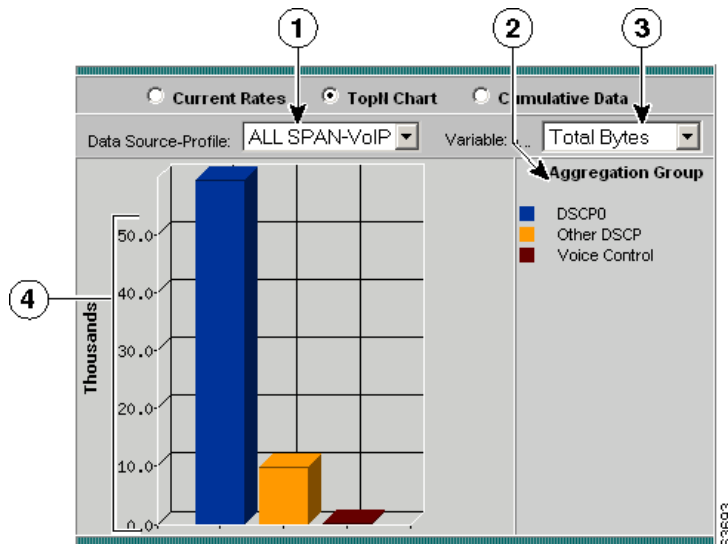
Viewing the DiffServ Traffic Top N Chart

Step 1 In the contents, click **Traffic Stats.**

Step 2 Click the TopN Chart radio button.

The [Top N DiffServ Aggregation Group Chart](#) (Figure 4-20) is displayed.

Figure 4-20 Top N DiffServ Aggregation Group Chart



1	Data Source-Profile list.	3	Variable list.
2	Top N aggregation groups.	4	Number of packets/bytes collected per second.

- Step 3** Select the data source and profile to monitor from the Data Source-profile list.
- Step 4** Select one of the following from the Variable list:
- Total Packets—Displays the number of total packets.
 - Total Bytes—Displays the number of total bytes.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the DiffServ Traffic Statistics Cumulative Data Table

- Step 1** In the contents, click **Traffic Stats**.
- Step 2** Click the Cumulative Data radio button.
- The [DiffServ Traffic Statistics Cumulative Data](#) (Table 4-32) is displayed.

Table 4-32 *DiffServ Traffic Statistics Cumulative Data*

Field	Description
Aggregation Group	Name of the aggregation group.
Packets	Total packets collected over the last interval.
Bytes	Total bytes collected over the last interval.

- Step 3** Select the data source and profile to monitor from the Data Source-profile list.
- Step 4** Enter the aggregation group to filter in the Aggregation text box, then click **Filter**.
- The specified aggregation group is displayed.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the DiffServ Application Statistics Current Rates Table

Step 1 In the contents, click **Application Stats**.

Step 2 Click the Current Rates Table radio button.

The [DiffServ Application Statistics Current Rates](#)(Table 4-33) is displayed.

Table 4-33 DiffServ Application Statistics Current Rates

Field	Description
Protocol Name	Name of the monitored protocol.
Packets/s	Total packets collected per second over the last interval.
Bytes/s	Total bytes collected per second over the last interval.

Step 3 Select the data source and profile to monitor from the Data Source-Profile list.

Step 4 Select the aggregation group from the Aggregation list.

Step 5 To view a specific protocol, enter the protocol in the Protocol text box, then click **Filter**.

The specified protocol is displayed.

**Tip**

To view the full protocol name, move the cursor over the protocol name

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

**Tip**

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Displaying Application Conversation Details From Application Statistics Table

To view the Application Conversations details table, click the protocol name in the Protocol Name column. The [Application Conversations Table](#) (Table 4-34) is displayed.

Table 4-34 Application Conversations Table

Field	Description
Source	Source host address of the conversation.
Destination	Destination host address of the conversation.
Packets	Number of packets during the conversation.
Bytes	Number of bytes during the conversation.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing Real-Time Traffic Statistics from the DiffServ Application Statistics Table

