Cisco Prime Network Analysis Module User Guide

Release 6.1
July 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-31779-01

Cisco Prime Network Analysis Module User Guide

Contents

Preface

This preface discusses the objectives, audience, conventions, and organization of the *Cisco Prime Network Analysis Module User Guide* and provides general information about Cisco Prime NAM software documentation. This preface has the following sections:

For a list of the platforms that Prime NAM supports, see Cisco Prime Network Analysis At-a-Glance.

Chapter Overview

This guide contains the following chapters:

Table 1 Organization

Chapter	Title	Description
Chapter 1	Overview	Summary of how Prime NAM provides deeper visibility into the network to accelerate troubleshooting and optimization decisions.
Chapter 2	Getting Started	Information about where to find quick start and Prime NAM customization tasks.
Chapter 3	Monitoring and Analyzing Traffic	Options for viewing and monitoring various types data.
Chapter 4	Capturing and Decoding Packets	Information about setting up multiple sessions for capturing, filtering, and decoding packet data, managing the data in a file control system, and displaying the contents of the packets.
Chapter 5	Performing User and System Administration	Information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance.
Chapter 6	NAM Deployment	Scenarios for Prime NAM deployment and the details you may need to know about them.

Table 1 Organization (continued)

Chapter	Title	Description
Chapter 7	Customizing Cisco Prime NAM	Setup details you can review to determine if you want to use advanced features.
Appendix A	Understanding Prime NAM Traffic Sources	Explains the various data sources that you can configure for **Prime NAM.**
Appendix B	Understanding Prime NAM Behavior Reference	Includes details on how Prime NAM e.works including how to navigate and use the control elements in the user interface
Appendix C	GUI Field Descriptions	Describes critical user interface fields.
Appendix D	Troubleshooting Network and NAM Issues	Lists common NAM and its network connection issues with recommendations on how to tackle them.

Audience

This publication is intended primarily for network administrators who are responsible for setting up and configuring Network Analysis Modules (NAMs) to monitor traffic and diagnose emerging problems on network segments. As a network administrator, you should be familiar with:

- Basic concepts and terminology used in internetworking.
- Network topology and protocols.
- Basic UNIX commands or basic Windows operations.

Conventions

This document uses the following conventions:

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
`italic screen` font	Examples of variables that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.

Convention	Description
[ ]	Default responses to system prompts appear in square brackets.
Option > Network Preferences	Selecting a menu item.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Notices

The *Cisco Prime Network Analysis Module Third Party and Open Source Copyright Notices* contains the licenses and notices for open source software used in Prime NAM. Prime NAM includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This document is available on www.cisco.com with the Prime NAM technical documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Overview

This chapter contains information about the Cisco Prime Network Analysis Module (NAM) software and describes task overviews.

This chapter contains the following sections:

Introducing Cisco Prime NAM

The Cisco Prime Network Analysis Module (Prime NAM) software is a network monitoring and analysis tool that combines flow-based and packet-based analysis into a single tool set. Prime NAM software provides network operations and engineering with user, command line, and application programming interfaces that you use for traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics. as well as ways to see deeper into your network. The robust graphical user interface makes traffic monitoring and troubleshooting simple and cost-effective.

This chapter contains an overview on ways to use Prime NAM to monitor and analyze your network traffic. See Table 1-1 for details on high-level task areas and how they map to the user interface.

For a list of the key features in this release, see the *Cisco Prime Network Analysis Module Release Notes*.

Table 1-1 Prime NAM Task Areas

Task Area	Menu Mapping	Task Description	Used By
Plan and Prepare	Setup menu	Create a list of your network performance goals. Set expected goals and limits for response time, expected ranges for MOS values, bandwidth usage per application, and utilization on critical WAN links. Determine on which performance issues you want to concentrate.	Network Engineers, Designers, and Architects
Monitor and Analyze	Home, Capture, Analyze and Monitor menus	View dashboards which give you a quick view of traffic performance information, and various incidents. Use interactive reports filter data when monitoring specific network traffic and troubleshooting problems. Monitor your network and perform other day-to-day operations related to proactive and reactive traffic analysis and troubleshooting. Analyze QoS policy traffic using alarms, syslogs, traps, and e-mail alerts. See Monitoring and Analyzing Traffic and Capturing and Decoding Packets.	Network Engineers, NOC Operators, and Service Operators
Administer	Administer menu	Change default system display, notification, and user settings, as well as manage database access control and view system diagnostics. See Performing User and System Administration.	Network Engineers
Deploy	Setup and Admin menus	Configure devices to share data with NAM. Configure managed devices and data sources. Perform customized setup of NAM including sites, alarms and thresholds, scheduled exports, and so on. Monitor an extended level of your managed device's data (health and interface information). Determine which locations are ingress or egress points of a logical network boundary (aggregation layer, core, campus edge, and so on) that can offer valuable insights into the network activity within that partition. Create a baseline of current metrics including applications, bandwidth per application, top conversations and hosts, QoS values used in the network, unrecognized protocols, and current server and end-to-end response time measurements. See Customizing Cisco Prime NAM.	Network Engineers, Designers, and Architects
Troubleshoot	Capture, Analyze and Monitor menus	Resolve common NAM issues including login problems and unresponsiveness, understand error messages, and troubleshoot network issues using Prime NAM. See Troubleshooting Network and NAM Issues.	Network Engineers, NOC Operators, and Service Operators

Overview of the Cisco NAM Platforms

Cisco NAM is supported on a variety of platforms. This guide does not discuss platforms, but focuses on tasks and capabilities.

For a list of Cisco NAM models and their features and capabilities, see the data sheets in Products & Services on Cisco.com.

It is important to note that the portfolio of Cisco NAM models differ in memory, performance, disk size, and other capabilities. Therefore, some allow for more features and capabilities (for example, the amount of memory allocated for capture).

Throughout this guide, there may be notes explaining that some features apply only to specific platforms. If there is no note, then that feature or aspect applies to all Cisco NAM platforms.

For details on memory, performance, disk size, and other capabilities, see the *NAM Compatibility Matrix*.

How to Use Prime NAM to Analyze Your Traffic

The Cisco Prime NAM software helps you to address the following major areas:

- Network Layer Traffic Analysis. Prime NAM provides comprehensive traffic analysis to identify what applications are running over the network, how much network resources are consumed, and who is using these applications. Prime NAM software offers a rich set of reports with which to view traffic by Hosts, Application, or Conversations. See the discussions about Dashboards, starting with Using Traffic Summary, page 3-4.
- Application Response Time. Prime NAM can provide passive measurement of TCP-based applications for any given server or client, supplying a wide variety of statistics like response time, network flight time, and transaction time. See Using Response Time Summary, page 3-5.
- Voice Quality Analysis. Prime NAM provides application performance for real time applications like Voice and Video. Prime NAM can compute MOS, as well as provide RTP analysis for the media stream. See Analyzing Media, page 3-30.
- Advanced Troubleshooting. Prime NAM provides robust capture and decode capabilities for packet traces that can be triggered or terminated based on user-defined thresholds. See Application Performance Monitoring Using Capture and Decode, page 4-5.
- WAN Optimization insight. Prime NAM provides 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. See
- Open instrumentation. Prime NAM is a mediation and instrumentation product offering, and provides a robust API that can be used by partner products as well as work with customer-created applications. Contact your account representative for a copy of the *Cisco Prime Network Analysis Module API Programmer's Guide*.

To understand which types of monitoring are supported by specific NAM data sources, see Table 1-2.

Table 1-2 Data Source Monitoring Capabilities

Data Sources	Monitoring Capabilities				
	Capture	Traffic	ART	RTP/Voice	URL
SPAN/VACL/ERSPAN	Yes	Yes	Yes	Yes	Yes
WAAS	No	Yes	Yes	No	No
NetFlow	No	Yes	No	No	No

For information on which data sources Prime NAM uses to deliver this functionality, see Understanding Prime NAM Traffic Sources. For information about which traffic sources are supported on each platform, see the *NAM Compatibility Matrix*.

Before You Begin

Depending on your Cisco NAM, ensure the following list of requirements are complete before you use Prime NAM. For detailed instructions, see your platform installation guide, except where noted:

- Reset your Cisco NAM root password
- Set up a data source to send traffic to the Cisco NAM
- Configure access to the Prime NAM user interface or CLI
- Synchronize your Cisco NAM to the standard time source outside the NAM in addition to the router or switch (depending on your platform). For detailed instructions, see Synchronizing Your System Time, page 5-5.

For optional advanced customizations, such as adding sites or configuring alarms and thresholds, see Advanced Configuration Overview, page 7-2.

Getting Started

This chapter contains getting started information for both users that want to use the NAM quickly without customizing the product or that want to customize the NAM. It includes some simple workflows that illustrate how to use Prime NAM to quickly to help troubleshoot performance and optimization issues.

There are many additional workflows for which Prime NAM can be used. These tasks are documented in the following chapters.

This chapter contains the following sections:

Before You Begin

This section contains tasks that must be performed prior to using NAM.

1. Ensure you perform all required tasks in your NAM installation guide. To review your platform's specific requirements, see http://www.cisco.com/go/nam/docs.
2. Ensure that the NAM system time is configured correctly. If the system time is incorrect, NAM data presentation may be inaccurate due to time ranges, hence providing incorrect interpretations of NAM data. Although some platforms are synchronized automatically, you must also synchronize the standard time source outside the NAM in addition to the NAM and the router or switch in order for the data to be accurate. For details, see Synchronizing Your System Time, page 5-5.

Quick Start

Use the following workflows to get started using your product. These tasks do not require additional configuration or setup. You can see other workflows and tasks within this user guide in the task-specific chapters.

- 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
- Filtering Data Using Global Search, page B-5
- Filtering Traffic for Viewing on the Dashboards, page B-4
- Filtering Data Using Global Search, page B-5

Where to Go to Learn How to Customize Your NAM

There are many capabilities beyond the tasks you can perform out-of-the box. These tasks require some level of customization before you can access some of the additional functionality within NAM.

To review the customization you may need to perform, see Advanced Configuration Overview, page 7-2.

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:

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 *rate* or *cumulative*, 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.

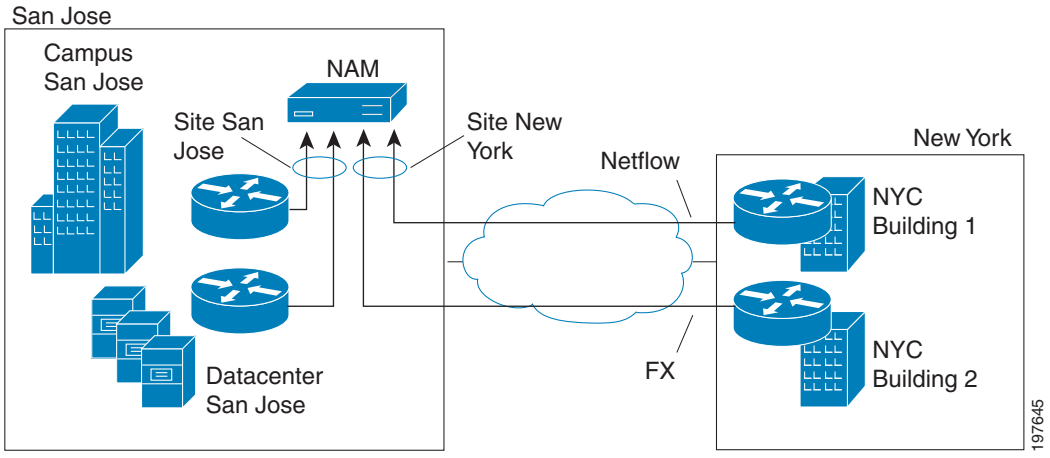
  You can also use the Filter button, both in this window and the All Alarms window, to display only alarms that meet the criteria you enter.

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

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:

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

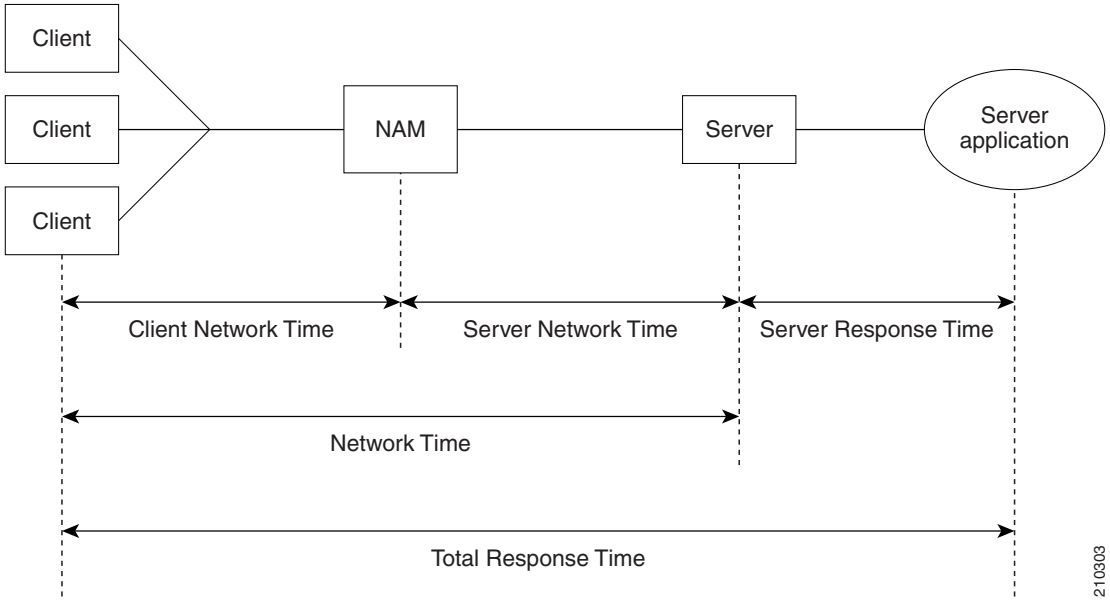


Figure 3-3 shows a representation of total transaction time as opposed to application response time.

