



Monitoring and Analyzing Traffic

Cisco Prime Network Analysis Module, or Prime NAM, provides several dashboards and tools to help you to monitor and analyze your network traffic data. Prime NAM starts collecting data once your network device's IP address is shared with the NAM. You can view the monitor dashboard, analyze traffic using various views, troubleshoot suspicious traffic using the capture tool, and decode capture sessions without any additional configuration on your part.

This chapter provides information about monitoring your network traffic and analyzing the information presented.

This chapter contains the following sections:

- [How To Make Dashboards Work for You, page 3-2](#)
- [Troubleshooting Application Slowness, page 3-3](#)
- [Using Traffic Summary, page 3-4](#)
- [Using Response Time Summary, page 3-5](#)
- [Using Site Summary, page 3-6](#)
- [Using Alarm Summary, page 3-7](#)
- [Analyzing Traffic, page 3-9](#)
- [Optimizing WAN, page 3-16](#)
- [Measuring Response Time, page 3-18](#)
- [Analyzing Device Interface and Health Data, page 3-23](#)
- [Analyzing Media, page 3-30](#)
- [Using the NAM Application Programming Interface, page 3-35](#)

If you want to customize Prime NAM to use more advanced configurations such as sites and filtering, see [Customizing Cisco Prime NAM, page 7-1](#).

How To Make Dashboards Work for You

You can view traffic in a *summary* view (available from the **Monitor** menu) which you can then further analyze using the more in-depth *analysis* view (available from the **Analyze** menu).

The Monitor dashboards allow you to view graphic depictions of network traffic, application performance, site performance, and alarms at a glance. From there, you can isolate one area, for example an application with response time issues, and then drill down to the Analyze dashboard for further investigation.

The following are some of the configuration tasks that enhance NAMs ability to provide more traffic details on dashboards:

- Turn on deep application classification in order to identify applications regardless of the ports on which the applications may be running. To enable deep packet inspection, see [Adding More Detail into Dashboard and Application Reports, page 7-46](#). For an example of how to troubleshoot using deep packet inspection, see [Troubleshooting Application Slowness, page 3-3](#).
- To understand how to use filters to easily find information and significantly change what you view in the dashboards, see [Filtering Traffic for Viewing on the Dashboards, page B-4](#) and [Filtering Data Using Global Search, page B-5](#).
- To make your custom application traffic more visible on the dashboards and reports, add HTTP URL or Server IP/Port definitions. See [Creating Deeper Visibility Into Application Traffic, page 7-48](#)

For more details about when or why to use specific dashboards, see [How Do I Solve My Problem?, page 3-2](#).

How Do I Solve My Problem?

This section includes a table that provides various problems you can solve with specific dashboards, as well as what details you might want to know and what dashboards are associated with that data.

What Problem Needs Solving	Why Do I Need to Know This	Where to Go
My application is slow	Dashboards provide multiple entry points into data.	Troubleshooting Application Slowness, page 3-3
My phone quality is poor.	NAM detects and computes Mean Opinion Scores (MOSs) for VoIP calls transported through Real Time Protocol (RTP) streams.	Using Site Summary, page 3-6 see Top N Sites by Average MOS and RTP Streams
Has my server reached capacity?	You can filter by data source and analyze host details	Filtering Traffic for Viewing on the Dashboards, page B-4 and Filtering Data Using Global Search, page B-5
I want more or specific details in my captures	Use various filters to select what gets included in your captures	Understanding Global Capture Settings, page 4-17 and Configuring Hardware Filters, page 4-9

What Problem Needs Solving	Why Do I Need to Know This	Where to Go
Is my interface overloaded?	View Analyze > Managed Device > Interface to see list of all interfaces and errors or discards on each interface.	Analyzing Device Interface and Health Data, page 3-23
I'm seeing a lot of unexpected or excessive applications traffic	This may be tied to the occurrence of multiple Unknown applications. video traffic for example	Configuring Application Classification, page 7-46
I want to identify my homegrown applications	Your traffic visibility into your application can be improved by adding your custom application details so it can be classified	Creating Deeper Visibility Into Application Traffic, page 7-48
How do get notified before a problem occurs?	Set up alarms and thresholds to notify you via email.	Setting Up Alarms and Alarm Thresholds, page 7-28

Troubleshooting Application Slowness

This section contains a sample workflow that describes one way to use Prime NAM to help troubleshoot common network slowness.

This example concentrates on how to troubleshoot application performance issues that stem from using common server applications (such as HTTP or Sharepoint).



Tip

This case applies to any instance where an application is suspected of causing network latency.

Before You Begin

NAM assumes that your system time is synchronized. If you do not have the time synchronized between the NAM and the standard time source outside the NAM, then you may see either incorrect data or no data. If you suspect inaccurate timestamps, you need to set up the System Time so that NAM data presentation is accurate. For instructions on how to set system time by choosing **Administration > System > System Time**, see [Synchronizing Your System Time, page 5-5](#).

To determine what may be causing network slowness for the remote desktop users:

- Step 1** In order to see Layer 7 application details, ensure deep packet inspection is enabled. This is the system default on new installations. To confirm this setting, choose **Setup > Classification > Applications Settings** and ensure the Deep Packet Inspection checkbox is selected. If not, see [Adding More Detail into Dashboard and Application Reports, page 7-46](#) for instructions.
- Step 2** Choose **Analyze > Application Traffic** in order to find the network devices that use a specific protocol or application.
 - a. In the Interactive Report Filter select the name of your application (for example, Sharepoint) as the Application option in order to collect network traffic details for that application only. If you do not see your application, you may need to download the latest protocol pack.
 - b. You can also customize the time range to ensure that your data collection provides enough data or focuses on specific points of time that have heavy traffic.

If you do not see any data, select a different time range in the filter and submit the search again in order to locate the surge traffic.

Step 3 Use the zoom/pan chart slider at the bottom of the Application Traffic chart in order to focus in on those details that are most important to you.

Focus on the traffic surges in the chart in order to identify the participating servers and the remote clients.

Step 4 Use the Top Hosts Traffic In and Out charts in order to drill down for more bandwidth details.

- a. Select the server with the most traffic and review the maximum and average bandwidth used by your application in order to pinpoint the source of the issue.

For the select server, assess the amount of traffic in order to view:

- A breakdown by each site
- Conversations by individual users

Step 5 Assess if there is enough capacity on the link connecting the site to the data center in order to determine if this might be part of the problem. Since this is out of this product's scope, we recommend you use other applications to perform this task.

Step 6 If your network capacity is limited, for example, a 256 Kbps link shared across multiple applications and there is a requirement to support multiple clients, consider the following options:

- Apply a control mechanism, for example Quality of Service policies
- Upgrade the link so that it can handle a higher bandwidth

Using Traffic Summary

The Traffic Summary Dashboard allows you to view the Top N Applications, Top N Application Groups, Top N Hosts (In and Out), IP Distribution, Top N DSCP, and Top N Encapsulations being monitored on your network. It provides automatic monitoring of traffic from all potential data sources (for example, SPAN, NetFlow, and WAAS). You can get to the Traffic Summary Dashboard by going to **Monitor > Overview > Traffic Summary**.

You can use the Interactive Report on the left to filter the information for a particular Site, Data Source, encapsulations, or reporting time distribution. You can specify just one type of criteria and leave the others blank, or specify all of them. You can also choose to view the rate or cumulative data from the Interactive Report. To set a system preference for bytes instead of bits, go to **Administration > System > Preferences**.

When you log into Prime NAM for the first time, the default view will be the Traffic Summary dashboard, and the top data source is selected by default.

[Table 3-1](#) provides an at-a-glance summary of the Traffic Summary dashboard. For each chart described below, you can left-click on any colored bar to get to a context menu, with which you can get more detailed information about that item. You can also place your cursor over the colored bar to see the number of bits per second collected or the total bits over the last time interval. To toggle your view from chart to table, select the icon under the table.