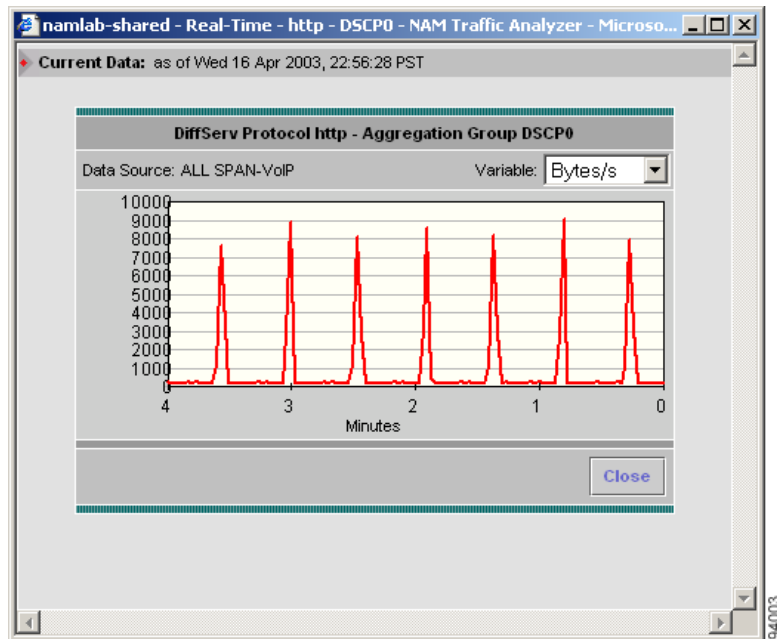
You can view real-time traffic statistics in a graphical format for a specific application protocol in the DiffServ Application Statistics table.

Select the application protocol from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-11](#)) is displayed.

**Note**

The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-21 Real-Time Graph



Viewing Reports from the DiffServ Application Statistics Table

You can view reports directly from the DiffServ Application Statistics table. Select the application protocol you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected application and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

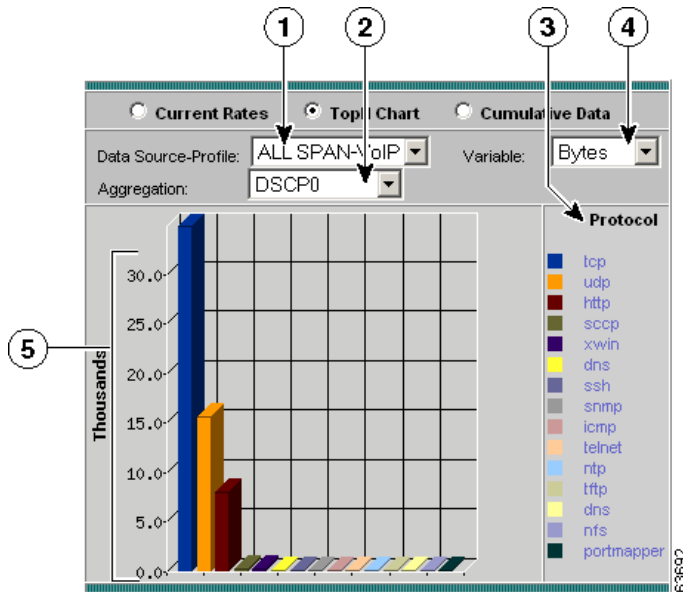
Viewing the DiffServ Application Statistics Top N Chart

Step 1 In the contents, click **Application Stats**.

Step 2 Click the TopN Chart radio button.

The [Top N DiffServ Application Statistics Chart](#) (Figure 4-22) is displayed.

Figure 4-22 Top N DiffServ Application Statistics Chart



1	Data Source-Profile list.	4	Variable list.
2	Aggregation group list.	5	Total packets/bytes collected per second for each protocol.
3	Top N protocols sorted by color.		

- Step 3** Select the data source to monitor from the Data Source list.
- Step 4** Select the aggregation group from the Aggregation list.
- Step 5** Select one of the following from the Variable list:
- Total Packets—Sorts the addresses based on the number of total packets.
 - Total Bytes—Sorts the addresses based on the number of total bytes.

**Tip**

To turn off auto refresh, deselect the Auto Refresh check box.
To view the full protocol name, move the cursor over the protocol name

Viewing the DiffServ Application Statistics Cumulative Data Table

- Step 1** In the contents, click **Application Stats**.
- Step 2** Click the Cumulative Data radio button.

The [DiffServ Application Statistics Cumulative Data Table](#) (Table 4-35) is displayed.

Table 4-35 *DiffServ Application Statistics Cumulative Data Table*

Field	Description
Protocol Name	Name of the monitored protocol.
Packets	Total packets collected over the last interval.
Bytes	Total bytes collected over the last interval.

- Step 3** Select the data source and profile to monitor from the Data Source-Profile list.

- Step 4** Select the aggregation group from the Aggregation list.
- Step 5** To view a specific protocol, enter the protocol in the Protocol text box, then click **Filter**.

The specified protocol is displayed.



Tip

To view the full protocol name, move the cursor over the protocol name



Tip

To turn off auto refresh, deselect the Auto Refresh check box.



Tip

To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Viewing the DiffServ Host Statistics Current Rates Table

- Step 1** In the contents, click **Host Stats**.
- Step 2** Click the Current Rates radio button.

The [DiffServ Host Statistics Current Rates Table](#) (Table 4-36) is displayed.