Figure 3-3 Transaction Time versus Response Time Measurements

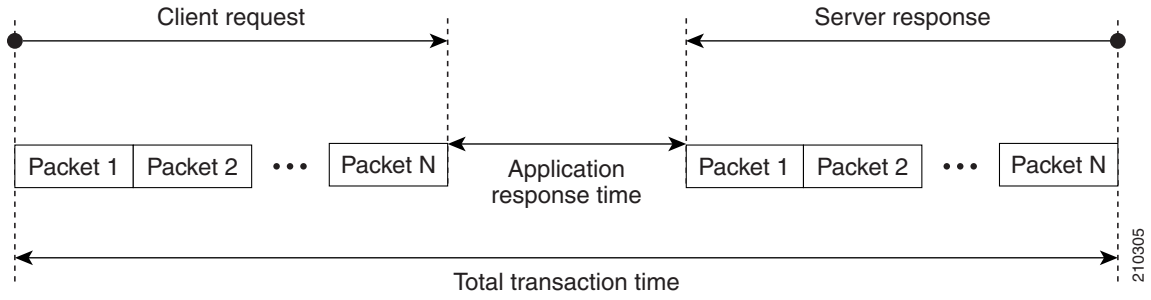


Table C-33 lists and describes the ART metrics measured by Prime NAM.

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

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.

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: • unknown • ac • dc • externalPowerSupply • internalRedundant
Power Supply Status	The current state of the power supply being instrumented. 1: normal 2: warning 3: critical 4: shutdown 5: notPresent 6: notFunctioning
Power Redundancy Mode	Power Redundancy Mode: The power-supply redundancy mode. 1: not supported 2: redundant 3: combined
Power Total	Total current available for FRU usage. 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. When Redundancy Mode is combined, the total current available will be the sum of the capacities of all operating power supplies.
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	Physical and configuration information about the module: **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. **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. **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. **Truncated Mode Allowed**—Indicates whether truncated mode is administratively enabled on the device or not.
Module Switching Mode	Indicates switching mode of the module: **busmode**—Module does not use fabric. Backplane is used for both lookup and data forwarding. **crossbarmode**—Module uses the backplane for forwarding decision and fabric for data forwarding. **dcefmode**—Module uses fabric for data forwarding and local forwarding is enabled.
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: • Normal • Warning • Critical • Shutdown • Not Present • Not Functioning • Unknown
Failures	The failing component of the power supply being measured: • 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: • unknown • ac • dc • externalPowerSupply • internalRedundant
Power Supply Status	The current state of the power supply being instrumented. 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:
  SUM (per-minute-mos * duration) / 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:
  SUM (per-interval-jitter * duration) / 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*.

Capturing and Decoding Packets

You can set up multiple sessions to capture, filter, and decode packet data using the Capture feature. You can then manage the data in local or remote storage and display the contents of the packets to collect troubleshooting information.

Note This software feature may be limited depending on your hardware platform. For details, see the *NAM Compatibility Matrix* or the *Cisco Prime Network Analysis Module Release Notes*.

This chapter contains the following sections:

How Do I Solve My Problem?

This section provides an overview of how to collect and analyze packet data to ensure your network is running well or pinpoint network issues.

There are many ways to collect data and analyze it using Prime NAM. In order to collect data, the prerequisite is to have set up SPAN or ERSPAN through your NAM dataports. For details on data source configuration, see Understanding Prime NAM Traffic Sources, page A-1. Many users want a quick capture to analyze their packet data. See Manually Starting a Capture, page 4-2 for details on how to get a quick capture.

Table 4-1 provides an at-a-glance summary of capture tasks you can perform to ensure your network is optimized and trouble-free.

Table 4-1 Data Collection and Analysis At-a-Glance

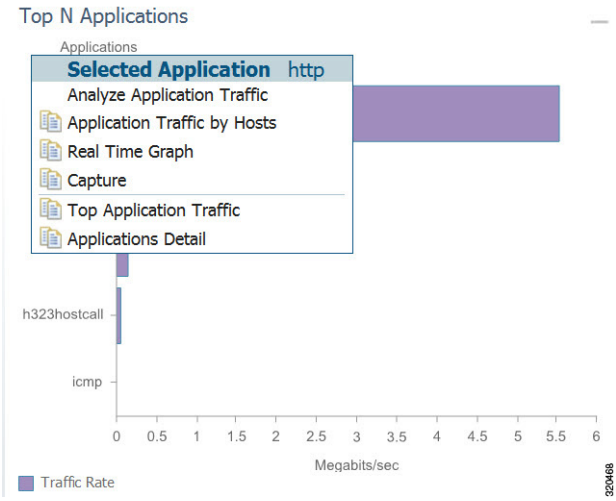
Basics	Operation	Description
Capture the traffic quickly from any NAM dashboard when anomalies are present	Quick Capture	Targets data collection based on the dashboard graph you select and provides a capture session and decode window to analyze the traffic immediately. See Manually Starting a Capture, page 4-2. Do not use quick capture if your context includes an NBAR application ID. Use **Capture > Packet Capture/Decode > Sessions** to configure and start your capture.
Proactively capture packet data to learn the cause of a network issue	Continuous capture or schedule capture	Allows you to set up data collection to: • Collect data prior to a network problem • Set up data collection based on an anomaly that reoccurs See Using Alarm-Triggered Captures, page 4-3 or Scheduling Captures, page 4-3.
Create hardware and software filters to focus on specific long-term packet data	**Capture > Packet Capture/Decode > Sessions**	On supported NAM hardware, helps to limit the amount of packet data processing. See Configuring Hardware Filters, page 4-9 and Configuring Software Filters, page 4-7.
Storing packet data for problem identification	Continuous capture	Allows you to save data to external storage targets, potentially for larger disk capacity and higher capture throughput or to offload capture files. Continuous capture overwrites itself in memory when the buffer is full. See About Capturing to Data Storage, page 4-22.
Create targeted monitoring for problem isolation	Stop Capture and Save to File	Allows you to decide when to use trigger capture sessions. This must be setup in **Setup > Alarms > Actions**. See Configuring Alarm Actions, page 7-29 and Using Alarm-Triggered Captures, page 4-3.
Set up storage for data collection	**Capture > Packet Capture/Decode > Data Storage**	Allows you to save data for extended periods either to memory or storage. See About Capturing to Data Storage, page 4-22.
Analyze data for potential issues	Decode	See Inspecting Packet Decode Information for Suspicious Traffic.

Manually Starting a Capture

You do not have to perform any configuration and can quickly collect packet data by selecting the context menu option, **Capture**. Figure 4-1 shows an example of a context menu for Top N Applications dashboard.

For details on how to use the decode window to analyze your data, see Inspecting Packet Decode Information for Suspicious Traffic, page 4-28.

Figure 4-1 Quick Capture



Using Alarm-Triggered Captures

You can configure multiple alarm-triggered captures that start and stop automatically by alarm events you define.

To set up an alarm-triggered capture:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session. For detailed instructions, see Configuring Capture Sessions, page 4-6.

Step 2 Create an alarm event from **Setup > Alarms > Actions** and click **Create** to make a new trigger capture action which uses the session from Step 1.

Configure an alarm event for the type of event for which you want to capture data. For detailed instructions, see Configuring Alarm Actions, page 7-29.

Step 3 Create a threshold which uses the alarm event action from Step 2. Choose **Setup > Alarms > Thresholds** window.

To configure the threshold of parameters of interest in the associated Alarm Event, see Defining Thresholds, page 7-31.

Scheduling Captures

You can configure multiple time-based triggered captures that start and stop automatically based on a certain time or period of time that you define. This is also referred to as continuous capture. Continuous capture overwrites itself in memory when the buffer is full. The following is an example of setting a 60 minute window to schedule capture packet data.

To set up a schedule capture:

Step 1 Create a new capture from the **Capture > Packet Capture/Decode > Sessions** window.

Step 2 Check the Auto Capture **Enable** check box.

Step 3 Set the Start Date and Time and Duration (in minutes) to *60*.

Step 4 Select an appropriate storage type to store your capture data. For example, select capture to *memory HDD*.

Step 5 Select appropriate software filters.

Step 6 Click **Submit**.

Step 7 To start the capture session, return to the **Capture > Packet Capture/Decode > Sessions** menu and select the capture session you previously created and click **Start**.

Troubleshooting Application Slowness Using Alarms

This section describes how to use Prime NAM to use triggered alarms and capture files to help you determine the source of some network problems.

Before You Begin

You must already create an alarm that notifies you when there is a surge in application traffic. If you need to create an alarm, thresholds, and set up email notification, see Setting Up Alarms and Alarm Thresholds, page 7-28.

To use existing alarms to help you to create and analyze captured packet files:

Step 1 After receiving an email that was triggered by an alarm notification, view the alarm summary and analyze the details. For example, if your alarm triggers when your application has reached a certain threshold, choose **Monitor > Alarm Summary** to view the Top N Applications by Alarm Count dashboard.

If you use sites, you could view the top sites by alarm count dashboard in order to see the alarm details and determine what threshold variable is causing the alarm to trigger.

Step 2 To view more details (or drill down) from this dashboard, left-click the row you are interested in and select **Application Response Time** in order to analyze the response time during the time interval of the alarm trigger. If you application is not listed in the graph, you can select the table icon to choose your application from the list of all the applications and drill down from there to analyze the response time.

Step 3 Adjust the Interactive filter to view specific time ranges and severity levels in order to view where the spike in response time occur. This helps to determine if the occurrence is limited to a one-time event, if it occurs more than once in a short period of time, or is an event related to a specific time of the day. For example, by changing the time range filter from 1 hour to 4 hours to 1 day, you can see the latest data trends that help you to determine what to do next. See Filtering Traffic for Viewing on the Dashboards, page B-4.

Step 4 In the graph that displays, focus in on the time frame when the event occurs by using the slider to pinpoint the event. Look for peak or valleys; these may be critical changes that require investigation. Using the legend you can determine whether the event was caused by the network or server. See Changing the Time Interval Using Zoom/Pan Charts, page B-6.

Step 5 Select any of the metrics provided below the application average response time graph.

a. To view if there are specific clients that have significant transaction time differences, see the Top Clients By Average Transaction Time graph in order to identify data such as Client-Server Application Transactions using an application-specific filter.

- To view a table of response time metrics and add new metrics for additional data (such as average server response time) and use the drop down menu to select which other metric data you want to appear in the graph.

Application Performance Monitoring Using Capture and Decode

This task explains how to proactively monitor your application performance, then use it to help isolate and troubleshoot application latency issues experienced by your end user.

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.

Step 1 Identify and monitor your business critical applications. In order to see Layer 7 application details, ensure you enable deep packet inspection. Choose **Setup > Classification > Applications Settings** and select the Deep Packet Inspection checkbox.

For detailed instructions, see Adding More Detail into Dashboard and Application Reports, page 7-46.

Step 2 Proactively detect performance degradation using threshold violation alerts. First, define your alarm by choosing **Setup > Alarms > Actions**. Then define the thresholds for your alarm by choosing **Setup > Alarms > Thresholds**.

For detailed instructions, see Setting Up Alarms and Alarm Thresholds, page 7-28.

Step 3 Validate a reported trouble ticket or network issue. Choose **Monitor > Overview > Response Time Summary** and use the Top N Applications by Transaction Time dashboard to identify which application may be impacted.

You can select the table view to see more than the top default applications. You can also use the other dashboards to view server or client transaction times. See Using Response Time Summary, page 3-5.

Step 4 Analyze the application performance behavior over time using the Interactive Report filter. Determine if the behavior is transient, persistent, recurring, and so on. For details on using the Interactive Report filters, see Filtering Traffic for Viewing on the Dashboards, page B-4.

Step 5 Zoom in to view specific spikes in the performance, and drill down to isolate whether the cause of the degradation stems from your network, server or application. See Changing the Time Interval Using Zoom/Pan Charts, page B-6.

Step 6 Analyze the server response time and network performance metric in order to eliminate one of them as the cause. See Server Response Time, page 3-21 and Network Response Time, page 3-20.

Step 7 Analyze server activity based on the traffic the server is placing on the network and assess the cause of increase in the server response time. See Analyzing Host Traffic, page 3-10.

Step 8 Perform packet captures in order to identify the root-cause. For details on quick captures or trigger captures, see Capturing and Decoding Packets, page 4-1.

Step 9 Perform additional actions to isolate and troubleshoot the problem including: QoS analysis and interface analysis.

Creating and Managing Capture Sessions

You can use capture sessions to capture, filter, and decode packet data, manage the data in a local or remote storage, and display the contents of the packets. The captured packets can be decoded and analyzed using Prime NAM for more efficient problem isolation.

This section contains the following topics:

Configuring Capture Sessions

Because it may be important for you to collect data over time and have various locations for which you want to analyze data, we support multiple sessions per capture location/target. You can collect data using multiple sessions per target, but only one session can be running per target. Prime NAM now supports up to 25 capture sessions. If you have external storage you can save to local disk and some number of LUNs. As part of configuring a capture session, you can also create software filters, if desired (see Creating a Software Capture Filter for a Capture Session, page 4-7).

To configure a new capture session:

Step 1 Choose **Capture > Packet/Capture Decode > Sessions**.

Step 2 Click **Create** to set up a new capture. The NAM displays the Configure Capture Session window.

Step 3 Enter information in the Capture Settings Fields (Table C-49) as appropriate.

When capturing to multiple files, a suffix is added to the file name. For example, the first file for a capture named *CaptureA* would be labeled as *CaptureA_1* the second *CaptureA_2*, and so on.

Step 4 Click **Submit** to finish configuration for this session, or configure Software Filters for this session (see Understanding Global Capture Settings, page 4-17).

Configuring Software Filters

You can create and save specialized filters that will disregard all capture data except the information in which you are interested (see Figure 4-3). You can configure multiple software filters for each session (up to six). This allows you to narrow in on the traffic that you are interested in, and it also saves resources (either memory or disk space).

Use the following topics for help on filtering network traffic using software filters:

- Creating a Software Capture Filter for a Capture Session, page 4-7
- Editing a Software Capture Filter, page 4-7
- Understanding Software Capture Filter Options, page 4-8

Creating a Software Capture Filter for a Capture Session

You can create software capture filter for many variables. This workflow examines how to create a capture session with a software filter.