Table 3-1 Traffic Summary At-a-Glance

Basics	Chart	Description
View top application traffic rate or traffic volume, based on the Interactive Report filter selection (data rate or cumulative, respectively)	Top N Applications	This chart reports application-level (L7 payload) bits. If you left-click on a colored bar and choose Capture from the context menu, you can start a capture on this data (see Capturing and Decoding Packets, page 4-1 for more information). You can also select other options to view various application traffic details. See Analyzing Application Traffic, page 3-10 .
View traffic rate or volume for top application groups	Top N Application Groups	In the Interactive Report, you can select either <i>rate</i> or <i>cumulative</i> , where rate is the bits per second, and cumulative is the total number of bits.
View host activity	Top N Hosts (In and Out)	To get more specific details about the host activity, left-click on the colored bar and make a selection. If you left-click on a colored bar, you can select additional options for host activity data. See Analyzing Host Traffic, page 3-10 .
View IP protocol traffic	IP Distribution	Shows the percentages of bits being distributed to IP protocols (for example, IPv4 TCP).
View statistics for top DSCP aggregation groups	Top N DSCP	For more detail, hover over the colored bar or left-click to select Details option. See DSCP, page 3-12
View encapsulation traffic	Top N Encapsulations	In the Interactive Report, you can select a VLAN and filter specific encapsulation protocols from within this chart (including OTV, VxLAN, LISP, and others). You can also narrow your data by filtering on certain time ranges. The default time range is 15 minutes. See Encapsulation, page 3-12 .

**Tip**

To change from bits to bytes, choose **Administration > System > Preferences** and change the **Data displayed in** selection.

To see a chart in table format, use the Show Chart/Show Table toggle buttons on the bottom left corner of the chart.

When viewing the data as a Grid, the numbers are formatted according to what you have configured in **Administration > System > Preferences**. On that page, you can also configure the number of Top N entries you would like to display.

Using Response Time Summary

The NAM software provides response time measurements and various user-experience-related metrics, which are computed by monitoring and time-stamping packets sent from the user to the server providing services. These Application Response Time Metrics are available to view under the Response Time Summary Dashboard (**Monitor > Overview > Response Time Summary**).

After the NAM is started, these metrics will begin to populate automatically. When you first navigate to Response Time Summary dashboard, the top data source is selected by default. This dashboard shows you performance statistics for site, data source, encapsulation, and a specific amount of time.

Use the Interactive Report window on the left side of the window to change the parameters for the information displayed. To see a chart in table format, use the Show Chart / Show Table toggle button on the bottom right corner of the chart.

The dashboard charts will show you the following information:

- **Top N Applications by Transaction Time**

This chart displays the server response times for the applications in the site, data traffic source, VLAN, or site clients or servers you selected in the Interactive Report window. For example, a selection *http* would show you the average response time of HTTP servers seen in the traffic category you have selected in the Interactive Report window. The data displays in microseconds (μ), milliseconds, or seconds depending on your preference settings.

- **Top N Site-to-Site Network Time**

This chart displays the top network time between the client site and the server site in the category you selected. The data displays in microseconds (μ), milliseconds, or seconds depending on your preference settings.

- **Top N Servers By Server Response Time**

This chart allows you to see how well servers are performing, by showing you the server that has the longest response time (the item appearing at the top). The data is shown in microseconds.

- **Top N Servers By Bits (or Bytes)**

This chart displays the total bits or rate of traffic for the top servers. You can choose to display NAM data in either Bits or Bytes in **Administration > System > Preferences**.

- **Top N Clients By Transaction Time**

This chart displays the transaction time per client. The client with the highest response time appears on top. The data displays in microseconds (μ), milliseconds, or seconds depending on your preference settings.

- **Top N Clients By Bits (or Bytes)**

This chart displays the total bits or rate of traffic for the top clients.

Using Site Summary

The Site Summary Dashboard (accessed by choosing **Monitor > Overview > Site Summary**) will show you information about the sites in your network. You can use the Interactive Report on the left side of the window to change the information displayed. For more information about sites, see [Configuring Sites, page 7-41](#).

The charts displayed on the Site Summary dashboard are:

- **Top N Sites by Average Transaction Time**

This chart shows the average transaction time by site.

- **Top N Site Pairs by Traffic**

This chart shows top site to site traffic.

- **Top N Sites by Average MOS**

This chart shows sites that have the highest average Mean Opinion Score (MOS).

MOS will normally range from 1-5, denoting the perceived quality of the transmission, where 1 is the lowest perceived quality, and 5 is the highest perceived quality measurement. The MOS is weighted depending on the duration.

- **Top N Sites by Traffic**

This chart shows the sites that have the most traffic (which are the most active). It is a total of all the traffic sent or received for hosts that belong to the particular site, which means that this traffic includes intra-site traffic as well.

To see any of the charts in table format, use the Show Chart / Show Table toggle button on the bottom right corner of the chart.

Using Alarm Summary

The Alarm Summary Dashboard (accessed by choosing **Monitor > Overview > Alarm Summary**) will show you the top alarms occurring in the network.

To display network traffic information for a particular amount of time, use the Interactive Report on the left side of the window. The Severity Selector in the Interactive Report allows you to choose to view high severity alarms only, low severity alarms only, or both high and low severity alarms (these settings are configured under **Setup > Alarms > Thresholds**). You can also choose the desired amount of time from the Time Range drop-down menu, or you can customize the time range.

On any chart on the Alarm Summary Dashboard, you can click on a colored bar to see the Context menu, with which you can get more information.

If you do not set any alarms or thresholds, the Alarm Summary Dashboard will have no data. For information on setting up alarms and thresholds, see [Setting Up Alarms and Alarm Thresholds](#), page 7-28.



Note

You could see a count of two alarms for the same occurrence if:

- both the source and the destination are in the same site in the Top N Site - Host Pair chart.
- both the source and the destination are in the same site in the Top N Site chart.
- both the source and the destination are in the same site using the same application in the Top N Site - Application Pair chart.



Note

You will not have any data in Top N Site - Application and Top N Application if there is no threshold configured that involves an application (for example: Response Time threshold or Application threshold).

NetFlow Interface alarms are not related to any site; therefore, they will not appear on the four colored site alarm charts on the Alarm Summary dashboard. Instead, the New Alarms Raised and Last 50 Alarms tables at the bottom of this window will contain NetFlow Interface alarms raised.

The five charts displayed on the Alarm Summary dashboard are:

- **Top N Sites by Alarm Count**

This chart lists the top sites that have the most alarm triggers during the selected time range. The number of sites displays based on the maximum number you set in preferences. If no thresholds are configured, this chart contains no data. The number on the bottom of the chart is the alarm count.

You can configure thresholds under **Setup > Alarms > Thresholds**. You can configure the Top N entries under **Administration > System > Preferences**.

- **Top N Hosts by Site and Alarm Count**

This chart shows the number of alarm messages during the selected time range that are triggered for Hosts across all sites, by the Site - Host Pair.

- **Top N Applications by Alarm Count**

This chart shows the number of alarms during the selected time range for Applications across all sites.

- **Top N Applications by Site and Alarm Count**

This chart shows the most alarm triggers during the selected time range by the application and site pair.

- **New Alarms Raised**

The New Alarms Raised table shows you all alarms that occurred during the interval selected in the Interactive Report window. Some alarms may have been triggered outside of the time period, but may still be occurring.

- **Last 50 Alarms**

The Last 50 Alarms table shows you the alarms that occurred during the interval selected in the Interactive Report window. Some alarms may have been triggered outside of the time period, but may still be occurring. See [Table C-40](#).

Click **All Alarms** to display a separate window, which shows all the alarms from that particular time interval.

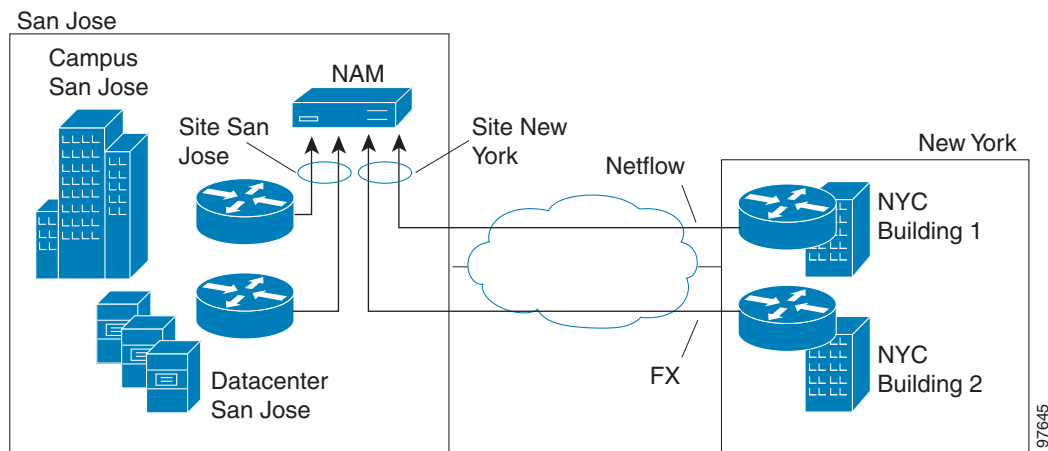
You can also use the Filter button, both in this window and the All Alarms window, to display only alarms that meet the criteria you enter.

Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment

In Prime NAM you can define a site, which enables you to aggregate and organize performance statistics. If you want to limit the view of your network analysis data to a specific city, a specific building, or even a specific floor of a building, you can use the sites function.

[Figure 3-1](#) shows a centralized NAM deployment analyzing multiple data sources from different locations in the network.

Figure 3-1 Site Level Aggregation



For this deployment, multiple sites can be created such as SanJose-Campus, SanJose-Datacenter, NewYork-NetFlow-Bldg1, and NewYork-WAAS-Bldg2. The data that does not match the site configuration will be displayed in the Default site. This helps to isolate the view and information for monitoring and troubleshooting so you can drill down to the specific area of interest.

You can also include multiple types of data sources in the site definition, and you can then get an aggregated view of all network traffic.

The predefined *Unassigned Site* makes it easy to bring up a NAM without having to configure user-defined sites. Hosts that do not belong to any user-defined site will automatically belong to the Unassigned Site.

You can create, view, or edit your sites by selecting **Setup > Network > Sites**. Unassigned sites cannot be changed.

The interactive dashboard can be used to drill down into either San Jose or New York sites to see Top applications, hosts, Encapsulations, DSCP, and application response time.

From each of the charts in the dashboard, you can access the context menu to further drill down to analyze data such as detailed application, host, and conversation traffic.

Analyzing Traffic

Prime NAM offers many ways to analyze your network traffic data using graphs, charts, and detailed views.

Use the links below to locate information about:

- [Analyzing Site Traffic, page 3-9](#)
- [Analyzing Application Traffic, page 3-10](#)
- [Analyzing Host Traffic, page 3-10](#)
- [NetFlow Interface Traffic Analysis, page 3-11](#)
- [DSCP, page 3-12](#)
- [Encapsulation, page 3-12](#)
- [URL Hits, page 3-12](#)
- [Detailed Traffic Analysis Views, page 3-13](#)
- [About Analyze Traffic Charts, page 3-15](#)

Analyzing Site Traffic

To show you the traffic level for a given site over a selected period of time:

-
- Step 1** Choose **Analyze > Traffic > Site**.
 - Step 2** To change the data to see the top application traffic coming into a specific site, out of a specific site, or all traffic within, coming in and moving out of that site, use the traffic selector buttons.
 - Step 3** To see site conversations about the conversation between sites to pinpoint specific applications or sites, select the Site Conversations button and choose filters from the Interactive Report to further pinpoint an application, data source, or time frame in question.

- Step 4** To view top applications transmitting and receiving traffic for the selected time period and drill down to collect more data utilizing capture data, real-time graphs, and application group detail), left click the Top N Application dashboard.
- Step 5** To see the criteria by which the NAM classifies the amount of application traffic on this site over this period of time, use the view Application Distribution graph. Hover over graph parts to view detailed information on speed and percentages or left-click a graph element for other menu options.
-

Analyzing Application Traffic

To show you the traffic level for a given application over a selected period of time:

- Step 1** Choose **Analyze > Traffic > Application**.
- Step 2** To see data for a different time interval (when *No data for select time interval displays*), click **Filter** on the Interactive Report, and expand the time range to allow more data to be viewed.
- Step 3** To focus in on a spike or area of interest, use the slider under the Application Traffic graph. Hover over the data points to see specific traffic details.
- Step 4** To see top application traffic details, click **Top Application Traffic** and choose filters from the Interactive Report to further pinpoint a data source, encapsulation method, or time frame in question.
- Step 5** To view top hosts transmitting and receiving traffic for the selected time period and drill down to collect more data utilizing capture data, real-time graphs, and application group detail), left-click a Top N Hosts graph element and select a specific task.
- Step 6** For example, select **Hosts Detail** to see the All Hosts window and the detailed information about all hosts. [Table C-38](#) describes the fields in this window.
- Step 7** To show the criteria by which the NAM classifies packets as that application, select one of the options under the Application Configuration. This is typically a list of TCP and/or UDP ports that identify the application. Some applications are identified by heuristic or other state-based algorithms. Then select **Configure Application** to configure specific applications in your network. For detailed instructions, see [Creating Deeper Visibility Into Application Traffic, page 7-48](#).
-

Analyzing Host Traffic

The Host Traffic Analysis window will show you at a quick glance the input and output of a particular host over a specified time range. It is available under the menu option **Analyze > Traffic > Host**. It will show you:

- Input and output traffic for the host
- Top N application activity of the host over the selected interval
- Total application usage distribution for the host
- Host Conversations—Shows detailed lists of all the conversations for a particular host.

Applications Detail

On the Top N Applications chart, you can left-click a colored bar to get the context menu, and choose **Applications Detail** to see the All Applications window and the detailed information about all applications. [Table C-31](#) describes the fields in this window.

NetFlow Interface Traffic Analysis

To view data collected for individual interfaces on a switch or router that is exporting NetFlow packets to the NAM, use the NetFlow Interface Analysis page. The displayed information represents the total data collected since the collection was created, or since the NAM was restarted.

Before You Begin

1. Ensure Auto-create is enabled for the NetFlow Data Export (NDE) data source. Once NDE data is sent to the NAM, an NDE data source is created.
2. Edit the NDE data source to enter SNMP credential information that allows the NAM to properly query the router/switch interface information. Go to **Setup > Traffic > NAM Data Sources**. For more information, see [Creating NetFlow Data Sources Using the Web GUI, page 7-16](#) or [Creating NetFlow Data Sources Using the CLI, page 7-16](#)
3. Go to NetFlow Interface Capacity page (**Setup > Network > NDE Interface Capacity**) to ensure all information is populated.

To view NetFlow Interface Analysis:

Step 1 Choose **Analyze > Traffic > NDE Interface**. The default view is Interface View.

Step 2 Select an interface from the Interface Selector to see traffic in the charts. Click the arrow icon to the left of the NetFlow data source name to display all interfaces, and then select an interface to see data for that interface.

When you go to the Group View tab, you see all interfaces and NetFlow data sources grouped into two static groups. You can select combinations of interfaces from each group and click **Submit**, and the charts on the right will sum up the metrics and display them for each group.



Note If the charts show no data, and you see a message “Interface needs to be selected,” you have not yet chosen an interface.

Once you have chosen the interface, you will see the following charts populated:

- Interface Traffic (Ingress % Utilization and Egress % Utilization)
- Top N Applications - Ingress
- Top N Applications - Egress
- Top N Hosts - Ingress
- Top N Hosts - Egress
- Top N DSCP Aggr - Ingress
- Top N DSCP Aggr - Egress

The interface speed can be entered manually through the Interface capacity table, or it can be auto configured if the SNMP settings for the NetFlow device are entered in data source table.

DSCP Detail

On the Top N DSCP Aggr - Ingress and Top N DSCP Aggr - Egress chart, left-click a colored bar to get the context menu. Choose **DSCP Detail** to see the All DSCP window. You can also get to this window by choosing **Analyze > Traffic > DSCP Traffic** from the menu and clicking the **All DSCPs** button on the right.

[Table C-37](#) describes the fields in this window.

DSCP

Differentiated services monitoring (DiffServ) is designed to monitor the network traffic usage of differentiated services code point (DSCP) values.

To monitor DSCP groups, you must configure at least one aggregation profile and one or more aggregation groups associated with each profile. For more information on configuring an aggregation profile, see [Configuring DSCP Groups, page 7-45](#).