Table 4-36 *DiffServ Host Statistics Current Rates Table*

Field	Description
Address	Address of the host.
Type	Type of protocol monitored.
In Packets/s	Total number of input packets collected per second.
Out Packets/s	Total number of output packets collected per second.
In Bytes/s	Total number of input bytes collected per second.
Total Bytes/s	Total number of output bytes collected per second.

- Step 3** Select the data source and profile to monitor from the Data Source-Profile list.
- Step 4** Select the aggregation group from the Aggregation list.
- Step 5** To view a specific address, enter the address in the Address text box, then click **Filter**.
- The specified address is displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.



Tip To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Displaying Host Conversation Details From the DiffServ Host Statistics Table

To view the Host Conversations details table, click the address name in the Address column. The [Host Conversations Table](#) (Table 4-37) is displayed.

Table 4-37 *Host Conversations Table*

Field	Description
Source	Source host address of the conversation.
Application	The application protocol used on the conversation.
Destination	Destination host address of the conversation.
Packets	Number of packets during the conversation.
Octets	Number of octets during the conversation.



Tip To turn off auto refresh, deselect the Auto Refresh check box.

Viewing Real-Time Data from the DiffServ Host Statistics Table

You can view real-time data in a graphical format for a specific host in the DiffServ Host Statistics table.

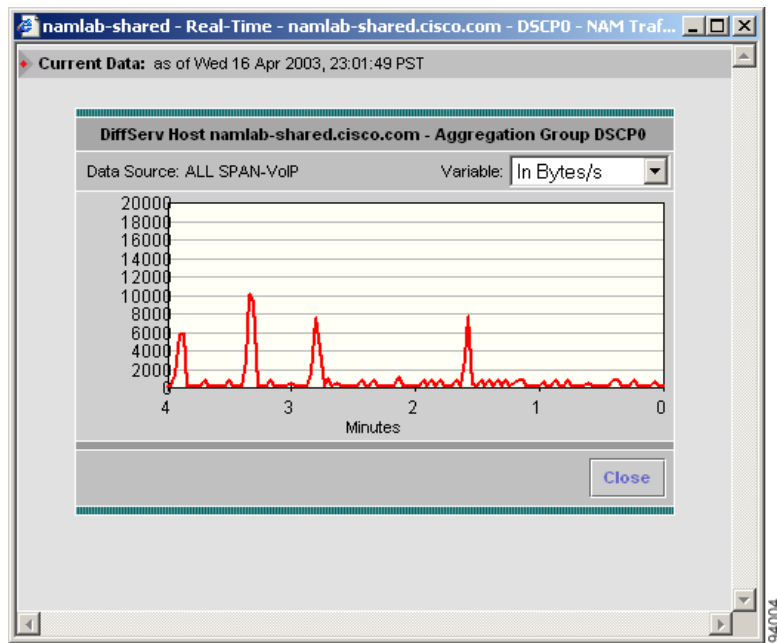
Select the host from the table, then click **Real-Time**. The Real-Time Graph (Figure 4-11) is displayed.



Note

The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-23 Real-Time Graph



Viewing Reports from the DiffServ Host Statistics Table

You can view reports directly from the DiffServ Host Statistics table. Select the host you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected host and data source.

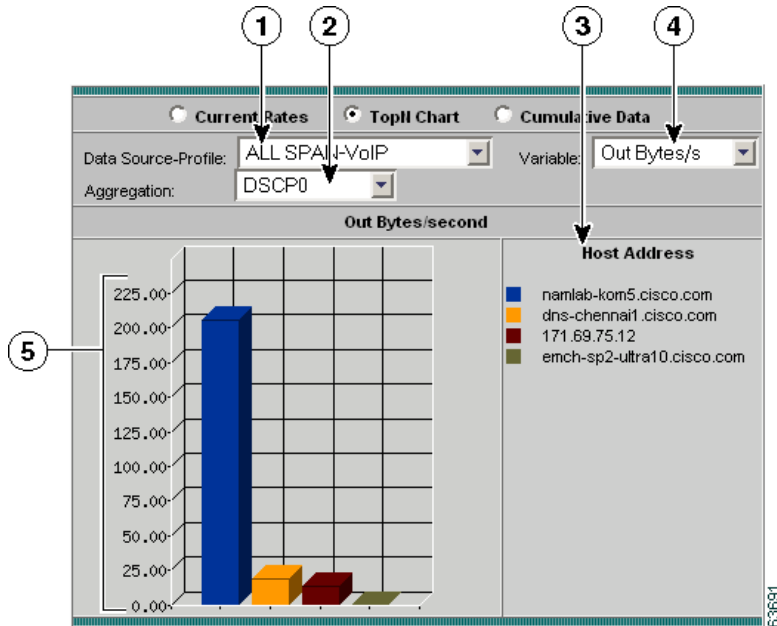
For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the DiffServ Host Statistics Top N Chart

-
- Step 1** In the contents, click **Host Stats**.
- Step 2** Click the TopN Chart radio button.