To create a software capture filter:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**.

Step 2 Click **Create** to create a new capture session.

If you already have a capture session to which you want to add a software filter, see Editing a Software Capture Filter, page 4-7 for detailed instructions.

Step 3 Enter information in each of the fields as appropriate. See Table C-55 for descriptions of the fields.

Step 4 Click **Submit** to create the filter, or click **Cancel** to close the dialog box without creating a software filter.

Editing a Software Capture Filter

To edit software capture filters:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**.

Step 2 Choose the session to edit, then click **Edit**.

The Software Filter dialog box displays. See Table C-55.

Step 3 Enter information in each of the fields as appropriate.

Step 4 Do one of the following:

- To apply the changes, click **Submit**.
- To cancel the changes, click **Cancel**.

Important Notes about Software Capture Filters

This section contains important software capture filters details that may be helpful to know.

- For NAM-3 and NAM-NX1 service modules, multiple software filters use the "OR" logic; in other words, if a packet passes any software filter, it is captured.
- If you create a session and then start it, you cannot edit the session or analyze it without stopping it. If you edit a session containing already captured data, you get a warning stating that the session will be cleared and the data removed. If clearing the session and removing the data is acceptable, ignore the warning dialog message, then add a filter to the session and click **Submit** to enable the new filter settings.
- The application filter can be used to filter on the highest layer of the protocol parsing; that is usually a layer 4 protocol (based on port). If you want to filter on the transport protocol (for example, UDP or TCP), you will need to use the IP Protocol selector. Selecting, for example, TCP in the "IP Protocol" selector will filter on all packets using TCP.

Tip Be careful when setting capture software filtering for encapsulation. If you set a software capture filter with encapsulation for the top three network traffic layers only, data displays only if the top three layers match the specified encapsulation type.

Understanding Software Capture Filter Options

You can define a software filter to filter based on any of the following options:

- Source host address
- Destination host address
- Network encapsulation
- VLAN or VLAN range
- Application
- Source port or port range
- Destination port or port range

Software capture filtering is not supported on URL-based applications.

Table C-55 contains descriptions of the Software Filter dialog box fields.

Note The parameters described in the table above are independently evaluated by the NAM. Therefore, the NAM will allow you to enter parameters that are contradictory, but you will not be able to get meaningful results if they do not match.

For example, the parameters Network Encapsulation and Source/Destination Address are independently evaluated. If a filter is specified with contradicting parameters such as "Network Encapsulation=IP4" and "Source Address=an IPv6 address", it will never match any traffic, and the result will be 0 packets captured.

Configuring Hardware Filters

You can use hardware filtering to help limit the amount of traffic allowed into the NAM for processing. In service modules, there is a hardware datapath throughput limitation and hardware filtering helps to reduce the traffic into the NAM. The NAM hardware platforms that support hardware filtering include:

- Service Modules—NAM-3 and NAM-NX1
- Specific NAM 2000 Series Appliances—2204, 2220, and 2320

Depending on your NAM, the hardware filter support varies:

- Creating NAM Service Modules Hardware Filters, page 4-9
- Creating NAM Appliance Hardware Filters, page 4-14

Creating NAM Service Modules Hardware Filters

This section is applicable only for NAM-3 and NAM-NX1 service modules.

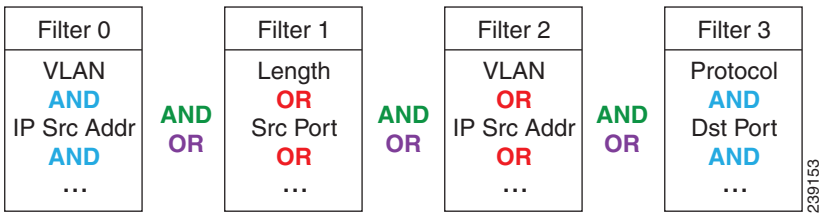
NAM-3 and NAM-NX1 service modules have specific hardware filter logic. These hardware filters allow you to improve capture performance by eliminating extraneous traffic, since packets excluded from capture processing.

Hardware filters and global packet slicing affect all capture sessions, except for ERSPAN capture sessions. See Figure 4-3, "NAM Capture Sessions Example" for an architectural overview.

NAM-3 and NAM-NX1 support up to four hardware filters. You can disable hardware filters without deleting them.

Within each filter, you can set up conditions with the AND/OR logic. Only the same logic type can be used within the same filter; you cannot mix the AND/OR logic within the same filter. Also, you can combine the filters together with the AND/OR logic. See Figure 4-2 for examples of filter logic you can use.

Figure 4-2 Hardware Filter Logic (AND/OR)



The selections are described in the following sections. For information about how you can achieve specific results, see Configuring Hardware Filter Examples, page 4-11.

Tip Software filters add flexibility to your filtering, but hardware filters are most efficient. The less traffic that requires software filtering, the more efficient the filtering.

See these topics for information about setting up and managing hardware filters:

- Creating or Editing a NAM Services Modules Hardware Filter, page 4-10
- Configuring Hardware Filter Settings, page 4-10
- Configuring Hardware Filter Examples, page 4-11

Choose **Capture > Packet Capture/Decode > Sessions** to view the status and settings of hardware filters that are configured on the Cisco NAM. The Hardware Filters box appears at the bottom of the Sessions page.

Creating or Editing a NAM Services Modules Hardware Filter

The Hardware Filters window displays the status and settings of the hardware filters if they have been defined. To configure a capture with hardware filters:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**. The top half of the window shows Capture Sessions, and the bottom half of the window shows Hardware Filters.

Step 2 In the Hardware Filters section on the bottom of the window, click **Create**. The Hardware Filter Dialog appears.

Step 3 Enter a name for the hardware filter in the Name field. The name should be less than 40 characters and contain only supported characters.

Step 4 Check the **Enable** check box to enable the filter. If the filter is created with the Enable check box unchecked, the filter will be saved but inactive. It can be enabled at a later time by editing the filter and checking the **Enable** check box.

Step 5 Choose either the **AND** or the **OR** radio button. This selection will apply to all of the selections you make in the next step (the selections are described in Table 4-3).

Step 6 Check the boxes for the attributes you want to filter on, and then in the corresponding drop-down menu, select the desired option. The **Check All** check box selects all check boxes. See Table C-53.

Step 7 Click **Apply** to complete the configuration of the hardware filter.

Configuring Hardware Filter Settings

The Hardware Filter Settings allows you to set global settings for all capture hardware filters.

To add settings that apply to all hardware filters:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**.

Step 2 In the Hardware Filters section at the bottom, click **Hardware Filter Settings**.

Step 3 Choose the **AND** or **OR** Combination Logic, which will be applied to all configured hardware filters. This logic is used to combine the filters; see the green text in Figure 4-2.

Step 4 Choose the **Include in capture** or **Exclude from capture** Packet Match Logic. This selection will apply to all configured hardware filters.

Exclude from capture will drop packets that match all of the hardware filters you have configured. Meanwhile, all packets that do not match will be captured.

Step 5 Click **Apply**.

Configuring Hardware Filter Examples

Use these topics to configure the following network traffic:

IP Subnet + L4 Port (L5 Application)

To capture all HTTP traffic emanating from the 10.1.1.0/24 subnet:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **AND** radio button (this will combine the selections you make below).

Step 4 Check the **Source IP Address** check box and enter the subnet “10.1.1.0/24”.

Step 5 Check the **L4 Source Port** check box and enter the port “80” for HTTP.

Step 6 Click **Apply**.

To see the opposite direction of the HTTP conversations:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **AND** radio button.

Step 4 Select **Destination IP Address** and enter the same subnet as before, 10.1.1.0/24

Step 5 Select **L4 Destination Port** and enter the same port, 80.

Step 6 Click **Apply**.

Step 7 To see the incoming and the outgoing, click **Hardware Filter Settings** and select the **OR** logic. This will combine the two hardware filters with the OR logic.

VLAN + L4 Protocol

To see all TCP traffic from VLAN 100:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **AND** radio button.

Step 4 Select **VLAN** and enter the VLAN, 100.

Step 5 Select **L4 Protocol** and choose TCP.

Step 6 Click **Apply**.

Multiple Hosts

To see traffic sent to and from multiple hosts: 1.1.1.1, 2.2.2.2, ...:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **OR** radio button.

Step 4 Check the **Source IP Address** check box and enter the first host: 1.1.1.1.

Step 5 Check the **Destination IP Address** and enter the same host: 1.1.1.1.

Step 6 Click **Apply**.

Step 7 Click **Create** to make a second hardware filter.

Step 8 Enter a name for the hardware filter in the Name field.

Step 9 Choose the Logic **OR** radio button.

Step 10 Check the **Source IP Address** check box and enter the second host, “2.2.2.2”.

Step 11 Check the **Destination IP Address** check box and enter the second host, “2.2.2.2”.

Step 12 Click **Apply**.

Step 13 Repeat Step 7 through Step 12 for a third and fourth host, if desired.

Step 14 Click **Hardware Filter Settings** and select the logic **OR** radio button.

VLAN Range

To see all traffic from VLANS 10 through 20:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Check the check box for **VLAN IDs** and choose **Greater Than** from the drop-down menu.

Step 4 In the empty field, enter the bottom VLAN range boundary, “9.”

Step 5 Click **Apply**.

Step 6 Click **Create** to make a second filter.

Step 7 Enter a name in the Name field.

Step 8 Check the check box for **VLAN IDs** and choose **Less Than** from the drop-down menu.

Step 9 In the empty field, enter the bottom VLAN range boundary, “21.”

Step 10 Click **Apply**.

Step 11 Click **Hardware Filter Settings** and select the **AND** radio button, which will combine the logic of all hardware filters.

Data Port + Frame Length

To see all traffic spanned to DATA PORT 1 that is less than 200 bytes:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **AND** radio button.

Step 4 In the **Data Port** drop-down list, choose **DATA PORT 1**.

Step 5 Check the check box for **Frame Length** and choose **Less Than** from the drop-down menu.

Step 6 In the empty field, enter the frame length ceiling, "200."

Step 7 Click **Apply**.

MPLS

To see traffic in which the first MPLS label is 300:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Check the check box for **MPLS Label**.

Step 4 In the empty field, enter the label, "300."

Step 5 Click **Apply**.

Bi-Direction Conversation

To see both directions of a conversation between hosts 1.1.1.1 and 2.2.2.2:

Step 1 On the Hardware Filters window, click **Create**.

Step 2 Enter a name in the Name field.

Step 3 Choose the Logic **AND** radio button.

Step 4 Click the **Source IP Address/Mask** check box, select **Equal To** from the drop-down menu, and enter the first host: "1.1.1.1".

Step 5 Select the **Destination Address/Mask** check box, select **Equal To** from the drop-down menu, and enter the second host: "2.2.2.2."

Step 6 Click **Apply**.

Step 7 Click **Create** to make a second hardware filter.

Step 8 Enter a name for the hardware filter in the Name field.

Step 9 Choose the Logic **AND** radio button.

Step 10 Click the **Source IP Address/Mask** check box, select **Equal To** from the drop-down menu, and enter the second host: 2.2.2.2.

Step 11 Select the **Destination Address/Mask** check box, select **Equal To** from the drop-down menu, and enter the first host: 1.1.1.1.

Step 12 Click **Apply**.

Step 13 Click **Hardware Filter Settings** and click **OR**.

Step 14 Click **Apply**.

Negative Filter Logic

In the previous example, you set up filters that match the packets. For negative filter logic, these now need to be blocked.

To see everything except the conversation from the previous example:

Step 1 On the Hardware Filters window, click **Hardware Filter Settings**.

Step 2 For Packet Match Logic, select the **Exclude from capture** radio button.

Step 3 Click **Apply**.

Go to the next section, Understanding Global Capture Settings, page 4-17, for information about configuring software filters for capture sessions.

Creating NAM Appliance Hardware Filters

This section describes how to create NAM appliance hardware filters.

Hardware filters allow you to improve capture performance by eliminating extraneous traffic, since packets filtered out are excluded from capture processing. This section applies to the NAM 2204, 2220, and 2320 appliances.

Note The NAM 2304 does not support hardware filters.

Software filters add flexibility to your filtering, but a capture session is most efficient when you use only hardware filters. The less traffic requiring software filtering, the more efficient the filtering.

For the NAM appliances that support hardware filtering, you can set up to five hardware filters per appliance.

Hardware filters and global packet slicing affect all capture sessions, except for ERSPAN capture sessions.

See Configuring Supported NAM Appliance Hardware Filters, page 4-14 for detailed steps.

Configuring Supported NAM Appliance Hardware Filters

The Hardware Filters window appears at the bottom of the **Capture > Packet Capture/Decode > Sessions** window. To configure a hardware filter:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**.

Step 2 At the bottom of the window, select a data port hardware filter and click **Create**.

Step 3 Enter a name in the Name field.

Step 4 Choose any or all of the following types of filters:

- Frame Length
- VLAN IDs
- MPLS Label
- Source Address/Mask
- Destination Address/Mask
- L4 Protocol
- L4 Source Port
- L4 Destination Port
- IP and Payload Data
- Payload Data

Step 5 Data fields will then appear that correspond with the type of hardware filter you select. Fill in the desired fields.

Step 6 Click **Submit** to complete the configuration of the capture session.

IP and Payload Data

To configure an IP and Payload Data hardware filter:

Step 1 Enter a Filter Name and select your options.

Step 2 Enter a Source Address / Mask (optional).

Step 3 Enter a Destination Address / Mask (optional).

Step 4 Choose a Layer 4 Protocol, either TCP or UDP.

Step 5 Enter the values for Pattern Match:

- Enter a Value of up to four bytes (eight hex characters).
- Enter a Mask of up to four bytes (eight hex characters).
- Enter an Offset from 1-1023. The offset is relative to the beginning of the payload (Layer 5).

Note Only one payload segment (one row) is required and provided. This is to guard against overlapping payload segments. If overlapping segments have different values the filter will never match anything due to the inherent AND logic.

Step 6 Click **Submit**.