You can monitor the DSCP information by going to **Analyze > Traffic > DSCP**. The data provided to you includes:

- Traffic volume over time for DSCP group
- Top N applications and application groups using that DSCP group
- Top N hosts transmitting and receiving traffic on that DSCP group

Encapsulation

You can analyze the encapsulation traffic collected by Prime NAM (for setup, see [Filtering Encapsulations, page 7-53](#)). This section contains the following use cases:

- Viewing Collected Encapsulation Data—see [Viewing Collected URLs, page 3-13](#)
- Filtering Various Encapsulations—see [Filtering a URL Collection List, page 3-13](#)

URL Hits

You can analyze the URLs collected by the NAM (for setup, see [Configuring URL Collections, page 7-57](#)).

This can help you determine what URLs are used in the network and then see what applications are affiliated with those URLs.

This section contains the following:

- [Viewing Collected URLs](#)
- [Filtering a URL Collection List](#)

Viewing Collected URLs

To view collected URLs and optionally create URL-based custom applications:

Step 1 Choose **Analyze > Traffic > URL Hits**.

The URL Hits Window displays with the collected URLs.



Note Only one URL collection can be active at one time. The data source is for information only.

Step 2 To create a URL-based custom application, click **Create URL-Based Application**.

For details on the URL-Based Applications window, see [Table C-27](#).

Filtering a URL Collection List

To filter a URL collection list:

Step 1 From the drop-down list in the URLs Window (**Analyze > Traffic > URL Hits**), choose which part of the URL to filter:

- **URL**—You can filter on any part of the URL
- **Host**—This filter applies only to the host part of collected URLs.
- **Path**—This filter applies only to the path part of the collected URLs
- **Arguments**—This filter applies only to the argument part of the collected URLs.

Step 2 Enter filter string.

Step 3 Click **Filter** to apply the filter.



Note To remove any display filter and show all URLs collected, click **Clear**.

Detailed Traffic Analysis Views

Prime NAM offers several detailed traffic analysis views which allow you to analyze the following data:

- [Sites Detailed Views, page 3-14](#)
- [Site Conversations Detailed Views, page 3-14](#)
- [Applications Detailed Views, page 3-14](#)
- [Application Groups Detailed Views, page 3-14](#)
- [Application Traffic By Hosts Detailed Views, page 3-14](#)
- [Top Application Traffic Detailed Views, page 3-14](#)
- [Hosts Detailed Views, page 3-15](#)

- [Host Conversations Detailed Views, page 3-15](#)
- [DCSPs Detailed Views, page 3-15](#)

Sites Detailed Views

Displays data for each site (including all unassigned sites) and see packet per second and bits per second details. Use the Interactive report filter to pinpoint specific attributes. There are no filter time limits for this data.

Site Conversations Detailed Views

Displays site traffic for all or selected sites. To pinpoint site traffic data between two devices, select the Interactive Report Filter.

Applications Detailed Views

To view the All Applications window and the detailed information about all application and filter on specific applications or other filter attributes, use the Interactive Report filter.

Application Groups Detailed Views

To see the All Application Groups window and the detailed information about all application groups, left-click a colored bar on the Top N Application Groups chart to get the context menu, and choose **Applications Groups Detail**. [Table C-32](#) describes the fields in the All Applications window.

Application Traffic By Hosts Detailed Views

Shows the traffic for a given application broken out by individual hosts using the application. You may specify the time period to view, as well as the application, site (optional), data source (optional), and VLAN (optional).

The NAM only supports a maximum Time Range of one hour filter for the Host Conversations, RTP Streams, Voice Calls Statistics, Calls Table, and RTP Conversations.

Top Application Traffic Detailed Views

Shows the top applications by traffic rate over a selected time and for the specified site and/or data source.

[Top Application Traffic Detailed Views](#) shows you all of the applications that have been running for the time period interval. The color-coded legend shows you what the applications are running.

The Display Other check box (which is underneath the Top Application Traffic heading) corresponds to the data for the applications not in the N list. If you check this check box, the chart will display the *Other* data in addition to the data for the N number of applications.

If you place your cursor over any of the data points, you will get more details about the exact values for each of the applications that are running.

Hosts Detailed Views

Shows the input and output of a particular host over time. Use the **Filter** button in the Interactive Report (left side of the window) to change the parameters of the information displayed.

Host Conversations Detailed Views

Shows detailed lists of all the conversations for a particular host.

You can view the following data:

- A table of hosts which are sending and receiving packets to the selected host, along with application, encapsulation, and traffic rate information.
- A breakout of application usage for the selected host.

Use the **Filter** button in the Interactive Report (left side of the window) to change the parameters of the information displayed.

The NAM only supports a maximum time range of one hour filter for the Host Conversations, RTP Streams, Voice Calls Statistics, Calls Table, and RTP Conversations.

Encapsulations Detailed Views

To show a detailed analysis of the various encapsulation layers, bits, and packet data, choose **Analyze > Traffic > Detailed Views > Encapsulations**.

Use the **Filter** button in the Interactive Report to change the information displayed and target data.

DCSPs Detailed Views

Shows a detailed analysis of all the network traffic usage of differentiated services code point (DSCP) values, choose **Analyze > Traffic > Detailed Views > DSCPs**.

Use the **Filter** button in the Interactive Report to change the information displayed and target data.

For details about setting your TOS key and the implications of doing so, see [Customizing System Preferences, page 5-10](#).

About Analyze Traffic Charts

The charts available under the **Analyze** menu show statistics that occur over time. You can use the Zoom/Pan feature, with which you can drag the beginning or end to change the time interval or distribution.

The time interval change on the zoom/pan chart will affect the data presented in the charts in the bottom of the window. The zoom/pan time interval also affects the drill down navigations; if the zoom/pan interval is modified, the context menu drill downs from that dashboard will use the zoom/pan time interval.



Note

In a bar chart which you can zoom/pan, each block represents data collected during the previous interval (the time stamp displayed at the bottom of each block is the end of the time range). Therefore, you may have to drag the zoom/pan one block further than expected to get the desired data to populate in the charts in the bottom of the window.

Optimizing WAN

Prime NAM can provide insight into WAN Optimization offerings that compress and optimize WAN traffic for pre- and post-deployment scenarios. This is applicable for optimized and passthru traffic.

WAN Optimization tasks include:

- [Ensuring WAN Optimization, page 3-16](#)
- [Analyzing Traffic for Optimization Using the Top Talkers Detail, page 3-17](#)
- [Analyzing Application Performance after WAAS Optimization, page 3-17](#)
- [Monitoring WAAS Traffic Across Multi-Segments, page 3-18](#)
- [Monitoring WAAS Single-Segment Traffic, page 3-18](#)

**Note**

To monitor the WAAS data, you must select the correct WAAS data source.

Ensuring WAN Optimization

In order to ensure that your applications are performing optimally and your WAN is optimized:

-
- Step 1** To identify sites with application performance challenges, choose **Monitor > Site Summary**.
If you do not have sites identified, you can use the Unknown site category or to learn about how to create sites, see [Configuring Sites, page 7-41](#).
- Step 2** Look for sites with the highest average transaction time and highest traffic rate.
- Step 3** To quantify the application performance:
- a. Choose **Monitor > Response Time Summary**.
 - b. Set up a filter that targets key areas such as a specific location and different time ranges (one day and one week). This allows you to focus in on exactly the data you want to analyze.
 - c. Right-click the application with the highest server response time and choose **Analyze Application Response Time**.
 - d. Specify a filter time range using the Interactive Filter. We recommend viewing data over a one day range to allow for possible peak times.
 - e. Identify applications with poor performance and quantify the response time by network time, server response time, and data transfer time.
- Step 4** To validate the impact of WAN optimization:
- a. Choose **Analyze > WAN optimization > Application Performance Analysis**.
 - b. Minimize WAN Opt Impact analysis filter (on the left pane).
 - c. View the effect of optimizing one of your applications (for example, to determine if your HTTP browser has lower transaction times and thus better end-client experience, lower compression ratios for better utilization of the WAN, and fewer average concurrent connections for better utilization of server through connection reuse).
- Step 5** To perform ongoing monitoring of WAN optimization and troubleshoot WAN optimized traffic:
- a. Choose **Analyze > Conversation Multi Segment**.

- b. View a detailed breakdown of latency and bandwidth measures for the server, WAN, and client network segments.

Analyzing Traffic for Optimization Using the Top Talkers Detail

While you are in the process of deploying WAAS devices, you can get data to assist in the WAAS planning and configuration.

This window allows you to display response time and concurrent connections for the top Application, Network Links, Clients, and Servers from WAN data sources before WAAS optimization.