The [DiffServ Top N Host Statistics Chart \(Figure 4-24\)](#) is displayed.

Figure 4-24 DiffServ Top N Host Statistics Chart



1	Data Source-Profile list.	4	Variable list.
2	Aggregation group list.	5	Total packets/bytes collected per second for each address.
3	Top N host addresses sorted by color.		

- Step 3** Select the data source and profile from the Data Source-Profile list.
- Step 4** Select the aggregation group from the Aggregation list.
- Step 5** Select one of the following from the Variable list:
- Total Packets—Sorts the addresses based on the number of total packets.
 - Total bytes—Sorts the addresses based on the number of total bytes.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the DiffServ Host Statistics Cumulative Data Table

- Step 1** In the contents, click **Host Stats**.
- Step 2** Click the Cumulative Data radio button.
- The [DiffServ Host Statistics Cumulative Data Table](#) (Table 4-38) is displayed.

Table 4-38 *DiffServ Host Statistics Cumulative Data Table*

Field	Description
Address	Address of the host.
Type	Type of protocol monitored.
In Packets	Total number of packets received over the last time interval.
Out Packets	Total number of packets sent over the last time interval.
In Bytes	Total number of bytes received over the last time interval.
Out Bytes	Total number of bytes sent over the last time interval.

- Step 3** Select the data source to monitor from the Data Source list.

- Step 4** Select the aggregation group from the Aggregation list.
- Step 5** To view a specific address, enter the address in the Address text box, then click **Filter**.
- The specified address is displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.



Tip To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

Monitoring Response Time Data

Response time data provides TCP response time distributions for TCP protocols. You can view this data for each server or between clients and servers.

- Step 1** Click the Monitor tab.
- Step 2** Click **Response Time**.
- The Response Time Server Table is displayed with two radio buttons above it. You can select a radio button for:
- [Viewing the Server Response Time Table, page 4-79.](#)
 - [Viewing the Server Response Time Top N Chart, page 4-81.](#)
- Step 3** To view the data based on the response time between clients and servers, click **Client/Server** in the contents.
- The Client/Server Response Time Table is displayed with two radio buttons above it. You can select a radio button for:
- [Viewing the Client/Server Response Time Table, page 4-82.](#)
 - [Viewing the Client/Server Response Time Top N Chart, page 4-84.](#)

Viewing the Server Response Time Table

Step 1 Click the All Data radio button.

The [Server Response Time Table](#) (Table 4-39) is displayed.

Table 4-39 *Server Response Time Table*

Field	Description
Select	Selects a specific entry.
Server	Host address of the server.
Protocol	Application layer protocol.
Clients	Number of clients the server has communicated with.
Avg Resp Time	Average response time in milliseconds observed during the report interval.
Min Resp Time	Minimum response time in milliseconds observed during the report interval.
Max Resp Time	Maximum value of the individual response times observed during the interval.
Retries	Total number of application layer client retries collected during the report interval.
Timeouts	Number of times the NAM has timed-out a client request while waiting for a server response.

Step 2 Select the data source to be monitored from the Data Source list.

Step 3 Select the variable you want to filter from the filter list.

Step 4 Enter the address of the server or name of the protocol you wish to filter in the filter text box, then click **Filter**.

The specified server addresses or protocol names are displayed.



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

To view the full protocol name, move the cursor over the protocol name in the Protocol column of the table.

Viewing Server Response Time Details

To view details for a specific server, click the radio button in the Select column, then click **Details**. The Response Time Server Detail window is displayed. You can view detailed information from the server as well as a chart displaying the response time distribution.

Capturing Server Protocol Data from the Server Response Time Table

You can capture data from a specific server protocol directly from the Server Response Time table.

Select the server protocol from the table, then click **Capture**. The Packet Browser is displayed. For more information on viewing packets using the Packet Browser, see the [“Viewing Protocol Decode Information”](#) section on page 6-12.

If a capture is already running, a message window is displayed. Click **Yes** to stop the current capture or **No** to disregard your selection.

The Capture button is only available for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters”](#) section on page 6-17.



Note

The Capture button is disabled for NetFlow-based data sources.

Viewing Reports from the Server Response Time Table

You can view reports directly from the Server Response Time table. Select the server you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected server and data source.