Payload Data

To configure a Payload Data hardware filter:

Step 1 Enter a Filter Name.

Step 2 Choose a Layer 4 Protocol, either TCP or UDP.

Step 3 Enter the values for Payload Data:

- Enter a Value of up to four bytes (eight hex characters).
- Enter a Mask of up to four bytes (eight hex characters).
- Enter an Offset from 1-1023. The offset is relative to the beginning of the payload (Layer 5).

Note Only one payload segment (one row) is required and provided. This is to guard against overlapping payload segments. If overlapping segments have different values the filter will never match anything due to the inherent AND logic.

Step 4 Click **Submit**.

Understanding Hardware and Software Capture Sessions Filters

You can filter specific traffic data and manage that information in local or remote storage. This increases your visibility into network issues and allows you to filter out unnecessary information. You can use either hardware or software filters to target specific packet data to receive.

As shown in Figure 4-3, if network packets coming into the NAM pass through the hardware filters you have configured, the packets go on to the next step. If no hardware filters are configured, all packets pass through.

Note Hardware filters are supported on specific Prime NAM platforms. See Configuring Hardware Filters, page 4-9 for details.

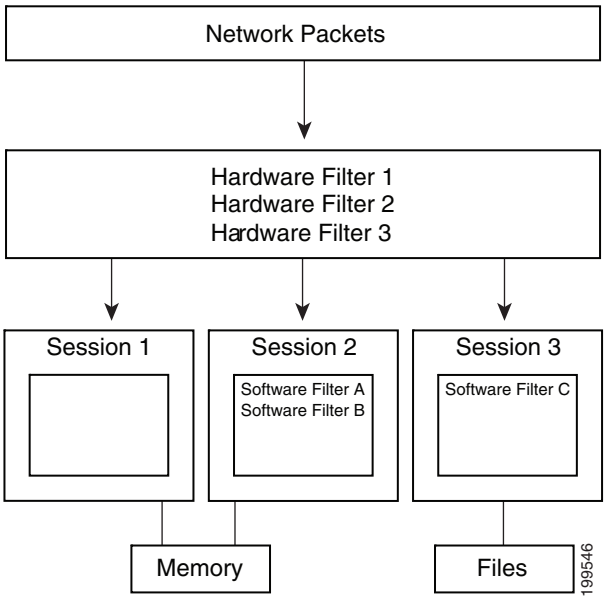
Packets must then pass at least one software filter in that particular session to be saved by that session. If no software filters are configured for a session, then all packets are captured. For more information about software filters, see Configuring Software Filters, page 4-7.

For better performance for the supported NAM platforms, hardware filters are recommended over software filters, and fewer sessions are recommended over more sessions.

You do not have to configure the items in Figure 4-3 in any particular order. For example, you can set Global Capture Settings first, and then configure Capture Sessions, and then create filters; or, you can create Hardware and Software filters first, and then configure Capture Sessions, and finally apply Global Capture Settings. We recommend that you “Start” the session last; otherwise, you will start capturing before you have configured any filters and before doing any packet slicing.

Global Capture Settings and Hardware Filters can be changed at any time, even when the session is running; they will affect running capture sessions immediately. We recommend that you first stop your capture session to edit it since you may capture some unexpected packets during the filter change. See Understanding Global Capture Settings, page 4-17 for details.

Figure 4-3 NAM Capture Sessions Example



Viewing Capture Sessions

To access the basic operations for capturing, viewing and decoding packet data on the NAM, choose **Capture > Packet Capture/Decode > Sessions**.

The Capture Sessions window shows the list of capture sessions. If none have been configured, the list will be blank. Table C-48 describes the Capture Sessions fields and operations that you can perform from the Capture Sessions window.

Understanding Global Capture Settings

You can limit the size of the captured packets by using the Global Capture Settings to apply a custom packet slice and error settings for all capture sessions. This setting applies to NAM-3 and NAM-NX1 only. You can change these settings even when a filter is running since they affect the running sessions immediately.

To enable the Global Capture Settings, click Global Capture Settings in the **Capture > Packet Capture/Decode > Sessions** then click **Enable** and complete your selections.

To understand these settings see:

- Global Packet Slicing
- Error Packets

Global Packet Slicing

Global packet slicing affects all capture sessions, as opposed to the per-session Packet Slice Size parameter, and is performed in hardware. Use this feature to capture packets more efficiently when only the first N bytes are of interest to you. The capture buffer/file is smaller and the NAM is able to capture more packets per second.

The default setting for Global Packet Slicing is Disabled.

This setting overrides individual capture session software slicing settings if it is shorter. For example, if you have a capture session with the slicing field set to 100, but you also have Global Packet Slicing set to 56, then all packets will be sliced down to 56 bytes.

Hardware filters and global packet slicing affect all capture sessions, except for ERSPAN capture sessions.

In addition to global packet slicing you can set choose to allow error packets in the packet. For details on error packet settings, see Error Packets, page 4-18.

Error Packets

Error packets are packets that would normally be dropped by the network interface card, such as under size and over size packets, as well as packets with CRC errors. Error packets can be very helpful for troubleshooting the network.

If you want to customize how Prime NAM treats error packets use the following options:

- **Include in capture** (Default)—Includes packets with and without errors.
- **Exclude from capture**—Omits error packets. The packet capture only includes packets without errors.
- **Only error packets in capture**—Omits packets without errors. The packet capture includes only packets with errors. This option will save disk space but may not be as helpful since you may be unable to see the big picture view of all packet details.

  This setting applies to all capture sessions on NAM-3 and NAM-NX1 only.

  This setting is applied to all capture sessions. In addition to setting error packets, you can also enable global packet slicing. For details on global packet slicing settings, see Global Packet Slicing, page 4-17.

Working with Capture Files

To decode, download, rename, convert/merge, delete, analyze, or error-scan saved packet capture files use the Files option.

This section covers the following topics:

Analyzing Capture Files

The Capture Files window (available at **Capture > Packet Capture/Decode > Files**) enables you to obtain various statistics including traffic rate (bytes/second) over a capture period and lists of hosts and protocols associated with network traffic.

This window also enables you to drill down for a more detailed look at a particular set of network traffic. The pane above the **Traffic over Time** graph displays the time shown in the graph in the **From:** and **To:** fields. It also provides fields for Protocol and Host/subnet, and a **Drill-Down** button.

Note After clicking the **Drill-Down** button, the Host Statistics results table will display both source and destination hosts, if either the source or destination host of the traffic belongs to the Host/Subnet that you had specified.

Each slice in the **Traffic over Time** graph displays the amount of traffic for the amount of time set in the Granularity of the capture file.

You can view more detail about a specific time frame by entering the time in the **From:** and **To:** fields and choosing **Drill-Down**. You can also drill down on a specific **Protocol** or **Host/subnet** address.

Table C-47 describes the different areas of the Capture Analysis window.

Drilling Down into Packet Error Details

You can further investigate, or drill down, into packet error details by viewing the decode packet data available on Prime NAM.

The Capture Errors and Warnings Information window shows warnings and errors, and packet irregularities. From here, you can launch the Packet Decode Window, where you can drill down to packet details.

To get to the Capture Errors and Warnings Information window, choose **Capture > Packet Capture/Decode > Files**. Highlight a file and click the **Errors Scan** button. The Error Scan window displays. The fields are described in Table C-50. Then select the packet details by selecting a row and clicking the **Decode Packets** button.

Downloading Capture Files

You can only download one capture file at a time. To download a capture file to your computer:

Step 1 Choose **Capture > Packet Capture/Decode > Files**.

Step 2 Choose a capture file from the list of captures.

Step 3 Click **Download**.

A **File Download** dialog box displays and asks "**Do you want to save this file?**"

Step 4 Click **Save**.

A **Save As** dialog box opens and provides a way for you to rename and save the file at a location of your choice.

Deleting a Capture File

To delete a capture file:

Step 1 Choose **Capture > Packet Capture/Decode > Files**.

Step 2 Check the check box to select a capture file from the list of captures, or select more than one if desired.

Step 3 Click **Delete**. A dialog box displays and asks "**Delete the following file(s)?**" and displays the file name.

Step 4 Click **OK** to delete the file(s) or **Cancel** to allow the file(s) to remain.

Deleting Multiple Capture Files

To delete all capture files at once:

Step 1 Choose **Capture > Packet Capture/Decode > Files**.

Step 2 Check at least one check box to select a capture.

Step 3 Click **Delete All** to delete all captures.

A dialog box displays and asks "**Are you sure you want to delete all files?**"

Step 4 Click **OK** to delete all the files or **Cancel** to allow them to remain.

Understanding Capture Sessions

To understand how Prime NAM creates capture files with saved packet data, it is important to learn about how NAM handles capture session triggers.

This section contains the following topics:

Types of Capture Triggers

Packet capture sessions can be triggered on the Prime NAM in several ways:

- Manually, by starting a capture using the Capture menu option or clicking the Start capture button.
- Scheduled, by specifying a start date/time and maximum duration when you create or edit a capture session.
- Alarmed, by creating an alarm with an associated trigger capture action that starts a particular capture session.

Resolving Session Conflicts

Prime NAM supports multiple capture sessions associated with the same capture storage location, but only one of these sessions can be running at any given time. Since there are several ways for such capture session to be started, it is possible for conflicts to arise among such capture sessions.

For example, suppose one capture session is started manually, but another capture session is scheduled to begin capturing while the first is still running. If these two sessions capture to the same storage location, there is a conflict. In this case, Prime NAM resolves the conflict by automatically stopping the manual session and allowing the scheduled session to begin.

In general, NAM resolves capture session conflicts by prioritizing them in the following (descending) order:

1. High-severity alarm triggered capture
2. Low-severity alarm triggered capture
3. Scheduled capture
4. Manual capture

For example, if a manually started capture session is saving data to the local disk and a scheduled capture is set to begin capturing to the same local disk, Prime NAM stops the manual session before the scheduled session begins.

If there are existing capture sessions already running on the same storage target, this means there is a conflicting alarm trigger. An alarm trigger is created when you configure an alarm threshold to start collecting packet data. Each alarm has a severity option.

Once a capture session is completed, you can manipulate the file. See

Manipulating Capture Files

This section provides an overview of the tasks you can complete with capture files. See Table 4-2.

For information about how to save capture sessions to files, see Creating and Managing Capture Sessions, page 4-6.

Caution If you have capture files with a state of ***Full*** and the NAM is rebooted, the capture is triggered again and these files may be overwritten by the new capture. If you want to retain the file, save the file before you reboot.

Table 4-2Actions You Can Complete with Capture Files

Action	Description
Decode	Display the packets in a file.
Download	Download a file to your computer in **.pcap** file format (based on your settings in Administration > System > Preferences). **Note** Do not add a file suffix when you provide the filename. The suffix **.pcap** is added automatically.
Rename	Give the file a new name. A dialog box displays and asks you to enter the new name for the selected capture file.

Table 4-2Actions You Can Complete with Capture Files (continued)

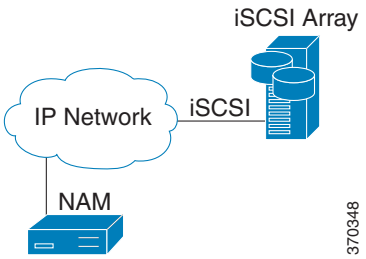
Action	Description
Merge	Merges capture files that were captured simultaneously in chronological order. **Note** Merged files cannot exceed 2,000 MB.
Delete	Delete selected capture files.
Analyze	View statistical analysis of the selected capture. See Analyzing Capture Files, page 4-18.
Errors Scan	View more information about the file (Packed ID, Protocol, Severity, Group, and Description). From here you can also decode the packet. For more information see Drilling Down into Packet Error Details, page 4-19.

Utilizing Capture Data Storage

Cisco Prime Network Analysis Module platforms offer external storage connectivity for extended capture durations and higher capture bandwidths. All platforms support iSCSI data storage. Some platforms may support other forms of data storage, but this document covers only iSCSI data storage.

This section covers the following topics:

Figure 4-4 External Storage Setup



For instructions on installing and configuring external storage not covered here, see your platform-specific guides on Cisco.com or related documentation in the *Cisco NAM Documentation Overview*.

About Capturing to Data Storage

To avoid filling up the local server disk on the NAM, you can capture files to external storage. One of the benefits of using external storage is that it can provide larger capacities, higher read/write speeds, and can be moved from one Cisco NAM to another. The capture files are decoded in the same manner as the **Capture > Packet Capture/Decode > Files** page.

Using Prime NAM, you can perform internal and external storage management using **Capture > Packet Capture/Decode > Data Storage.** This window lists detected storage devices, including the internal hard drive, if one is available. For details on how to install and configure local and external storage, see Installing and Configuring Local and External Storage, page 4-23.

This release supports 32 external data storage targets, or Logical Unit Numbers (LUNs).

You can create multiple capture sessions per target. Only one capture per storage target (file location) is allowed at a time. Additionally you can have multiple sessions to memory.

Installing and Configuring Local and External Storage

You can use local or external storage as a repository for long term data for performance comparisons.

This topic covers:

Configuring the iSCSI Array

You may decide that in addition to or instead of local storage that you want to set up an external storage drive using iSCSI. This section contains the required settings for Prime NAM.

Use your vendor's user documentation to ensure you have properly configured the iSCSI array. The Prime NAM is independent of most array settings, but some are important for accessibility and performance.

Step 1 To configure the disk volumes on the array there is often a *Segment Size* setting. Larger segment sizes can improve write speeds. Configure the *Segment Size* setting to use the largest possible segment size (up to 512 KB).

Multiple volumes can be configured on a single array.

Step 2 Assign a Logical Unit Number (LUN) to the disk volume. This number is used for volume identification by the host.

Step 3 Map the LUNs to iSCSI Qualified Names (IQNs) on the array. Each IQN represents a different list of LUNs which hosts (such as the Prime NAM) can access.

Prime NAM supports up to 32 LUNs between all protocols and multiple LUNs mapped to one IQN.

Step 4 Prime NAM also has an IQN, which represents the host side of an iSCSI session. You must give the Prime NAM's IQN access to the iSCSI array's LUNs. The array calls this *Host Access*. Be sure to give the Prime NAM's IQN read-write access. Most arrays require this for security reasons to ensure that only certain hosts can access the LUNs.