To analyze traffic for optimization using the Top Talkers Detail:

- Step 1** Choose **Analyze > WAN Optimization > Top Talkers Detail** and filter data using the Interactive Report window to select the traffic you want to analyze for optimization.

If the data source is from SPAN or WAAS, it does not include the packet header; if the data source is NetFlow, it will include the packet header.



Note You can choose to display NAM data in either Bits or Bytes in **Administration > System > Preferences**.

Based on the results, you can then configure the WAAS products to optimize your network.

Analyzing Application Performance after WAAS Optimization

WAN optimization allows you to display response time, concurrent connections, traffic volume and compression ratio from WAN data sources after WAAS optimization. To analyze the WAAS traffic, choose **Analyze > WAN Optimization > Application Performance Analysis**.

The tasks associated with this analysis include:

- [Comparing Transaction Time \(Client Experience\)](#), page 3-17
- [Comparing Traffic Volume and Compression Ratio](#), page 3-18
- [Planning Capacity Using Average Concurrent Connections \(Optimized vs. Passthru\)](#), page 3-18
- [Optimizing Usage Using Multi-Segment Network Time \(Client LAN - WAN - Server LAN\)](#), page 3-18

Comparing Transaction Time (Client Experience)

To compare client transaction time, choose **Analyze > WAN Optimization > Application Performance Analysis** and using this chart. It displays the average client transaction time. One line represents pass-through traffic (in which optimization is turned off), and the second represents optimized traffic. After setting up optimization for a certain period, you can compare the two lines and see where the vertical drop in the chart occurs. Depending on your Response Time Display unit preference setting, the data may display in microseconds, milliseconds, or seconds.

Comparing Traffic Volume and Compression Ratio

You can compare the bandwidth reduction ratio between the number of bits before compression and the number of bits after compression using this chart.

Planning Capacity Using Average Concurrent Connections (Optimized vs. Passthru)

You can use the number of concurrent connections during a specified time to assist with peak and off-period identification. This information can be used for capacity planning.

Optimizing Usage Using Multi-Segment Network Time (Client LAN - WAN - Server LAN)

You can use the network time between the multiple segments to identify lagging performance issues. The data is shown in microseconds.

Monitoring WAAS Traffic Across Multi-Segments

To monitor WAAS traffic across multiple segments use the Conversation Multiple Segments window. This window provides a correlation of data from different data sources, and allows you to view and compare response time metrics from multiple WAAS segments (data sources). You can access this window from **Analyze > WAN Optimization > Conversation Multi-segments**.

The window shows network time, server response time, and other metrics of the selected server or client-server pair from applicable segments. The relevant metrics from all segments are combined into one row per client-server conversation.

Monitoring WAAS Single-Segment Traffic

To monitor WAAS traffic across a single segment use the data in the Conversation Single-Segments window to see data from different data sources, and view and compare response time metrics from different WAAS segments (data sources). You can access this window from **Analyze > WAN Optimization > Conversation Single-Segment**.

The window shows network time, server response time, and other metrics of the selected server or client-server pair (one row per segment).

Measuring Response Time

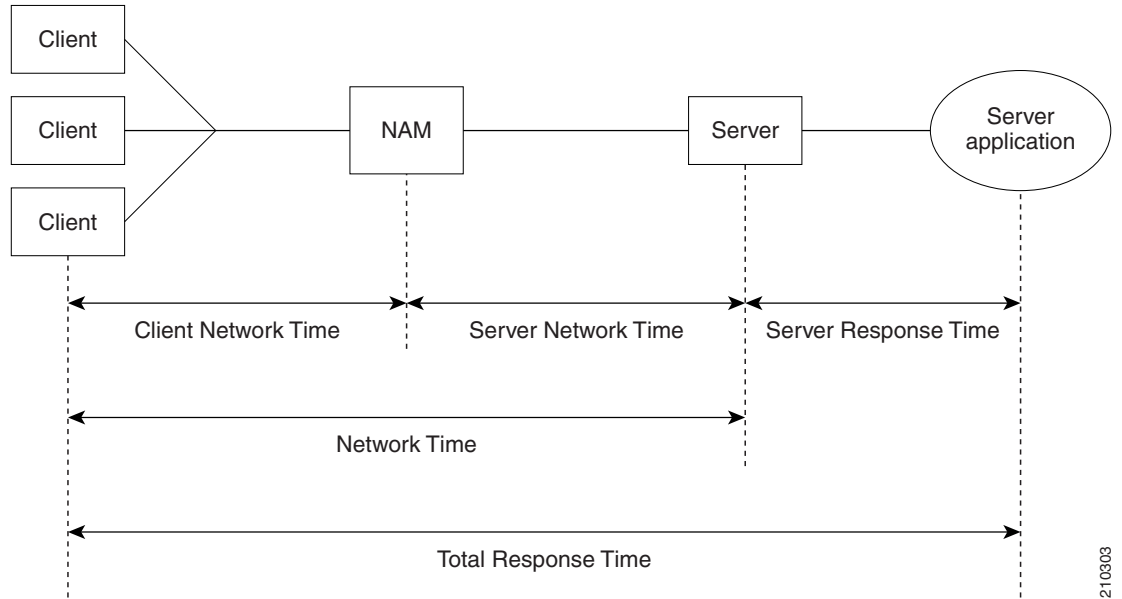
The NAM monitors TCP packet flow between client and server, and measures response time data to provide more visibility into application response times (ART) and network latency. Prime NAM response time monitoring provides end-to-end response times to help you locate possible network and application delays.

**Note**

Prime NAM software supports IPv6 for response time monitoring.

You can set up the NAM to measure network time, client response time, server response time, and total transaction time to improve application performance. Figure 3-2 shows the various points in network packet flow where the NAM gathers data and the trip times you can monitor. This is one example that represents only a subset of measurements.

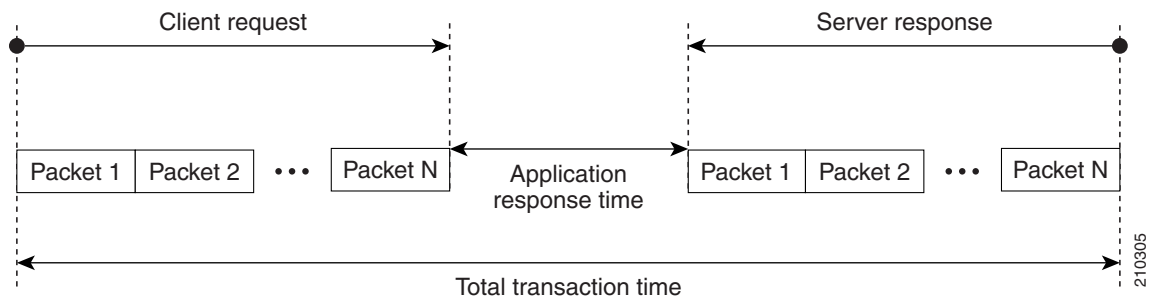
Figure 3-2 NAM Application Response Time Measurements



210303

Figure 3-3 shows a representation of total transaction time as opposed to application response time.

Figure 3-3 Transaction Time versus Response Time Measurements



210305

Table C-33 lists and describes the ART metrics measured by Prime NAM.

Application Response Time Metrics are available on the response Response Time Summary Dashboard (**Monitor > Response Time Summary**), which allows you to see a summary view of the data.

To analyze Response Time data over time, use the selections found under **Analyze > Response Time**:

- [Application Response Time, page 3-20](#)
- [Network Response Time, page 3-20](#)
- [Server Response Time, page 3-21](#)

- [Client Response Time](#), page 3-21
- [Client-Server Response Time](#), page 3-21

When you select **Analyze > Response Time > Detailed Views**, you will be able to select one of the following, each of which contains detailed lists of the response events.

- [Server Application Responses](#), page 3-21
- [Server Application Transactions](#), page 3-21
- [Server Network Responses](#), page 3-22
- [Client-Server Application Responses](#), page 3-22
- [Client-Server Application Transactions](#), page 3-23
- [Client-Server Network Responses](#), page 3-23

Application Response Time

The Application Analysis window allows you to view the performance of a particular application over time. It is accessed from **Analyze > Response Time > Application**.

The Transaction Time chart shows you the average transaction time for the application you have selected. It is broken down into three components: Network Time, Server Response Time, and Data Time.