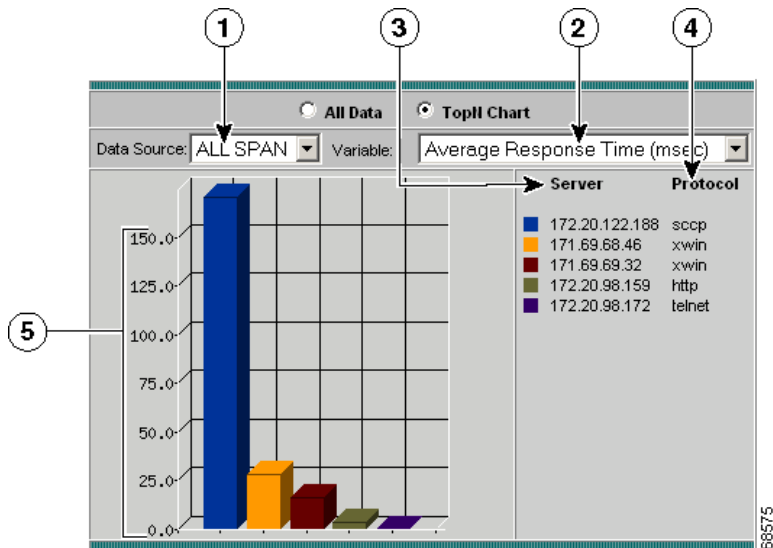
For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the Server Response Time Top N Chart

Step 1 Click the Top N Chart radio button.

The [Server Response Time Top N Chart](#) (Figure 4-25) is displayed.

Figure 4-25 Server Response Time Top N Chart



1	Data Source list.	4	Protocol used by server.
2	Variable list.	5	Variable value displayed per second.
3	Top N server addresses sorted by color.		

Step 2 Select the data source to be monitored from the Data Source list.

Step 3 Select the sorting option from the Variable list.

The specified option is displayed in the chart.

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To view the full protocol name, move the cursor over the protocol name in the Protocol column of the table.

Viewing the Client/Server Response Time Table

Step 1 In the contents, click **Client/Server**.

Step 2 Click the All radio button.

The [Client/Server Response Time Table](#)(Table 4-40) is displayed.

Table 4-40 *Client/Server Response Time Table*

Field	Description
Select	Selects a specific entry.
Server	Host address of the server.
Client	Host address of the client.
Protocol	Application layer protocol.
Avg Resp Time	Average response time in milliseconds observed during the report interval.
Min Resp Time	Minimum response time in milliseconds observed during the report interval.
Max Resp Time	Maximum value of the individual response times observed during the interval.
Retries	Total number of application layer client retries collected during the report interval.
Late Responses	Number of replies that have exceeded the RspTimeMax value.

Step 3 Select the data source to be monitored from the Data Source list.

Step 4 Select a variable to filter from the filter list.

Step 5 Enter the name of the variable to filter in the filter box, then click **Filter**.

The specified variable is displayed.

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To view the full protocol name, move the cursor over the protocol name in the Protocol column of the table.

Viewing Client/Server Response Time Details

To view details for a specific client/server conversation, click the radio button in the Select column, and click **Details**. The Response Time Client/Server Detail window is displayed. You can view detailed information from the client/server conversation as well as a chart displaying the response time distribution.

Capturing Protocol Data from the Client/Server Response Time Table

You can capture data for a specific protocol directly from the Client/Server Response Time table.

Select the server protocol from the table, then click **Capture**. The Packet Browser is displayed. For more information on viewing packets using the Packet Browser, see the [“Viewing Protocol Decode Information”](#) section on page 6-12.

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters”](#) section on page 6-17.

**Note**

The Capture button is disabled for NetFlow-based data sources.

Viewing Reports from the Client/Server Response Time Table

You can view reports directly from the Client/Server Response Time table. Select the protocol you wish to view a report on, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected client/server and data source.

For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

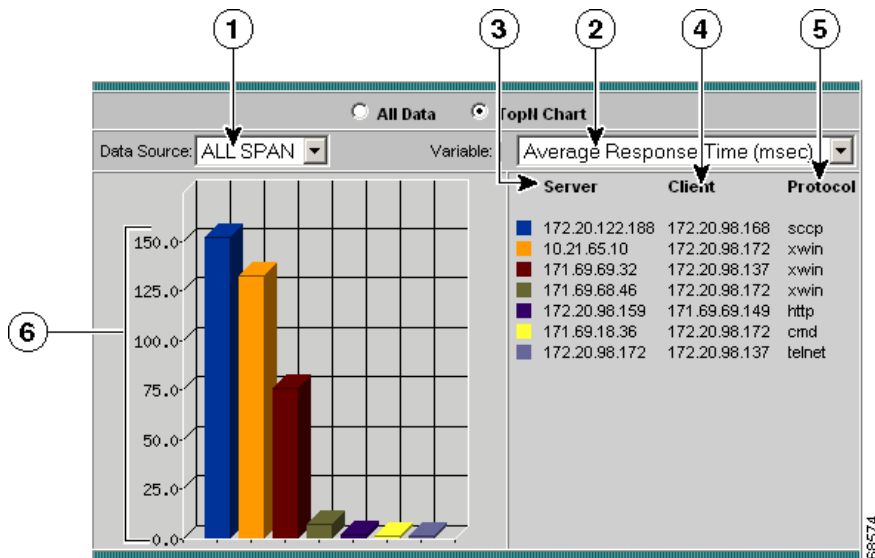
Viewing the Client/Server Response Time Top N Chart