Each Prime NAM has a unique IQN, so perform this required step for each Prime NAM that requires access and for each target LUN that you want to access. For more details about which CLI command to use, see Locating the Prime NAM IQN, page 4-24.

Caution Only one Prime NAM should connect to a LUN because only one host can have write access at a time. If multiple Prime NAMs connect to the same LUN simultaneously, there will be access conflicts and capture operations may not work properly.

Step 5 Ensure the Prime NAM management port has IP connectivity to the iSCSI array. For details on how to complete this required task, see Connecting the Storage Array, page 4-24.

Locating the Prime NAM IQN

To find the Prime NAM IQN, use the **remote-storage iscsi local-iqn** CLI command:

```
root@nam.domain# remote-storage iscsi local-iqn
Local iSCSI Qualified Name: iqn.1987-05.com.cisco:WS-SVC-NAM3-6G-K9.00:19:55:07:15:9A
```

For details on how to complete the storage array configuration, see Connecting the Storage Array, page 4-24.

Connecting the Storage Array

After you configure the iSCSI storage arrays, ensure that the array has an IP path to the Prime NAM management port. The array can be connected while the Prime NAM is running.

Some arrays come with multiple storage controller modules. As a security feature, module ownership must often be mapped to each LUN or IQN.

The Prime NAM logs into the storage to start an iSCSI session using the IP address and IQN(s) of the storage array.

To connect the storage array using the user interface:

Step 1 Log into the Prime NAM web interface. To access the Data Storage page, choose **Capture > Packet Capture/Decode > Data Storage**.

Step 2 Click **iSCSI Login** and enter the iSCSI array IP address. Then click **Search IQN Targets**.

A list of IQNs available to the Prime NAMs host IQN appear.

Step 3 Depending on the outcome, perform one of the following steps:

a. If the IQNs do not appear, check **remote-storage iscsi list** to verify the iSCSI session was properly started.

The follow example shows how to verify the iSCSI session.

```
root@nam.domain# remote-storage iscsi list
Storage ID: 16
Label:
Status: Ready
Protocol: ISCSI
Target IP: 172.20.122.81
Target IQN: iqn.2011-09:celeros.target11
Type: LUN
Model: IET VIRTUAL-DISK
```

```
LUN: 4
Capacity: 24.98GB
Available: 24.98GB
Active iSCSI Sessions:
tcp: [8] 172.20.122.81:3260,1 iqn.2011-09:celeros.target11
```

The LUN number (in the above example, *LUN 4)* helps you identify one LUN from others mapped to the same IQN. This number is unique to each IQN, meaning two LUNs from different IQNs can have the same number.

b. If the iSCSI session was properly started, check the storage array configuration to verify that:

- The LUNs are mapped to the target IQN, and
- The Prime NAM IQN has been given Read/Write access to the LUNs.

c. If you make any configuration changes, logout of the iSCSI session and login again. To logout, use the CLI **remote-storage iscsi logout** or use the GUI and click **iSCSI Logout**. All LUNs mapped to that target IQN will be disconnected from the Prime NAM.

Preparing LUNs for File Storage

Some arrays come with multiple storage controller modules, and the module ownership must often be mapped to each LUN (Logical Unit Numbers). This is a common security feature.

To see if the NAM can access the storage array LUNs and prepare them to store files:

Step 1 Choose **Capture > Packet Capture/Decode > Data Storage**.

New LUNs which have not been used by the NAM show a status of *Unformatted*.

a. Skip to Step 3 if your LUNs are formatted.

b. If no LUNs appear, see Installing and Configuring Local and External Storage, page 4-23 and Configuring the iSCSI Array, page 4-23 for detailed instructions on how to set up your storage array.

Step 2 To prepare these LUNs for capture use, select the LUN and click **Format**. After a few minutes, the status should change to *Ready.*

Step 3 To apply optional user labels to the LUNs to help differentiate between them, select the LUN and click **Label**.

The Label dialog appears with information about the current label and the last time the LUN was formatted.

You are now ready to use the external storage for capture files.

Using LUNs to Store Packets from a Capture Session

To use a LUN to store packets from a capture session:

Step 1 Go to **Capture > Packet Capture/Decode > Sessions**.

Step 2 Under the Capture Sessions table, click **Create**.

Step 3 Fill in the appropriate fields for creating a session, and for Storage Type choose the **Files** option.

Step 4 Use the File Location table to select the LUN you wish to use. Each list entry includes the protocol and either the model or the user label if it is set. Note that the list will only include targets which are in the *Ready* state.

Step 5 Click **Submit** to create the session.

When a session is *STARTED*, the associated LUN state changes to *In Use*. At that point, no other session can use that LUN until the session is deleted. This prevents contention, corrupted data, and write bandwidth degradation.

Logging In and Out of External Storage LUNs

You can use iSCSI to facilitate data transfers over intranets and to manage your remote capture data storage.

Prime NAM provides a more streamlined workflow to log in and out of your data storage targets. You must log into iSCSI in order to save capture sessions to remote storage. If you do not log in, capture sessions are saved to either local disk or memory locations.

To log in or out of your available remote data storage LUNs:

Step 1 Ensure you have configured your target iSCSI system with read/write permission to your NAM for at least one LUN in the storage array. For details, see About Capturing to Data Storage, page 4-22.

Step 2 Choose **Capture > Packet Capture/Decode > Data Storage** and click **iSCSI Login**.

Step 3 To enable auto discovery of any iSCSI Qualified Name (IQN) target, enter the target IP address of the storage location and click **Search IQN Targets**.

All available IQNs for that location display in the table.

Step 4 To log out, click **iSCSI Logout**. The list of IQNs to which you are currently logged into displays in a table.

Step 5 To view the LUNs which the system will log you out, select one of the IQNs and a popup displays the associated LUNs to select.

Connecting and Disconnecting External Storage

Before physically disconnecting an external storage device, it is highly recommended to use the **Unmount** button on the **Capture > Packet Capture/Decode > Storage** window. This notifies the Cisco NAM that the device will be disconnected, so that the Prime NAM can perform important cleanup procedures. After this is done, the storage target displays as *Unmounted* in the status column, and it is safe to remove the external storage device. External storage is automatically unmounted in this manner when the Cisco NAM is powered down.

Caution If this step is skipped, it is possible to corrupt the storage data upon physical disconnect.

If a device has been logically disconnected using the **Unmount** button, but the storage is still physically connected, it can be reactivated using the **Mount** button. It will restore the storage target's previous state. This makes it unnecessary to physically disconnect and reconnect the storage, which can be particularly useful if the storage is located far away from you.

Recovering Data Storage

In the event that a previously working target displays as *Unformatted*, you can use the CLI to determine what happened by running a filesystem check on it. Use the command **remote-storage <protocol> fsck <storage ID>**, when you know the protocol. You can find the storage ID using **remote-storage <protocol> list**. The filesystem check can potentially resolve filesystem corruption or state issues. If the command succeeds, it automatically mounts the storage and displays as *Ready.*

The following shows a iSCSI recovery example:

```
root@nam.cisco.com# remote-storage iscsi list
Storage ID: 16
     Label:
    Status: Unformatted
  Protocol: ISCSI
 Target IP: 172.20.10.81
Target IQN: iqn.2011-09:celeros.target11
Model: IET VIRTUAL-DISK
       LUN: 4
  Capacity: 24.98GB
 Available: 24.98GB

Storage ID: 15
     Label: target 16
    Status: In Use
  Protocol: ISCSI
 Target IP: 172.20.10.81
Target IQN: iqn.2011-09:celeros.target16
Model: IET VIRTUAL-DISK
       LUN: 5
  Capacity: 24.98GB
 Available: 16.47GB

Active iSCSI Sessions:
tcp: [8] 172.20.10.81:3260,1 iqn.2011-09:celeros.target11
tcp: [7] 172.20.10.81:3260,1 iqn.2011-09:celeros.target16

root@nam.cisco.com# remote-storage iscsi fsck 16
FS check completed successfully.
root@nam.cisco.com# remote-storage iscsi list
Storage ID: 16
     Label:
    Status: Ready
  Protocol: ISCSI
 Target IP: 172.20.10.81
Target IQN: iqn.2011-09:celeros.target11
Model: IET VIRTUAL-DISK
       LUN: 4
  Capacity: 24.98GB
 Available: 9.87GB

Storage ID: 15
     Label: target 16
    Status: In Use
  Protocol: ISCSI
 Target IP: 172.20.10.81
```

```
Target IQN: iqn.2011-09:celeros.target16
Model: IET VIRTUAL-DISK
       LUN: 5
  Capacity: 24.98GB
 Available: 16.47GB

Active iSCSI Sessions:
tcp: [8] 172.20.10.81:3260,1 iqn.2011-09:celeros.target11
tcp: [7] 172.20.10.81:3260,1 iqn.2011-09:celeros.target16
```

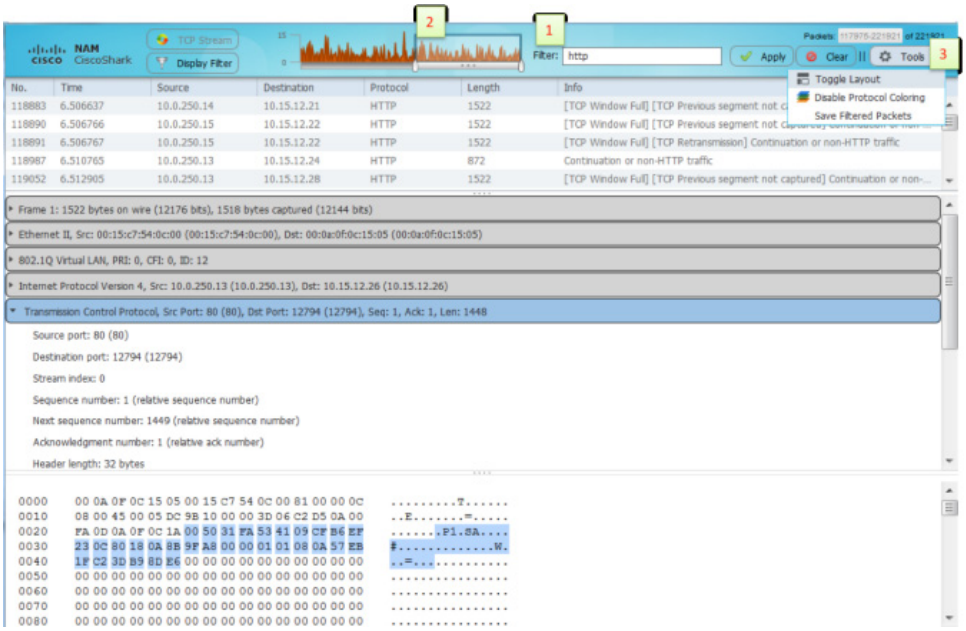
Inspecting Packet Decode Information for Suspicious Traffic

After you have captured some traffic data packets, you can use the NAM Packet Analyzer to view the packet contents and inspect for suspicious traffic.

This section includes the following sections:

Analyzing Packets in the NAM Packet Analyzer

Figure 4-5 NAM Packet Analyzer Window



Note To use these decode features, you must be capturing to memory with the no rotate option selected. Otherwise, captures must be paused or stopped. For detailed descriptions about the features in this window, see Understanding the NAM Packet Analyzer.

To inspect packet decode information for suspicious traffic:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session. If you already have a capture session choose **Capture > Packet Capture/Decode > Files**.

Step 2 Choose a capture session or file, and then click **Decode**. The NAM Packet Analyzer window displays. See Figure 4-5. For table descriptions see Table C-53.

Step 3 To quickly filter on a key word or phrase, for example rtp to focus on voice quality, enter the word in the Filter text box (see callout 1 in Figure 4-5). The window refreshes displaying only data that includes the filtered information.

Step 4 To filter packet data based on multiple filters, click **Display Filter** and enter your options in the window, then click **Apply**. This action displays only the distribution of the packets that match your filter. For detailed steps, see Filtering Packets Displayed in the NAM Packet Analyzer, page 4-30.

Step 5 To save filters for future use, click **Saved Filters** on the Display Filter window. You can also edit or remove existing filters as needed.

Step 6 To view the packet capture flow and focus in on a specific time interval or area of interest click on the slider in the Packet Histogram and move the left or right cursors to zoom in (see callout 2 in Figure 4-5). To pan this filtered data, click and hold the slider while moving it inside the histogram. This provides a visual of packet capture flow and enables you to navigate through the packet list.

Step 7 To toggle

- between a one and two-column layout view, choose **Tools > Toggle Layout**.
- between the Packet Histogram and the packet paging controls, choose **Tools > Show ...**

Step 8 To disable the default colors in the packet window, choose **Tools > Disable Protocol Coloring**.

Step 9 To review capture file information, choose **Tools > Capture Info**.

Step 10 To save the current filtered packet info displayed on this page, choose **Tools > Save Filtered Packets**. Only visible when filters are in use. Saves to memory or to the capture file based on the options in your Capture Sessions window. See Configuring Capture Sessions, page 4-6.

Step 11 To make the font size larger or smaller for the hex data pane, hover over the top-right corner of the pane to see the enlarge option. To increase the font, select the **A+** or to decrease it select the **A-**.

Step 12 Use the Tools menu to perform validation tasks—options have limited support. Options include:

- TCP Checksum Validation check box—filter on TCP in the decode window and use the TCP pane to verify that the checksum has been validated.
- UDP Checksum Validations check box—filter on UDP in the decode window and use the UDP pane to verify that the checksum has been validated.
- IP Host Name Resolution—perform global host name resolution for NAM. Synchronizes with the Administration preferences.

Step 13 To view packet details including packet range displayed, data port, and number of filtered packets, see the heading in the upper right corner of the NAM Packet Analyzer window.

Filtering Packets Displayed in the NAM Packet Analyzer

To filter packets based on multiple options for display in the NAM Packet Analyzer:

Step 1 From the NAM Packet Analyzer, click **Display Filter**. The NAM Packet Analyzer - Display Filter Window displays.