The Other Metrics chart allows you to see information over time after you have selected the desired metrics from the Metric Group 1 and Metric Group 2 drop-down.

Next are the Top Clients and Top Servers charts. These show you the clients and servers with the most bits of traffic for the chosen application.



Note You can choose to display NAM data in either Bits or Bytes in **Administration > System > Preferences**.

Network Response Time

After you have selected a client site and a server site, the chart will show you the transaction time of the network link between the client site and server site. It is accessed from **Analyze > Response Time > Network**.



Note If you do not specify any application, the chart will show the network time instead of transaction time.

The Other Metrics chart allows you to see information about the network link between sites, after you have selected the desired metrics from the Metric Group 1 and Metric Group 2 drop-down.

The Top Clients and Top Servers charts show you the top clients and servers that are communicating through the network link (in bits or bytes).

Server Response Time

Choose the Client Site and Server Site from the Interactive Report on the left, and enter the IP address for the server that you want to analyze. The Server Transaction Time Composition chart will display the network time, server response time, data time, and transaction time.

The Other Metrics chart allows you to see information about the server performance after you have selected the desired metrics from the Metric Group 1 and Metric Group 2 drop-down.

Top Client shows you top client talking to the server you have selected; Server Top Clients Sites shows the top client sites (traffic bits).



Note You can choose to display NAM data in either Bits or Bytes in **Administration > System > Preferences**.

Client Response Time

After entering the client IP address and application in the Interactive Report Filter, you can analyze the transaction time of that client in the Client Transaction Time Composition chart.

The Other Metrics chart allows you to see client performance over time after you have selected the desired metrics from the Metric Group 1 and Metric Group 2 drop-down.

The Clients Top Applications chart show you the applications being used the most by the client selected, and the Top Servers chart show you the servers being used most by the client.

Client-Server Response Time

After you enter the client IP address and server IP address in the Interactive Report, you can analyze the transaction times between the client and server you have selected in the Client-Server Transaction Composition Over Time chart.

The Other Metrics chart allows you to see Client-Server transaction information after you have selected the desired metrics from the Metric Group 1 and Metric Group 2 drop-down.

Server Application Responses

The Server Application Responses Table displays when you choose **Analyze > Response Time > Detailed Views > Server Application Responses**.

If you click on a row of data, you can then choose **Response Time Details** to see more information.

[Table C-41](#) provides definitions of each field of the Server Application Responses window.

Server Application Transactions

The Server Application Transaction window displays when you select **Analyze > Response Time > Detailed Views > Server Application Transactions**.

The Server Application Transactions window provides a summary of the server application transaction response times (ART) per server application displaying the server IP address, application used, and minimum, average, and maximum response times for the following:

- Application Response Time
- Data Transfer Time
- Retransmit Time
- Round Trip Time

**Note**

NAM uses the TCP three-way handshake to calculate network delay. If there are no new TCP connections during the polling interval, the NAM GUI displays a dash (-) for the delay value indicating there is no delay data for that interval.

[Table C-42](#) provides definitions of each field of the Server Application Transactions window.

Server Network Responses

The Server Network Responses window shows the network connectivity and responsiveness between the server and the switch. It is located at **Analyze > Response Time > Detailed Views > Server Network Responses**.

**Note**

NAM uses the TCP three-way handshake to calculate network delay. If there are no new TCP connections during the polling interval, the NAM GUI displays a dash (-) for the delay value indicating there is no delay data for that interval.

[Table C-43](#) provides definitions of each field of the Server Network Response Times window.

Client-Server Application Responses

To view the Client-Server Application Responses window, choose **Analyze > Response Time > Detailed Views > Client-Server Application Responses**.

The Client-Server Application Responses window displays. [Table C-34](#) provides definitions of each field of the Client-Server Application Responses window.

**Note**

NAM uses the TCP three-way handshake to calculate network delay. If there are no new TCP connections during the polling interval, the NAM GUI displays a dash (-) for the delay value indicating there is no delay data for that interval.

Client-Server Application Transactions

The Client-Server Application Transactions window provides a summary of the server application transaction response times (ART) per server application displaying the server IP address, application used, and minimum, average, and maximum response times for the following:

- Application Response Time
- Data Transfer Time
- Retransmit Time
- Round Trip Time

**Note**

NAM uses the TCP three-way handshake to calculate network delay. If there are no new TCP connections during the polling interval, the NAM GUI displays a dash (-) for the delay value indicating there is no delay data for that interval.

The Client-Server Application Transaction window displays when you click **Analyze > Response Time > Detailed Views > Client-Server Application Transactions**. You can also view the TopN Chart to view the most active network.

[Table C-35](#) provides definitions of each field of the Client-Server Application Responses window.

Client-Server Network Responses

The Client-Server Network Responses window shows information about network connectivity (also known as network flight time) between servers and clients.

To view the Client-Server Network Responses window, choose **Analyze > Response Time > Detailed Views > Client-Server Network Responses**.

NAM uses the TCP three-way handshake to calculate network delay. If there are no new TCP connections during the polling interval, the NAM GUI displays a dash (-) for the delay value indicating there is no delay data for that interval.

[Table C-36](#) describes the fields of the Server-Client Network Response Time window.

Analyzing Device Interface and Health Data

You can view interface information and system health data using the **Analyze > Managed Device** window. The menu selections for analyzing Managed Devices are:

- [Viewing Interface Information, page 3-23](#)
- [Viewing Health Data, page 3-24](#)

Viewing Interface Information

You can view the following interface information:

- [Interfaces Stats Table, page 3-24](#)
- [Interface Statistics Over Time, page 3-24](#)

Interfaces Stats Table

To view packet distribution details on the interfaces, choose **Analyze > Managed Device > Interface**. The Interfaces Stats table displays and shows the total packet distribution on all interfaces. Depending on the interface chosen, the chart below the table refreshes with that information. Use the Interactive Report and the Filter button on the left to change the time range displayed. The Discards and Errors are measured in packets per second.

Interface Statistics Over Time

When you select an interface in the Interface Statistics Table, the statistics for that interface updates in the graph below the Interface Statistics Table.

You can check the check boxes for the information you would like displayed in the graph:

- Bits: In Bits, Out Bits
- Packets: In Packets (inUcastPkts + inNUcastPkts), Out Packets (outUcastPkts + outNUcastPkts)
- Discards: In Discards, Out Discards
- Errors: In Errors, Out Errors



Note You can choose to display NAM data in either Bits or Bytes in **Administration > System > Preferences**.

Viewing Health Data

You can use the NAM to view system health data. To view system health data collected for the switch or router, choose **Analyze > Managed Device > Health** from the menu.

For more details on the options available in each windows, see:

- [Switch Health Options, page 3-24](#)
- [Router Health Options, page 3-28](#)



Note This section applies to all NAM platforms *except* the NAM-NX1.

Switch Health Options

For a switch, the Health window is displayed with a drop-down menu that provides the following options:

- [Chassis Health, page 3-25](#)
- [Chassis Information, page 3-25](#)
- [Crossbar Switching Fabric, page 3-26](#)
- [Ternary Content Addressable Memory Information, page 3-27](#)

Chassis Health

The Chassis Health window displays two real-time graphs: CPU usage and Backplane Utilization.

CPU usage

CPU type

- Usage for last 1 minute (%)
- Usage for last 5 minutes (%)

Backplane Utilization

- Peak %
- Peak Time (For example: Mon October 1 2007, 15:26:55)

The Health window also displays a matrix with the following information:

- Minor Alarm (on, off)
- Major Alarm (on, off)
- Temperature Alarm (on, off)
- Fan Status (other, ok, minorFault, majorFault, unknown)

Table 3-2 Chassis Memory Information

Column	Description
Memory Type	Type of memory including DRAM, FLASH, NVRAM, MBUF, CLUSTER, MALLOC.
Used	Number of used MB for a particular memory type.
Free	Number of free MB for a particular memory type.
Largest Free	Number of largest contiguous free MB for a particular memory type.

Chassis Information

Table 3-3 describes the Chassis Information window.

Table 3-3 Chassis Information

Field	Description
Name	Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.
Hardware	A textual description which should contain the manufacturer's name for the physical entity and be set to a distinct value for each version or model of the physical entity.
Backplane	The chassis backplane type.
Supervisor Software Version	The full name and version identification of the system's software operating-system and networking software.
UpTime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
Location	The physical location of this node.