Step 1 In the contents, click **Client/Server**.

Step 2 Click the TopN Chart radio button.

The **Client/Server Response Time Top N Chart** (Figure 4-26) is displayed.

Figure 4-26 Client/Server Response Time Top N Chart



1	Data Source list.	4	Top N clients sorted by color.
2	Variable list.	5	Protocol used for the conversation.
3	Top N servers sorted by color.	6	Variable value (per second) for each client/server conversation.

Step 3 Select the data source to be monitored from the Data Source list.

Step 4 Select the sorting option from the Variable list.

The specified option is displayed in the chart.

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
 - To view the full protocol name, move the cursor over the protocol name in the Protocol column of the table.
-

Viewing Port/Interface Statistics Data

To view the various data collected for the switch or router, click the Monitor tab, then click **Port Stats**. For NM-NAM devices, click **Interface Stats**. The Port/Interface Stats table is displayed with three radio buttons above it.

For Port Stats, you can click a radio button for:

- [Viewing the Port Stats Current Rates Table, page 4-85.](#)
- [Viewing the Top N Port Stats Chart, page 4-89.](#)
- [Viewing the Port Stats Cumulative Data Table, page 4-93.](#)

For Interface Stats you can click a radio button for:

- [Viewing the Interface Stats Current Rates Table, page 4-87.](#)
- [Viewing the Top N Interface Stats Chart, page 4-91.](#)
- [Viewing the Interface Stats Cumulative Data Table, page 4-94.](#)

Viewing the Port Stats Current Rates Table

The Port Stats Current Rates table allows you to view the various data collected for the switch. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the “[Setting Global Preferences for All Users](#)” section on page 3-55.

- Step 1** Click the Current Rates Table radio button.
The [Port Stats Current Rates Table](#) (Table 4-41) is displayed.

Table 4-41 Port Stats Current Rates Table

Field	Description
Port Name	Port number.
Utilization %	Utilization percentage of the port.
Dropped Events/s	Number of dropped events per second.
Bytes/s	Number of bytes collected on the port per second.
Packets/s	Number of packets collected on the port per second.
Broadcast Packets/s	Number of broadcast packets collected per second.
Multicast Packets/s	Number of multicast packets collected per second.
CRC Align Errors/s	Number of CRC align errors collected per second.
Undersize packets/s	Number of packets collected under 64 octets in length.
Oversize Packets/s	Number of packets collected over 1518 octets in length.
Fragments/s	Number of packets collected per second that were less than 64 octets in length and had bad a Frame Check Sequence (FCS).
Jabbers/s	Number of collected packets collected per second that were longer than 1518 octets in length and had a bad Frame Check Sequence (FCS).
Collisions/s	Number of collisions collected per second on the Ethernet segment.

- Step 2** Enter the port name to filter in the Port Name text box, then press **Filter**.
The specified port name is displayed.



Tip To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the Interface Stats Current Rates Table

The Interface Stats Current Rates table allows you to view the various data collected for the router. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

Step 1 Click the Current Rates radio button.

The [Interface Stats Current Rates Table](#) (Table 4-41) is displayed.

Table 4-42 *Interface Stats Current Rates Table*

Field	Description
Interface	Interface number.
In % Utilization	Utilization percentage of the port.
Out % Utilization	Utilization percentage of the port.
In Packets/s	Number of packets collected per second.
Out Packets/s	Number of packets sent out per second.
In Bytes/s	Number of bytes collected per second.
Out Bytes/s	Number of bytes sent out per second.
In Non-Unicasts/s	Number of non-unicasts collected per second.
Out Non-Unicasts/s	Number of non-unicasts sent out per second.
In Discards/s	Number of discards collected per second.
Out Discards/s	Number of discards sent out per second.
In Errors/s	Number of errors collected per second.
Out Errors/s	Number of errors sent out per second.

Step 2 Enter the name of the to filter in the Filter text box, then click **Filter**.

The specified interface name is displayed.

Viewing Port/Interface Details

To view packet distribution details on a specific port or interface, click the number of the port in the Port Name column or the number of the interface in the Interface column. The detail window displays a chart that shows the packet distribution per second on the specified port or interface.