Step 2 Do the following:

- Choose a **Filter Mode**:
  - **Inclusive** displays packets that match the condition(s.)
  - **Exclusive** displays packets that do not match the condition(s).
- Choose an **Address Filter**:
  - **IP/Host** address filters on IP address.
  - **MAC** address filters on MAC address.
  - **Source** allows you to specify the source address, or leave it blank if not applicable.
  - **Destination** allows you to specify the destination address, or leave it blank if not applicable.
  - **Both Directions** allows you to match of packets traveling in both directions.
- Define a **Protocol Filter**:
  - Click **Match any (or)** to display packets that match any of the protocols or fields.

  or
  - Click **Match all (and)** to display packets that match all of the protocols or fields.
  - Choose a protocol from the **Protocols** list.

Note You can enter the first few letters of the protocol name to go directly to the protocol. If you make a typo, press **ESC** or **SPACE** to reset.

  - Choose a protocol field from the Fields list, then specify the field value if applicable.

Step 3 To add more protocol filters, click the **+** sign.

Step 4 To delete a defined Protocol Filter, click the **-** sign.

Step 5 Click **OK** to apply the filter and close the window or **Apply** to apply the filter and keep the window open.

Viewing Detailed Protocol Decode Information

To view detailed protocol information:

Step 1 Highlight the packet number about which you want more information.

Detailed information about that packet is displayed in the Protocol Decode and hexadecimal dump panes at the bottom of the window.

Note If you highlight the details in the Protocol Decode pane, the corresponding bytes are highlighted in the hexadecimal dump pane below it.

Step 2 To review the information, use the scrolling bar in the lower panes.

Note When you decode SCCP traffic, Prime NAM lists the protocol as *skinny*, not SCCP.

Tip

- Protocols are color coded both in the Packet Browser and the Protocol Decode pane.
- Choose the protocol name in the Protocol Decode pane to collapse and expand protocol information.
- To adjust the size of any of the panes, click and drag the pane frame up or down.

Understanding the NAM Packet Analyzer

The NAM Packet Analyzer, also known as the packet decoder, uses two levels of packet analysis: basic and full. Because preparing a large capture file for full analysis can take a long time, NAM automatically chooses which level to use based on your filtering complexity. This allows you to browse your captured packet data more quickly without having to wait for analysis.

When you select a capture file to analyze for the first time, NAM limits some of the more complex display filters you can use. For example, you can filter using protocol identifiers such as TCP, UDP, SDP, and SIP which allow the packet decode to display more quickly than an advanced filtering selection.

If you enter more advanced filters (such as those with and/or logic operators on the protocol field), NAM automatically begins the full analysis of the capture file and then applies your complex filter to display the results. For example, if you filter using ‘ip.src==192.168.1.1 && tcp.dstport==80’, the NAM Packet Analyzer starts the full analysis and displays it only after the results have been filtered.

Understanding the NAM Packet Analyzer Window and Browser Pane

The NAM Packet Analyzer window shows three views of a packet:

- a summary line briefly describes the packet type
- the protocol field of interest can be shown and analyzed in the portion of the window directly below the summary line
- a hexadecimal dump shows exactly what the packet looks like when it goes across the wire.

There are many unique features in the NAM Packet Analyzer decode window; for example, it can assemble all the packets in a TCP conversation and highlight the ASCII data in that conversation. You can use the expanded display filter functionality to allow you to view more focused data.

Figure 4-5 is an example of the NAM Packet Analyzer window. Table C-54 describes the packet decoder operations on the NAM Packet Analyzer decoder window.

You can perform the following tasks in the NAM Packet Analyzer window:

- Show Packet histogram display the number of packets over a specific time range. This provides a feel of the packet flow for the capture. You can use the histogram selector control to navigate through the packet list as well. You can apply a display filter to make the histogram show the distribution of the packets that match the applied filter. Can set time range and move across histogram. Firefox is faster than IE performance with this feature.
- Toggle to Show Packet Paging Controls displays the buffer divided into pages.
- Toggle layout changes how the three content panes in the decoder are arranged.
- Display Hex data font size by hovering over two buttons in the top right corner of the hex data content pane of the decoder. You can increase or decrease the font size of the contents.
- Display the current range of packets in the packet list by selecting the Packet range button. You can also enter the range of packets to view.
- Use the Display Filter button yo display Saved Display Filters and Manage Display Filters windows.
- Alter Protocol coloring. You can map custom colors to specific protocols in this release. Default colors
- Use the Tools menu—options have limited support. Options include:
  - TCP Checksum Validation check box—filter on TCP in the decode window and use the TCP pane to verify that the checksum has been validated.
  - UDP Checksum Validations check box—filter on UDP in the decode window and use the UDP pane to verify that the checksum has been validated.
  - IP Host Name Resolution—perform global host name resolution for NAM. Synchronizes with the Administration preferences.
- Display Filter input field to manually enter display filters.

Customizing Display Filters

Use custom display filters to create and save customized filters to use in the NAM Packet Analyzer decode window to limit which packets are displayed.

NAM supports most software display filters with the following exceptions:

- Filters using Perl Regular Expressions. For example:

```
http.request.uri matches "gl=se$"
```

- Filters on a protocol payload (a protocol section in a packet). For example:

```
udp[8:3]==81:60:03
```

See these topics for help setting up and managing custom display filters:

- Creating Custom Display Filters, page 4-33
- Editing or Deleting Custom Display Filters, page 4-35

Creating Custom Display Filters

To create custom display filters:

Step 1 Choose **Capture > Packet Capture/Decode > Sessions**.

The Hardware Filters box is displayed at the bottom of the page.

Step 2 Click **Create**. The Hardware Filters Dialog box displays. See Table C-52.

Step 3 Enter information in each of the fields as appropriate.

Step 4 Do one of the following:

- To create the filter, click **Submit**.
- To cancel filter creation, click **Cancel**.

Tips for Creating Custom Decode Filter Expressions

You can construct custom decode filter expressions using the following logical and comparison operators listed in Table 4-3.

Table 4-3 Logical and Comparison Operators

Operator	Meaning
and	Logical AND
or	Logical OR
xor	Logical XOR
not	Logical NOT
==	Equal
!=	Not equal
>	Greater than

To group subexpressions within parentheses, use the fields in Table C-51 to help you add filter expressions.

Examples of Custom Decode Filter Expressions

Table 4-4 provides some examples of basic NAM display filters you can use to filter on application types.

Table 4-4 Basic NAM Display Filters (Limited to Application Types)

Filter	Meaning
tcp	Find all TCP-based applications
udp	Find all UDP-based applications
! eth	Find all packets other than Ethernet
tcp and not vlan	Find all TCP traffic NOT running over vlan

Table 4-4 Basic NAM Display Filters (Limited to Application Types)

Filter	Meaning
http	Find all src/dst HTTP application packets (may be not standard port 80 if different application 'decode as' port specified; e.g. 'tcp.port==8080,http')
ftp || http	Find either ftp or http packets
not tcp	Exclude all TCP packets
! tcp	Exclude all TCP packets
! (ftp || http)	Exclude all FTP and HTTP packets

Table 4-5 provides some examples of complex NAM display filters.

Table 4-5 Compound NAM Display Filters

Filter	Meaning
tcp.port eq 80	Find all src/dst HTTP packets on standard HTTP port 80
ip.addr == 192.168.1.0/24	Find all packets in Class C network (subnet)
tcp.flags.reset == 1	Find all TCP resets
tcp.window_size == 0 && tcp.flags.reset != 1	Src is instructing dst to stop sending data (TCP buffer full)
Ipv6.addr == ::1	Correct statement with IPv6 label and IPv6 address.

Table 4-6 provides some examples of protocol field hexbyte filters.

Table 4-6 Protocol Field Hexbyte Filters

Filter	Meaning
eth.src==00:3c:06:0a:02:68	Find source MAC
eth.dst==00:3c:06:0a:02:68	Find destination MAC
eth.addr==00:3c:06:0a:02:68	Find source or dest MAC
! (eth.addr==00:3c:06:0a:02:68)	Find all MAC except specific address
eth.addr contains 00:3c	Find bytes in any protocol field subrange

Table 4-7 provides some examples of protocol field hexbyte subrange filters.

Table 4-7 Protocol Field Hexbyte Subrange Filters

Filter	Meaning
eth.addr[0:2]==00:3c	Find specific subrange in MAC
eth.addr[1:3]==3c:06:0a	Find specific subrange in MAC

Table 4-8 provides some examples of hexbyte data representations syntax.

Table 4-8 Hexbyte Data Representations (Syntax)

Filter	Meaning
eth.dst == ff:ff:ff:ff:ff:ff	Hexbyte separators can be colons
eth.dst == ff-ff-ff-ff-ff-ff	Hexbyte separators can be dashes
eth.dst == ffff.ffff.ffff	Hexbyte separators can be dots (one or two bytes

Note You can use a filter expression with other fields in the Custom Decode Filter dialog box. In this case, the filter expression is ANDed with other conditions. Invalid or conflicting filter expressions result in no packet match.

Editing or Deleting Custom Display Filters

To edit custom display filters:

Step 1 From the NAM Packet Analyzer, choose **Display Filters**.

Step 2 To edit a filter, choose the filter to edit then click **Edit**.

Step 3 Change the information in each of the fields as appropriate.

Step 4 To delete a filter, choose the filter to delete from the Hardware Filters Data Port 1 or Data Port 2 pane, then click **Delete**.

Performing User and System Administration

This chapter provides information about what user and system administration tasks are required or optional, how to generate diagnostic information when requesting technical assistance, and provide user access.

This chapter contains the following topics:

Performing System Administration

You can perform the following system administration tasks:

For at-a-glance details on why you may want to perform these system administration tasks, see Table 5-1.

Table 5-1 System Administration At-A-Glance

Task	Choose...
View system health and traffic details	**Administration > System > Overview**
Use IP hostname resolution/DNS lookup	**Administration > System > Network Parameters**
Add extra security and allow additional host details to be displayed in NAM traffic information	**Administration > System > SNMP Agent**
Ensure that the NAM system time is configured correctly (required)	**Administration > System > System Time**
Provide e-mail notification of alarms and reports	**Administration > System > E-Mail Setting**
Allow general web users and websites to access selected NAM monitor and report windows without a login session	**Administration > System > Web Data Publication**
Specify whether syslog messages should be logged locally on the NAM, on a remote host, or both	**Administration > System > Syslog Setting**
Set a host destination to which Prime NAM sends trap	**Administration > System > SNMP Trap Setting**
Change the Prime NAM display or logging characteristics	**Administration > System > Preferences**

Monitoring Prime NAM Health and Traffic Statistics

Ensuring that your Cisco NAM processes your traffic efficiently and effectively without becoming overloaded is a critical task.

To view the network traffic coming into the Cisco NAM as well as data about its health (such as server network details and CPU, memory, and data usage) use **Administration > System > Overview**.

Use the data provided in the Inputs and Resources tabs to determine scalability issues and to assist with troubleshooting.

Table C-56 describes the types of information of the System Overview window.

Setting Network Parameters

If you want to use IP hostname resolution in Prime NAM, you must configure the nameservers first. Prime NAM supports three DNS servers. If this task is not complete, you will be unable to perform DNS lookup. You can also set

Tip Ensure your name server addresses are correct, otherwise some of your Monitor dashboards and Capture Decode windows may seem slow to load.

To view and set your name servers:

Step 1 Choose **Administration > System > Network Parameters**.

The Network Parameters window displays.

Step 2 Enter or change the IPv4 or IPv6 information.

Step 3 To validate the accuracy of the nameservers, click **Validate Nameservers.**

Step 4 Do one of the following:

- To save the changes, click **Submit**.
- To cancel the changes, click **Reset**.

Step 5 Ensure you have turned on IP hostname resolution using **Administration > System > Preferences**. See Customizing System Preferences, page 5-10.

Setting the SNMP Agent

An SNMP Agent is a network management software module that resides in a managed device. It has local knowledge of management information and translates that information into a form compatible with SNMP.

You can manage devices with SNMPv3 in addition to SNMPv2 and SNMPv1. The NAM polls the managed device to get its basic health and interface statistics. For NAM blades, the managed device is the switch in which the NAM is inserted, and the NAM software negotiates with the switch to use SNMP and a community string to do the polling. This community string is only valid for use with the NAM. For security purposes, the switch associates the community string with the NAM's IP address only, and no other SNMP application can use this community string to communicate with the switch. For more information about community strings, see Working with NAM Community Strings, page 5-4.

Also, to further alleviate any security concerns, the SNMP exchanges between NAM blades and the switch take place on an internal backplane bus. These SNMP packets are not visible on any network, nor any interface outside of the switch. It is a completely secure out-of-band channel inside the switch.

For other platforms, such as Cisco NAM appliances, you can type in any IP address and use it as the managed device. In setting managed devices, virtual NAM platforms managed devices function just like the NAM appliances. On all platforms, NAM can only monitor and display data for one managed device at a time.

In this case, the managed device may only want to use SNMPv3 since it is more secure.

Note NAM blades use SNMPv2 to manage the locally managed device.

To view and set the NAM SNMP Agent:

Step 1 Choose **Administration > System > SNMP Agent**.

Step 2 Enter or change the information in the NAM SNMP window. The fields are detailed in Table C-57.

Step 3 To create community strings, see Creating NAM Community Strings, page 5-4.

Step 4 To delete community strings, select the entry and click **Delete**.

Step 5 To save the changes, click **Submit**.

Working with NAM Community Strings

You use community strings so that other applications can send SNMP get and set requests to the NAM, set up collections, poll data, and so on.

Creating NAM Community Strings

To create the NAM community strings:

Step 1 Choose **Administration > System > SNMP Agent**.

Step 2 Click **Create** under NAM Community Strings.

The System SNMP Agent Dialog Box displays.

Step 3 Enter the community string (use a meaningful name).

Step 4 Enter the community string again in the Verify Community field.

Step 5 Assign read-only or read-write permissions using the following criteria:

- Read-only allows only read access to SNMP MIB variables (get).
- Read-write allows full read and write access to SNMP MIB variables (get and set).

Step 6 To make the changes, click **Submit**.