Table 3-3 Chassis Information (continued)

Field	Description
Contact	The textual identification of the contact person for this managed node and information on how to contact this person.
Modem	Indicates whether the RS-232 port modem control lines are enabled.
Baud rate	The baud rate in bits per second of the RS-232 port.
Power Supply	Description of the power supply being instrumented.
Power Supply Type	The power supply source: <ul style="list-style-type: none"> • unknown • ac • dc • externalPowerSupply • internalRedundant
Power Supply Status	The current state of the power supply being instrumented. <ul style="list-style-type: none"> 1: normal 2: warning 3: critical 4: shutdown 5: notPresent 6: notFunctioning
Power Redundancy Mode	Power Redundancy Mode: <p>The power-supply redundancy mode.</p> <ul style="list-style-type: none"> 1: not supported 2: redundant 3: combined
Power Total	Total current available for FRU usage. <p>When Redundancy Mode is redundant, the total current available will be the capability of a power supply with the lesser power capability of the two power supplies.</p> <p>When Redundancy Mode is combined, the total current available will be the sum of the capacities of all operating power supplies.</p>
Power Drawn	Total Current Drawn by powered-on FRUs.

Crossbar Switching Fabric

[Table 3-4](#) describes the Crossbar Switching Fabric information.

Table 3-4 Crossbar Switching Fabric Information

Field	Description
Crossbar Switching Fabric	<p>Physical and configuration information about the module:</p> <p>Active slot—Indicates the slot number of the active switching fabric module. A value of NONE indicates that the active switching fabric module is either powered down or not present in the chassis.</p> <p>Backup slot—Indicates the slot number of the backup switching fabric module. A value of NONE indicates that the backup switching fabric module is either powered down or not present in the chassis.</p> <p>Bus Only Mode Allowed—Determines the value of each module. If set to True, each and every module is allowed to run in bus-only mode. If set to False, none of the modules are allowed to run in bus-only mode. (All the non-fabric capable modules will be powered off.) Absence of fabric module results in all the fabric capable modules being powered off.</p> <p>Truncated Mode Allowed—Indicates whether truncated mode is administratively enabled on the device or not.</p>
Module Switching Mode	<p>Indicates switching mode of the module:</p> <p>busmode—Module does not use fabric. Backplane is used for both lookup and data forwarding.</p> <p>crossbarmode—Module uses the backplane for forwarding decision and fabric for data forwarding.</p> <p>dcefmode—Module uses fabric for data forwarding and local forwarding is enabled.</p>
Module-Channel	Module slot number
Module-Status	Status of the fabric channel at the module
Fabric Status	Status of the fabric channel at the slot
Speed (MB)	Speed (MB/second) of the module
Module-Channel	Channel for the module
In Errors	The total number of error packets received since this entry was last initialized.
Our Errors	The total number of error packets transmitted since this entry was last initialized.
Dropped	The total number of dropped packets transmitted since this entry was last initialized.
In Utilization (%)	Input utilization of the channel for the module.
Out Utilization (%)	Output utilization of the channel for the module.

Ternary Content Addressable Memory Information

Shows the Ternary Content Addressable Memory (TCAM) usage information. [Table 3-5](#) lists and describes the TCAM information.

Table 3-5 Ternary Content Addressable Memory Information

Field	Description
Security Acl Mask	Indicates that TCAM space is allocated to store ACL masks.
Security Acl Value	Indicates that TCAM space is allocated to store ACL value.
Dynamic Security Acl Mask	Indicates that TCAM space is allocated to dynamically store ACL masks.
Dynamic Security Acl Value	Indicates that TCAM space is allocated to dynamically store ACL values.
Qos Acl Mask	Indicates that TCAM space is allocated to store QoS masks.
Qos Acl Value	Indicates that TCAM space is allocated to store QoS value.
Dynamic Qos Acl Mask	Indicates that TCAM space is allocated to dynamically store QoS masks.
Dynamic Qos Acl Value	Indicates that TCAM space is allocated to dynamically store ACL values.
Layer 4 Port Operator	Indicates that TCAM space is allocated for layer 4 port operators purpose.
Interface Mapping Module	Indicates that TCAM space is allocated for interface mapping purpose.

Router Health Options

If your device is a router, the Router Health window displays with a drop-down box that provides the following options:

- [Router Health, page 3-28](#)
- [Router Information, page 3-29](#)

Router Health

The Router Health window displays a real-time graph and information about the health of a router. [Table 3-6](#) describes the contents of the Router Health window.

Table 3-6 Router Health Information

Field	Description
CPU Usage (graph)	Overall CPU busy percentage in the last 5 minute period
CPU Type	Describes type of CPU being monitored
Last 1 minute	Overall CPU busy percentage in the last 1 minute period.
Last 5 minutes	Overall CPU busy percentage in the last 5 minute period.
Temperature Description	Description of the test point being measured

Table 3-6 Router Health Information (continued)

Field	Description
Temperature Status	The current state of the test point being instrumented; one of the following are the states: <ul style="list-style-type: none"> • Normal • Warning • Critical • Shutdown • Not Present • Not Functioning • Unknown
Failures	The failing component of the power supply being measured: <ul style="list-style-type: none"> • None—No failure • inputVoltage—Input power lost in one of the power supplies • dcOutputVoltage—DC output voltage lost in one of the power supplies • Thermal—Power supply thermal failure. • Multiple—Multiple failures. • Fan—Fan failure • Overvoltage—Over voltage.
Memory Type	Type of memory including processor and I/O.
Used	Number of used MB for a particular memory type.
Free	Number of free MB for a particular memory type.
Largest Free	Number of largest contiguous free MB for a particular memory type.

Router Information

The Router Information window displays router information. [Table 3-7](#) lists and describes the fields of the Router Information window.

Table 3-7 Router Information

Field	Description
Name	Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.
Hardware	A textual description which should contain the manufacturer's name for the physical entity and be set to a distinct value for each version or model of the physical entity.
Supervisor Software Version	The full name and version identification of the system's software operating-system and networking software.
Up Time	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Table 3-7 Router Information (continued)

Field	Description
Location	The physical location of this node.
Contact	The textual identification of the contact person for this managed node and information on how to contact this person.
Modem	Indicates whether the RS-232 port modem control lines are enabled.
Baud	The baud rate in bits per second of the RS-232 port.
Power Supply	Description of the power supply being instrumented.
Power Supply Type	The power supply source: <ul style="list-style-type: none"> • unknown • ac • dc • externalPowerSupply • internalRedundant
Power Supply Status	The current state of the power supply being instrumented. <ul style="list-style-type: none"> 1: normal 2: warning 3: critical 4: shutdown 5: notPresent 6: notFunctioning

Analyzing Media

The menu selections for Analyzing Media are:

- [RTP Streams, page 3-30](#)
- [Voice Call Statistics, page 3-33](#)
- [Calls Table, page 3-33](#)
- [RTP Conversation, page 3-34](#)
- [Site MOS, page 3-35](#)

RTP Streams

- [Understanding the RTP Stream Data, page 3-31](#)
- [Monitoring RTP Streams, page 3-32](#)

Understanding the RTP Stream Data

To view RTP stream information, summary statistics on the stream, and per-interval statistics, use the RTP Streams.

This window shows you three pieces of information:

RTP Stream Information

- Source IP Address and Port: IP address and UDP port of the originator of the RTP stream.
- Destination IP Address and Port: IP address and UDP port of the receiver of the RTP stream.
- SSRC: Synchronization source number as it appeared in the RTP header of the RTP stream.
- codec: encoding decoding format of the RTP stream.

RTP Stream Stats Summary

This shows you the summary of the RTP stream for the entire duration of RTP stream.

- Duration: duration of the RTP stream. This may not be the entire duration of the stream. It depends on the viewing time interval of the window which launched this RTP stream detail window.
- Worst / Duration Weighted / Max MOS: the lowest score among per-interval reports, the score of all per-interval reports that takes duration into account, and the highest score among per-interval reports of the stream.



Note Duration-weighted is calculated with the following formula:

$$\text{SUM (per-minute-mos * duration)} / \text{SUM (duration)}$$

- Worst / Duration Weighted / Min Jitter: the largest jitter among per-interval reports, the jitter that takes into account of the duration of all per-interval reports, and the smallest jitter values among per-interval reports of the stream.