Viewing Real-Time Traffic Data from the Port/Interface Stats Table

You can view real-time data in a graphical format for a specific switch port or interface in the Port Stats or Interface Stats table.

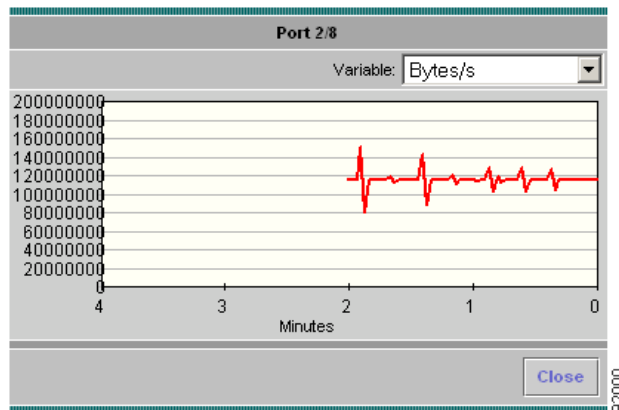
Select the switch port or interface from the table, then click **Real-Time**. The Real-Time Graph (Figure 4-27) is displayed.



Note

The Real-Time button is disabled for NetFlow-based data sources.

Figure 4-27 Real-Time Graph



Viewing Reports from the Port/Interface Stats Table

You can view reports directly from the Port Stats or Interface Stats table. Select the switch port or interface for which to view a report, then click **Report**. The Basic Reports graph is displayed. If a report is not configured, the Basic Reports screen appears and a new report is created for the selected port and data source.

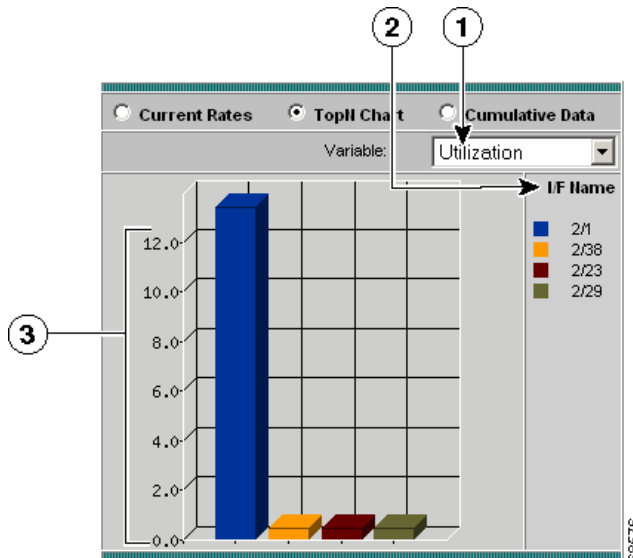
For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

Viewing the Top N Port Stats Chart

The Port Stats Top N Chart allows you to view the various data collected for each port in a graphical format. The information displayed represents the data collected per second over the last time interval.

- Step 1** Click the TopN Chart radio button.
The [Top N Port Stats Chart](#)([Figure 4-28](#)) is displayed.

Figure 4-28 Top N Port Stats Chart



1	Variable list.	3	Variable value (per second) for each switch port.
2	Top N switch ports.		

Step 2 Select one of the following from the Variable list:

- Utilization—Sorts the interface number based on the utilization percentage. If the utilization percentage is less than 0.1%, the percentage is displayed as 0.0% in the chart.
- Dropped Events—Sorts the interface number based on the number of dropped events.
- Bytes—Sorts the interface number based on the number of bytes.
- Packets—Sorts the interface number based on the number of packets.
- Broadcast Pkts—Sorts the interface number based on the number of broadcast packets.
- Multicast Pkts—Sorts the interface number based on the number of multicast packets.
- CRC Align Errors—Sorts the interface number based on the number of CRC Align errors.
- Undersize Pks—Sorts the interface number based on the number of undersize packets.
- Oversize Pks—Sorts the interface number based on the number of oversize packets.
- Fragments—Sorts the interface number based on the number of fragments.
- Jabbers—Sorts the interface number based on the number of jabbers.
- Collisions—Sorts the interface number based on the number of collisions.