Deleting NAM Community Strings

To delete the NAM community strings:

Step 1 Choose **Administration > System > SNMP Agent**.

Step 2 Select an entry, then click **Delete**.

Caution Deleting the NAM community strings blocks SNMP requests to the NAM from outside SNMP agents.

Testing the Router Community Strings

Before the router can send information to the NAM using SNMP, the router community strings set in the NAM must match the community strings set on the actual router. The Router Parameters dialog box displays the router name, hardware, Supervisor engine software version, system uptime, location, and contact information.

The local router IP address and the SNMP community string must be configured so that the NAM can communicate with the local router.

To set the community strings on the router, use the router CLI. For information on using the CLI, see the documentation that accompanied your device.

Caution The router community string you enter must match the read-write community strings on the router. Otherwise you cannot communicate with the router.

To test router community strings:

Step 1 Choose **Setup > Managed Device > Device Information**.

The Device Information dialog box displays.

Step 2 Enter the Device's Community String.

Step 3 Click **Test Connectivity**.

Step 4 Wait for a while for NAM to communicate with the Device. If it comes back OK, then click on **Submit**.

Synchronizing Your System Time

Ensure that the NAM system time is configured correctly. If the system time is incorrect, NAM data presentation may be inaccurate due to time ranges, hence providing incorrect interpretations of NAM data.

Some platforms are synchronized automatically, but you must also synchronize the standard time source outside the NAM in addition to the NAM and the router, switch, or in order for the data to be accurate. We recommend you perform the time synchronization for your platform, especially if you see the following message on the dashboard interface: `Client or NAM time is incorrect`.

You can configure the NAM system time by using one of the following methods:

- Configuring the NAM System Time with an NTP Server, page 5-6

  This is valid for all platforms and is the recommended option.

- Synchronizing the NAM System Time with the Switch or Router, page 5-6

  This option is valid only for NAM-3, SM-SREs, and NAM-NX1.

- Synchronizing the NAM System Time Locally, page 5-6

  This option is valid for Cisco NAM appliances, Nexus 1000 VSB, and vNAM.
- Configuring the NAM System Time with Precision Time Protocol (IEEE 1588), page 5-7

  This option is valid for NAM-3 and NAM-NX1.

Configuring the NAM System Time with an NTP Server

To configure the NAM system time with an NTP server:

Step 1 Choose **Administration > System > System Time**.

Step 2 Choose the **NTP Server** radio button.

Step 3 Enter one or two NTP server names or IP address in the NTP server name/IP Address text boxes.

Step 4 Select the Region and local time zone from the lists.

Step 5 To save the changes, click **Submit**.

Synchronizing the NAM System Time with the Switch or Router

Note This section is valid only for NAM-3, SM-SREs, and NAM-NX1. For additional platform options, see Synchronizing Your System Time, page 5-5.

To configure the NAM system time from the switch or router:

Step 1 Choose **Administration > System > System Time**.

Step 2 Choose:

- **Local** to sync to your switch or router. If you choose this option you must <is there anything on the router side that needs to be done?>
- **NTP Server**

Step 3 Select the Region and local time zone from the lists. This should be the region in which your NAM is located.

Step 4 Click **Submit**.

Synchronizing the NAM System Time Locally

Note This section is valid for Cisco NAM appliances, Nexus 1000V, and vNAM. For additional platform options, see Synchronizing Your System Time, page 5-5.

To configure the NAM system time locally using the NAM command line:

Step 1 Log into the NAM command line interface.

Step 2 Set the clock using the CLI **clock set** command.

clock set <*hh:mm:ss:*> <*mm/dd/yyyy*>

Step 3 On the Prime NAM GUI, choose **Administration > System > System Time**.

Step 4 Click the **Local** radio button.

Step 5 Select the Region and local time zone from the lists.

Step 6 Click **Submit** to save the changes.

Configuring the NAM System Time with Precision Time Protocol (IEEE 1588)

To use Precision Time Protocol (PTP), you will need to have a PTP-aware or multicast-enabled switch connected to the sync port on the front of the NAM-3 or NAM-NX1, as well as a PTP master connected to the switch.

Note This section is applicable to the NAM-3 and NAM-NX1. For details on any hardware setup requirements related to this feature, see your specific NAM installation guide. For additional platform options, see Synchronizing Your System Time, page 5-5.

To configure the NAM system time using PTP:

Step 1 On the NAM, choose **Administration > System > System Time**.

Step 2 Choose the **PTP** radio button.

Step 3 Enter the IP address of the PTP interface in the PTP Interface IP Address field.

Tip Set the PTP interface IP address so that it is not in the same subnet as the management interface. If they are in the same subnet, there may be routing issues for outbound management traffic (http, for example).

Step 4 Enter the subnet mask in the PTP Interface Subnet Mask field.

Step 5 For NAM Local Time Zone, select the Region and the Zone from the drop-down lists.

Step 6 To save the changes, click **Submit**.

Understanding NAM System Time

Ensure that the Prime NAM software application's Linux system time is synchronized with the packet timestamp and the standard time source outside of the NAM platform. Packet timing analysis uses system time to support application response time measurements, voice and video quality metrics, packet decode data, reporting, and many other network statistics.

The NAM gets the UTC (GMT) time from several sources, depending on its NAM platform type. All NAMs can be set up to get their time from an external NTP server. Other NAM platforms may prefer to use an IEEE 1588 Precision Time Protocol (PTP)-based time master due to its high accuracy and precision.

You should also configure any PTP switches that are between the NAM and the master clock to use Edge-to Edge (E2E) mode. E2E is preferred because it reduces PTP messaging bandwidth and eliminates delay accumulation when daisy chaining many nodes. If the master clock and/or PTP switches are not configured correctly, all of the clocks on the NAM will be synced with each other, but to the wrong time.

Caution Both the client computer and the NAM server must have the time set accurately for their respective time zones. If either the client or the server time is incorrect, then the data shown in the GUI is incorrect.

The clock identity is the first three octets of the MAC address, followed by "ff fe," and then the last three octets of the MAC address, as shown in the example below.

```
0xec:44:76:ff:fe:5d:12:0
```

After the NAM acquires the time, you can set the local time zone using the NAM System Time configuration window.

For details on how to configure the NAM system time for your specific hardware platform, see Synchronizing Your System Time, page 5-5.

Setting Up E-Mail Notifications for Alarms

You can configure Prime NAM to provide e-mail notification of alarms and to e-mail reports.

To set up e-mail notifications:

Step 1 Choose **Administration > System > E-Mail Setting**.

Step 2 Check the **Enable Mail** check box and enter the required or optional field information.

Table C-58 describes the Mail Configuration Options.

Step 3 Check the optional **Advanced Settings** check box and enter the details in the fields provided.

Step 4 Click **Submit** to save your modifications, or click **Reset** to clear the dialog of any characters you entered or restore the previous settings.

Sharing NAM Data by Enabling Web Data Publication

Web Data Publication allows general web users and websites to access (or link to) selected NAM monitor and report windows without a login session.

Web Data Publication can be open or restricted using Access Control List (ACL) and/or publication code. The publication code, if required, must be present in the URL address or cookie to enable access to published data.

To enable Web Data Publishing:

Step 1 Choose **Administration > System > Web Data Publication**.

Step 2 Check the **Enable Web Data Publication** check box.

Step 3 Enter a Publication Code (Optional). This is the pass code required in a URL's cookie to access the published page. For example, a publication code set to *abc123* would be able to access the following published window:

http://<nam-hostname>/application-analysis/index?publicationcode=abc123

Step 4 Enter an ACL Permit IP Address/Subnets to permit only those IP addresses or subnets access to web publications. No entry provides open access to all.

Step 5 Click **Submit** to enable web publishing, or click **Reset** to clear the dialog of any characters you entered.

Note Before the new iSCSI storage entry takes effect, you must reboot the NAM system.

Setting Remote Servers to Receive Syslog Messages

NAM syslogs are created for alarm threshold events, voice threshold events, or system alerts. You can specify whether syslog messages should be logged locally on the NAM, on a remote host, or both. You can use the NAM to view the local NAM syslogs.

If logging on a remote host, in most Unix-based systems, the syslog collector that handles the incoming syslog messages uses the facility field to determine what file to write the message to, and it will use a facility called *local7*. Check the syslog collector configuration to ensure that *local7* is handled properly.

To set up the NAM syslog:

Step 1 Choose **Administration > System > Syslog Setting**.

The NAM Syslog Setting window displays.

Step 2 In the Remote Server Names field, enter the IP address or DNS name of up to five remote systems where syslog messages are logged. Each address you enter receives syslog messages from all three alarms (Alarm Thresholds, Voice Signaling Thresholds, and System).

Step 3 Click **Submit** to save your changes, or click **Reset** to cancel.

Configuring Hosts to Receive SNMP Traps from Prime NAM

Traps are used to store alarms triggered by threshold crossing events. When an alarm is triggered, you can trap the event and send it to a separate host. Trap-directed notifications can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests.

To configure, edit, or delete a host destination to which Prime NAM will send traps:

Step 1 Choose **Administration > System > SNMP Trap Setting**.

The SNMP Trap Setting window displays.

Step 2 Click **Create**.

Step 3 In the Community field, enter the community string set in the NAM Thresholds.

Step 4 In the IP Address field, enter the IP address to which the trap is sent if the alarm and trap community strings match.

Step 5 In the UDP Port field, enter the UDP port number.

Step 6 Click **Submit** to save your changes, or click **Reset** to cancel and leave the configuration unchanged.

Customizing System Preferences

To change the Prime NAM display or logging characteristics, choose **Administration > System > Preferences**. See Table C-58 describes the fields of the Preferences window and why you may want to change the defaults.

Upgrading Your License

Certain software-only NAM platforms require software licenses to run. You can see your NAM platform installation guide for details.

To obtain a NAM license, go to the following URL:

http://www.cisco.com/go/license

Follow the instructions on this page to obtain a NAM license file. You will need your NAM platform's PID and SN to obtain the license file.

Tip Use the Prime NAM **show inventory** command to obtain the PID and SN for licensing.

After you enter the PID and SN or the Product Authorization Key, a license file will be sent to you by e-mail. Store this license file on an available FTP server. Use the license install command to install the license after the NAM software installation completes.

Several Cisco Prime Network Analysis Module platforms require you to install a product license in the form of a text file (see your release notes as platform support changes with each release). An evaluation license allows you to use the software for up to 60 days. The NAM login window indicates how many days remain before the evaluation license expires. After that time, you will be unable to log into the NAM GUI.

You can provide licensing information, also known as node-locking information, during software installation or after software installation using the NAM CLI.

For details on licensing install and management CLI commands, see the *Cisco Prime Network Analysis Module Command Reference Guide*.

There is no license required for the protocol pack usage in Prime NAM.

Troubleshooting Using Diagnostics Tools

The Diagnostics option of the **Administration** menu provides tools to aid in troubleshooting. You can use these tools when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC). There are options for:

- System Alerts
- Audit Trail
- Tech Support

For additional information on troubleshooting NAM, see Troubleshooting Network and NAM Issues.

System Alerts

You can view any failures or problems that the NAM has detected during normal operations. To view System Alerts, choose **Administration > Diagnostics > System Alerts**.

Each alert includes a date, the time the alert occurred, and a message describing the alert. The NAM displays up to one thousand (1,000) of the most-recent alerts. If more than 1,000 alerts have occurred, you need to use the NAM CLI command **show tech-support** to see all of the alerts.

If you notice an alert condition and troubleshoot and attempt to solve the condition causing the alert, you might want to click **Clear** to remove the list of alerts to see if additional alerts occur.

Audit Trail

The Audit Trail option displays a listing of recent critical activities that have been recorded in an internal **syslog** log file. Syslog messages can also be sent to an external log using **Administration > System > Syslog Setting**.

The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NetFlow data source changes
- Enabling and disabling data collections
- Starting and stopping captures
- Adding and deleting users

Each log entry will contain the following:

- User ID
- Time stamp
- IP address (in case of remote web access)
- Activity description

To access the audit trail window:

Step 1 Choose **Administration > Diagnostics > Audit Trail**.

The Audit Trail Window displays.

The Audit Trail window provides a way to view the user access log and filter entries based on time, user, (IP address) from or activity. The internal log files are rotated after reaching certain size limits.

Tech Support

The NAM syslog records NAM system alerts that contain event descriptions and date and timestamps, indicating unexpected or potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs. For a list of user activities logged in the audit trail window, see Audit Trail.

This information is unlikely to be meaningful to the average user. It is intended to be used by your technical support team for debugging purposes. You are not expected to understand this information; instead, you should save the information and attach it to an e-mail message to your support team or, if applicable, Cisco TAC.

Before You Begin

Before you can view the Tech Support page, you must enable the System Config user privilege on the **Administration > Users > Local Database** page. For more information on editing user privileges, see Establishing TACACS+ Authentication and Authorization.

Note You can also view this information from the NAM CLI. For information on using the NAM CLI, see *Cisco Network Analysis Module Command Reference*.

To view the tech support information:

Step 1 Choose **Administration > Diagnostics > Tech Support**.

After a few minutes, extensive diagnostic information generates and displays in the window.

Step 2 To save the information, click **Download log files**. Save the files to your local disk. You can analyze the files locally or, if requested forward on to your technical support team for review.

Downloading Core Files

To download core files from the Tech Support page, click **Download log files** and follow the instructions.

Controlling User Access

In order to make your Cisco NAM solution more secure, you can take several steps including:

- Enable Secure Sockets Layer (SSL) on the Cisco NAM for secure, encrypted HTTP sessions. See your installation guide for details.
- Enable Secure Shell (SSH) protocol for secure Telnet to the Cisco NAM.
- Enable TACACS+ for authentication and authorization. Cisco NAMs provide support for multiple TACACS+ servers.

This section covers how to control your user's access using the Administration options:

- Local Database
- Establishing TACACS+ Authentication and Authorization
- Configuring a TACACS+ Server to Support NAM Authentication and Authorization
- Current User Sessions

Local Database

When you first install the NAM, use the NAM command-line interface (CLI) to enable the HTTP server and establish a username and password to access the NAM for the first time.