Note Duration-weighted are used with the following formula:

$$\text{SUM (per-interval-jitter * duration)} / \text{SUM (duration)}$$

- Worst / Overall / Min Actual Packet Loss: Loss percent of RTP packets that are not seen by NAM and RTP packets that arrived beyond the buffer capability of the receiving endpoint. This includes the highest percentile among per-interval reports, the sum of packets loss against total packets of all per-interval reports, and the lowest percentile loss among per-interval reports.
- Worst / Overall / Min Actual Packet Loss: Similar to above, but the percent loss only includes RTP packets that were not seen by the NAM.
- Worst / Total / Min Concealment Seconds: Number of seconds in which NAM detected packet loss during the duration of the stream. This includes lowest concealment seconds among per-interval reports, total concealment seconds of the entire duration of the stream, and highest concealment seconds among per-minute stream reports.
- Severe Concealment Seconds: Similar to above; severe condition is met when the seconds have more than 5 percent loss.

RTP Stream Stats Details

This table shows the per-interval stats calculated by NAM at each interval. The columns of the tables are:

- Report Time: time when the stats were calculated. This is the end time of the interval.

- Report Duration: the stream duration during the report interval.
- Worst MOS: the lowest score of the stream among 3-second MOS score. NAM internally evaluates the MOS value of the stream every 3 seconds. This is the lowest score among them.
- Average MOS: average score of the 3-second score values during the duration of the stream in the interval. This value is used in deriving the Duration Weighted MOS value in NAM.
- Jitter: variation of packet arrival time compare to the expected time.
- Actual Packet Loss percentile: percentile of packets that are not seen by NAM.
- Adjusted Packet Loss percentile: percentile of packets that include the actual packets lost an packets that had arrived too late to get into buffer prior to paying back at the endpoint.
- Concealment Seconds: number of seconds in which the NAM sees packet loss.
- Severe Concealment Seconds: number of seconds in which the NAM detected more 5 percent of packet loss.
- Packets: total packets NAM have seen for the interval.

Monitoring RTP Streams

Use Prime NAM to monitor the network to ensure that call quality is good. If quality issues appear, isolate and troubleshoot the problem rapidly.

-
- Step 1** View RTP Streams using the menu selection **Analyze > Media**. You can access this from the RTP Conversation table by clicking on a specific stream or from the Call Detail window by clicking on the stream that is associated with the call.
- This chart indicates current voice quality of all RTP streams being monitored. MOS values range from 1 to 5, where 1 is poor and 5 is excellent (see the legend for a breakdown into categories-Poor, Fair, Good and Excellent). Use the Top N RTP Streams source and destination endpoints to view whether there are calls that are in the poor range.
- Step 2** To isolate calls that have had a poor MOS, scroll down to Top N RTP Streams and click on the chart to drill down into the RTP Stream Details. Note that MOS values for calls below 3.0 might be considered low. You can also look at the other metrics provided in the same row (for example, row one. note the jitter and packet loss rate scores to see if they also result in a low MOS value. This information can help you determine if jitter is the root cause of the poor calls; or if it is instead packet loss somewhere in the network.
- Step 3** With the endpoints' IP addresses, you can look at the network topology to identify where in the network your subnet is located.
- Navigate to that NAM and go to the menu selection **Analyze > Managed Device > Interface**. This page lists all interfaces and errors or discards on each interface. Look up the link that leaves the site in question. That interface is likely the source of the packet loss. Check the interface for faults and fix as needed.

Understanding RTP Streams

To monitor the RTP streams, choose **Analyze > Media > RTP Streams**. You can also arrive at this page by:

- From the RTP Conversation table, clicking on a specific stream
- From the Call Detail window, clicking on the stream that is associated with the call

In this window, at least one of the following is required: Site or data source.

The five charts available in this window are:

- **RTP Streams:** Number of streams that fall in the quality bands of excellent, good, fair, and poor during the selected interval.
- **Top N Source Endpoints:** Endpoints that generated the lowest duration weighted MOS during the selected interval.
- **Top N Destination Endpoints:** Endpoints that experienced the lowest duration weighted MOS during the selected interval.
- **Top N RTP streams:** RTP streams that have the lowest duration weighted MOS during the selected interval.
- **Top N RTP streams by Adjusted Packet Loss:** RTP streams that have the highest overall adjusted packet loss percent during the selected interval.

Voice Call Statistics

To monitor voice quality, choose **Analyze > Media > Voice Call Statistics**. The charts will provide an overview of voice quality.

The charts available are:

- **Voice Call Statistics:** Number of calls per signaling protocol (SCCP, SIP, MGCP, and H.323) at each interval during the selected interval.
- **Top N End Points by Jitter (ms):** Endpoints that have the largest average of endpoint reported jitter during the selected interval.
- **Top N End Points by Packet Loss (%):** Endpoints that have the largest average of endpoint reported packet loss during the selected interval.
- **Top N Calls by Jitter (ms):** Calls that have the longest endpoint-reported jitter during the selected interval.
- **Top N Calls by Packet Loss (%):** Calls that have the most endpoint reported packet loss percent during the selected interval.

Calls Table

The Calls Table shows you calls that the NAM detected by inspecting voice signaling protocols' payload. For this table to have data, the NAM must see:

- SCCP protocol: Call Information message of the call.
- SIP protocol: SIP INVITE message of the call. Note that SIP protocol will be detected as per call leg.
- H.323 protocol: Call SETUP of the call.
- MGCP protocol: Create connection message of the call. Note that MGCP will be detected per call leg.



Note

SIP and MGCP will be detected per call leg. Each call could be two or more parties. Each party has its own call leg from the call party to control entity; for example, Cisco Unified Communications Manager or MGCP gateway. Any information that is not detected by NAM will be displayed as “-” or blank.

To view the active calls, choose **Analyze > Media > Detailed Views > Call Table**. The Calls Table and RTP Streams for the Selected Call Table display. These tables show a list of all currently active calls.

**Note**

Some values in the Calls table are not available until the end of the call, and Cisco Unified Communications Manager must be configured to have the IP phones send out the call status and quality information.

**Note**

All calculated metrics in [Table C-44, Calls Table](#), are based on a one minute interval.

[Table C-44](#) provides descriptions of the Calls Table fields.

If you click on a call row in the table, in the RTP Streams for the Selected Call display at the bottom of the page you will see all streams that are associated with the call. It will display the RTP streams that:

- have source address and port matched the call's calling host address and calling port or called host address and called port
- have destination address and port that matched the call's calling host address and calling port or called address and called port

**Note**

There is a delay of two minutes of RTP streams statistics. As the result, there may not be any RTP stream information of the call.

The RTP Streams of the Selected Call table shows the overall RTP streams statistics that are calculated by the NAM. You can use this information to compare the views of the call endpoints and the NAM regarding the call quality. The columns of the RTP Stream report are described in [Table C-45](#).

You can see more detailed information about each RTP stream by selecting the RTP stream and clicking on the **RTP Stream Details** button. A pop up window will show more detailed information of the stream displayed.

RTP Conversation

To get detailed information about RTP conversations, choose **Analyze > Media > Detailed Views > RTP Conversations**. This table shows you the overview of RTP streams analyzed by NAM during the selected interval. You can drill down to each stream to get stream statistics, which are analyzed by the NAM at each interval. To get more detailed information, you can:

- Click on the RTP stream for which you want to see more information.
- Click on the "RTP Stream Details" context menu. A pop up window will show you the detailed information of the stream.

The columns of the RTP Conversation tables are described in [Table C-46](#).

Site MOS

You can use the Mean Opinion Score (MOS) to quantify the perceived level of quality you are receiving in your network voice traffic. This allows you to assess the work of codecs, or algorithms, which compress audio traffic to save on bandwidth utilization but may result in a drop in quality.

You must first set up the software to monitor voice data, then you can view the collected voice data using **Analyze > Media > Detailed Views > Site MOS**.

[Table C-29](#) contains details on Site MOS scores.

Using the NAM Application Programming Interface

NAM provides an Application Programming Interface (API) that allows you to configure and retrieve data from the NAM. The API follows the commonly used Representational State Transfer (REST) style of providing services over HTTP or HTTPS. The NAM REST API is also referred to as the Northbound Interface (NBI).

For application developers who want to use the NAM REST API, ask your Cisco representative about the *Cisco Prime Network Analysis Module REST API Guide*.