Tip

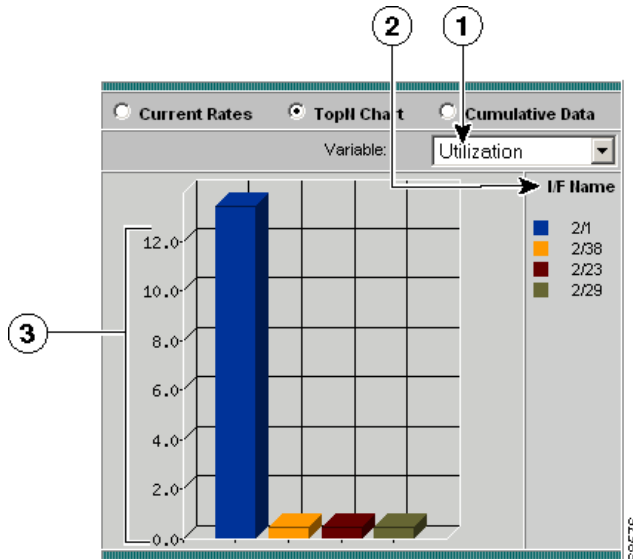
To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the Top N Interface Stats Chart

The Interface Stats Top N Chart enables you to view the various data collected for each interface in a graphical format. The displayed information represents the data collected per second over the last time interval.

- Step 1** Click the TopN Chart radio button.
The [Top N Interface Stats Chart](#)(Figure 4-29) is displayed.

Figure 4-29 Top N Interface Stats Chart



1	Variable list.	3	Variable value (per second) for each interface.
2	Top N interfaces.		

Step 2 Select one of the following from the Variable list:

- In Packets/s—Sorts the interface number based packets collected per second.
 - Out Packets/s—Sorts the interface number based on the number of packets sent out per second.
 - In Bytes/s—Sorts the interface number based on the number of bytes collected per second.
 - Out Bytes/s—Sorts the interface number based on the number of bytes sent out per second.
 - In Non-Unicast Pkts/s—Sorts the interface number based on the number of non-unicast packets collected per second.
 - Out Non-Unicast Pkts/s—Sorts the interface number based on the number of non-unicast packets sent out per second.
 - In Errors/s—Sorts the interface number based on the number of errors collected per second.
 - Out Errors/s—Sorts the interface number based on the number of errors sent out per second.
 - In Discards/s—Sorts the interface number based on the number of discards collected per second.
 - Out Discards/s—Sorts the interface number based on the number of discards sent out per second.
-



Tip

To turn off auto refresh, deselect the Auto Refresh check box.

Viewing the Port Stats Cumulative Data Table

The Port Stats Cumulative Data table allows you to view the various data collected for the switch. The information displayed represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences for All Users” section on page 3-55](#).

-
- Step 1** Click the Cumulative Data radio button.
The [Port Stats Cumulative Data Table \(Table 4-43\)](#) is displayed.

Table 4-43 Port Stats Cumulative Data Table

Field	Description
Port Name	Port number.
Dropped Events	Number of dropped events.
Bytes	Number of bytes collected on the port.
Packets	Number of packets collected on the port.
Broadcast Packets	Number of broadcast packets collected.
Multicast Packets	Number of multicast packets collected.
CRC Align Errors	Number of CRC align errors collected.
Under size packets	Number of collected packets under 64 octets long.
Over size Packets	Number of collected packets over 1518 octets long.
Fragments	Number of collected packets collected that were less than 64 octets long and had bad Frame Check Sequence (FCS).
Jabbers	Number of collected packets collected that were longer than 1518 octets long and had bad Frame Check Sequence (FCS).
Collisions	Number of collected collisions on the Ethernet segment.

- Step 2** To refresh the data in the table, click **Refresh**.
- Step 3** Enter the port name to filter in the Port Name text box, then press **Filter**.
The specified port name is displayed.

Viewing the Interface Stats Cumulative Data Table

The Interface Stats Cumulative Data table enables you to view the various data collected for the router. The displayed information represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences for All Users”](#) section on page 3-55.

- Step 1** Click the Cumulative Data radio button.
The [Interface Stats Cumulative Data Table](#) (Table 4-44) is displayed.

Table 4-44 Interface Stats Cumulative Data Table

Field	Description
Interface	Interface number.
In Packets/s	Number of packets collected per second.
Out Packets/s	Number of packets sent out per second.
In Bytes/s	Number of bytes collected per second.
Out Bytes/s	Number of bytes sent out per second.
In Non-Unicasts/s	Number of non-unicasts collected per second.
Out Non-Unicasts/s	Number of non-unicasts sent out per second.
In Discards/s	Number of discards collected per second.
Out Discards/s	Number of discards sent out per second.
In Errors/s	Number of errors collected per second.
Out Errors/s	Number of errors sent out per second.

- Step 2** To refresh the data in the table, click **Refresh**.
- Step 3** Enter the interface name to filter in the Filter text box, then click **Filter**.
The specified interface name is displayed.
-

Viewing Interface Details

To view packet distribution details on a specific interface, click the interface number in the Interface column. The detail window displays with a chart that shows the total packet distribution on the specified interface.