After setting up the initial user accounts (root, admin, and webuser), you can create additional accounts, enabling or disabling different levels of access independently for each user.

Table C-60 provides information about User Privileges and describes each privilege.

For additional information about creating and editing users, see Creating a New User and Establishing TACACS+ Authentication and Authorization.

If you have forgotten your password, use the helper utility to reset your root or user passwords (see Resetting Passwords).

Resetting Passwords

There are several methods you can use to reset your NAM passwords. Use the options documented in Table 5-2 based on your needs.

Table 5-2 Password Reset Options

NAM User	Method	Description
Root, Admin, and webuser	Boot into helper utility	Restart your NAM and choose **option 5** or enter **reboot -helper** at the NAM CLI.
Root and webuser	**clear system-passwords** NAM CLI command	The easiest way to reset NAM passwords. This command resets both the root and guest user passwords to the factory default state. You must have appropriate privileges to reset passwords.
Root, Admin, and webuser	CLI commands on the switch or router	See your platform installation guide.

Table 5-2 Password Reset Options

NAM User	Method	Description
NAM Admin users	**Admin > Users > Local Database**	Delete the user for whom you have forgotten the password; then create a new one.
Webuser	**rmwebusers** NAM CLI command	Use if no other local users are configured other than the user for whom you have forgotten the password. Then enable http or https to prompt for the creation of a NAM user.

Changing Predefined NAM User Accounts on the Switch or Router

The predefined root and guest NAM user accounts (accessible through either a switch or router **session** command or a Telnet login to the NAM CLI) are static and independent of the NAM. You cannot change these static accounts nor can you add other CLI-based users with the NAM.

Creating a New User

To create a new user:

Step 1 Choose **Administration > Users > Local Database**.

The GUI displays the users in the local database. Checks indicate the privileges each user has for the functions listed.

Step 2 Click **Create**.

The GUI displays the New User Dialog Box.

Step 3 Enter the information required to create new user and select each privilege to grant to the user. See Table C-61 for an explanation of user privileges. Table C-59 describes the fields in the New User Dialog Box.

Note If you delete user accounts while users are logged in, they remain logged in and retain their privileges. The session remains in effect until they log out. Deleting an account or changing permissions in mid-session affects only future sessions. To force off a user who is logged in, restart the NAM.

Step 4 Select a single or multiple check box to set user privileges. Table C-61 provides information about each privilege.

Step 5 Click **Submit** to create the user or **Reset** to clear the dialog of any characters you entered.

Invalid User Name and Password Characters

For usernames, do not use the following:

- Exclamation point !
- At sign @
- Pound sign #

- Dollar sign $
- Percent %
- Carot ^
- Ampersand &
- Asterisk *
- Left or right parentheses ( )
- Greater than <
- Less than >
- Comma ,
- Period .
- Double quote "
- Single quote '
- Forward slash /
- Backward slash \

For web user passwords, do not use the following:

- Double quote "
- Single quote '
- Greater than <
- Less than <

For **root** or **guest** user passwords, only the single quote is not allowed.

Establishing TACACS+ Authentication and Authorization

Terminal Access Controller Access Control System (TACACS) is an authentication protocol that provides remote access authentication, authorization, and related services such as event logging. With TACACS, user passwords and privileges are administered in a central database instead of an individual switch or router to provide scalability.

TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization.

When a user logs into the NAM, TACACS+ determines if the username and password are valid and what the access privileges are.

To establish TACACS+ authentication and authorization:

Step 1 Choose **Administration > Users > TACACS+**. The TACACS+ Authentication and Authorization Dialog Box displays.

Step 2 Enter or select the appropriate information in Table C-62, TACACS+ Authentication and Authorization Dialog Box.

Step 3 Do one of the following:

- To save the changes, click **Submit**.
- To cancel, click **Reset**.

Tip If you cannot log into the NAM with TACACS+ configured, verify that you entered the correct TACACS+ server name and secret key.

Configuring a TACACS+ Server to Support NAM Authentication and Authorization

In addition to enabling the TACACS+ option, you must configure your TACACS+ server so that it can authenticate and authorize NAM users. NAM supports ACS versions 5.2, 5.1 (including Patch 1), and 4.2.

Note Configuration methods vary depending on the type of TACACS+ server you use. When configuring NAM within ACS 5.x, uncheck the check box for the Single Connect Device option under the TACACS+ settings.

Continue to the section specific to your particular version:

- Configuring a Cisco ACS Server, Version 4.2
- Configuring a Cisco ACS Server, Version 5.x
- Configuring a Generic TACACS+ Server

Configuring a Cisco ACS Server, Version 4.2

To configure a version 4.2 Cisco ACS server, you must perform two tasks:

- Configure the NAM hostname and IP address on the ACS server. See Configuring NAM on ACS for Windows NT and 2000 Systems for Version 4.2.
- Add a NAM user or user group. See Adding a NAM User or User Group for Version 4.2.

Configuring NAM on ACS for Windows NT and 2000 Systems for Version 4.2

To configure a Cisco ACS TACACS+ server (version 4.2):

Step 1 Log into the ACS server.

Step 2 Click **Network Configuration**.

Step 3 Click **Add Entry**.

Step 4 For the Network Access Server, enter the NAM hostname and IP address.

Step 5 Enter the secret key.

Note The secret key must be the same as the one configured on the NAM.

Step 6 In the Authenticate Using field, select **TACACS+**.

Step 7 Click **Submit+Apply**.

Step 8 Continue to Adding a NAM User or User Group for Version 4.2 to complete the next configuration task.

Adding a NAM User or User Group for Version 4.2

To add a NAM user or user group:

Step 1 Click **User Setup**.

Step 2 Enter the user login name.

Step 3 Click **Add/Edit**.

Step 4 Enter the user data.

Step 5 Enter a user password.

Step 6 If necessary, assign a user group.

Step 7 In the TACACS+ settings:

a. Select **Shell**.

b. Select **IOS Command**.

c. Select **Permit**.

d. Select **Command**.

e. Enter **web**.

f. In the Arguments field, enter:

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

Step 8 In Unlisted Arguments, select **Deny**.

Step 9 Click **Submit**.

Configuring a Cisco ACS Server, Version 5.x

To configure a version 5.1 (Patch 1) or 5.2 Cisco ACS server, you must perform these tasks. There is an additional configuration task that enables you to set up policy rules for your users or groups.

Use the following sections to configure your Cisco ACS server:

- Configure the NAM hostname and IP address on the ACS server. See Configuring NAM on ACS For Windows NT and 2000 Systems for Version 5.x.
- Add a NAM user or user group. See Adding a NAM User or User Group for Version 5.x.
- Set up your policy rules. See Configuring Access Policies for ACS and NAM for Version 5.x.

Configuring NAM on ACS For Windows NT and 2000 Systems for Version 5.x

To configure a Cisco ACS TACACS+ server (version 5.1(P1) or 5.2):

Step 1 Log into the ACS server.

Step 2 To set up an optional device type for NAM, click **Network Resources > Network Device Groups > Device Type** and create a device type. For example, you may choose to name your device type *NAM_Module*.

Step 3 Click **Network Resources > Network Devices and AAA Clients** to add NAM devices.

Step 4 For the Network Access Server, enter the NAM hostname and IP address.

Step 5 Under Authentication Options field, select **TACACS+**.

Step 6 Enter the secret key and deselect the check box for the Single Connect Device option under the TACACS+ settings.

Note The secret key must be the same as the one configured on the NAM.

Step 7 Click **Submit**.

Step 8 Continue to Adding a NAM User or User Group for Version 5.x to complete the next configuration task.

Adding a NAM User or User Group for Version 5.x

To add a NAM user or user group:

Step 1 Click **Users and Identity Stores > Internal Identity Stores > Users.**

Step 2 Click **Create**.

Step 3 Enter the user login name.

Step 4 Enter the user data.

Step 5 If necessary, assign a user group.

Step 6 Enter the password information.

Step 7 Click **Submit**.

Configuring Access Policies for ACS and NAM for Version 5.x

In versions 5.1(P1), 5.2, and 5.3 you must set up access policies to complete your ACS and NAM configuration.

Step 1 On the ACS server, click **Policy Elements > Authorization and Permissions > Device Administration > Command Sets** and click **Create** to create NAM command sets.

For example, if you want to provide full access to the NAM, create a command set called *NAMfullAccess* and check the check box **Permit any command that is not in the table below**.

Step 2 Click **Submit** when you have completed entering the NAM command sets. Ensure you include all of the following commands:

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

Step 3 Click **Access Policies > Access Services > Create** to create a new Service (for example, name = *namAdmin*; Service Type = Device Administration.)

Step 4 Go to **Access Policies > Access Services >** *namAdmin* **> Authorization > Customize** to set up customized conditions which are needed in later step. For example, you may choose: NDG: Device Type, Device IP Address, and so on). Replace *namAdmin* with the service you created in this step.

Step 5 Go to **Access Policies > Access Services >** *namAdmin* **> Authorization > Create** to set up the condition to qualify all login requests. NAM devices use these conditions and follow the command set (created in Step 1). For example, your condition may be == NDG: Device Type is All Device Types: NAM device which you set up in Step 2.

Step 6 Click **Access Policies > Service Selection Rules** to choose a service (for example, the service you created in Step 3).

Step 7 Log into the NAM and click **NAM > Administration > Users > TACACS+** to set up the ACS server IP and secret key.

Configuring a Generic TACACS+ Server

To configure a generic TACACS+ server:

Step 1 Specify the NAM IP address as a Remote Access Server.

Step 2 Configure a secret key for the TACACS+ server to communicate with the NAM.

Note The secret key must be the same as the one configured on the NAM.

Step 3 For each user or group to be allowed access to the NAM, configure the following TACACS+ parameters:

Parameter	Enter
service	`shell`
cmd	`web`

cmd-arg	One or more the following:
	`accountmgmt`
	`system`
	`capture`
	`alarm`
	`collection`
	`view`

password authentication method—Password Authentication Protocol (PAP)	`pap`

Current User Sessions

The Current User Sessions table is a record of the users who are logged into the application. The user session times out after 30 minutes of inactivity. After a user session times out, that row is removed from the table.

To view the current user sessions table:

Step 1 Choose **Administration > Users > Current Users**.

The Current User Sessions table (Table C-63) displays.

Managing System Data

One of the roles of an administrator is to manage Prime NAM's network data collection and retention so that it:

- Scales to fit the real needs of the system's users.
- Minimizes the burden on monitored devices, applications, and network bandwidth.
- Survives hardware failures.

The following sections explain how to achieve these goals, and how to perform other data management tasks.

- Handling Backups
- Shrinking Storage Requirements

Handling Backups

It is critical to have your system backed up so that you can restore your configuration and data if required. Ensure you have sufficient data backups scheduled. Use the **config upload** command to back up your current configuration. For detailed instructions see your installation guide on Cisco.com.

Shrinking Storage Requirements

Network administrators are consistently looking for ways to shrink their network storage requirements and improve bandwidth efficiency on tasks like backup and recovery.

By configuring Prime NAM packet deduplication on supported platforms, packets whose inspected segments match another packet within the specific time window are marked as duplicates and not forwarded.

For configuration guidelines and instructions, see Configuring Hardware Deduplication.

You can also move capture files to an external storage location to save on local disk space. See About Capturing to Data Storage.

NAM Deployment

This chapter describes some usage cases on how to deploy NAM in your networks. It contains details on network performance management as well as usage scenarios for the Cisco Prime Network Analysis Module Software.

To view which release versions run on the supported NAM platforms, see the *NAM Compatibility Matrix*.

The use cases focus on a specific need to be addressed or a problem to be solved. Each scenario takes into account the deployment considerations discussed in Overview and then uses one or more of NAM's features to meet the need or solve the problem. The goal of these use cases is to provide real-world examples. These examples discuss best practices and approaches to effective NAM deployment and are grouped into several categories.

This chapter contains the following sections:

Note Some of the graphics represented in this section may be different than what you see on the screen. These illustrations are for examples only.

Deploying in the Data Center

Deploying in a Campus Environment

- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-17
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications, page 6-17
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-10
- Using NAMs to Monitor VoIP Quality, page 6-3

Deploying in the Branch

- , page 6-6
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-17
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications, page 6-17
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-10
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-6
- Using NAMs to Monitor VoIP Quality, page 6-3

General Usage Scenarios

These use cases are applicable to any part of the network:

- Using NAM for Historical Trends via Interactive Report, page 6-14
- Using NAM for Problem Isolation, page 6-19
- Creating Custom Applications, page 6-5
- Autodiscovery Capabilities of NAM, page 6-4
- Using NAM for SmartGrid Visibility, page 6-19

NAM Integrations with Monitoring and Reporting Applications

- Integrating NAM with Prime Infrastructure, page 6-5
- Integrating NAM with Third Party Reporting Tools, page 6-6

Deployment Examples

- Using NAMs to Monitor VoIP Quality, page 6-3
- Autodiscovery Capabilities of NAM, page 6-4
- Creating Custom Applications, page 6-5
- Integrating NAM with Third Party Reporting Tools, page 6-6

Using NAMs to Monitor VoIP Quality

Voice quality analysis has been significantly enhanced in Cisco NAM. The software is now capable of accurately measuring voice quality by using the industry-standard MOS algorithm. Call quality measurements are computed every 1 minute and made available through the GUI. Note that the voice-related screens on the NAM GUI are significantly different from previous releases. Changes have been made to provide useful information quickly and automatically, while allowing easy navigation to details.

Deployment: NAM deployments for voice quality analysis require that NAM be able to monitor VoIP packets from the calling phone to the called phone. The branch edge location in the network provides visibility into all calls entering and leaving the branch; similarly a campus edge location monitors calls crossing the campus boundary. Often, the distribution layer is a good location to deploy NAMs for this purpose, especially if specific phones or particular portions of the network are to be monitored. For example, a new Multi protocol Label Switching (MPLS) link is being piloted and three buildings that are part of Company X's headquarters are part of the pilot. In order to monitor voice quality for those three buildings, a NAM could be deployed at the distribution Catalyst 6500 that serves those users.

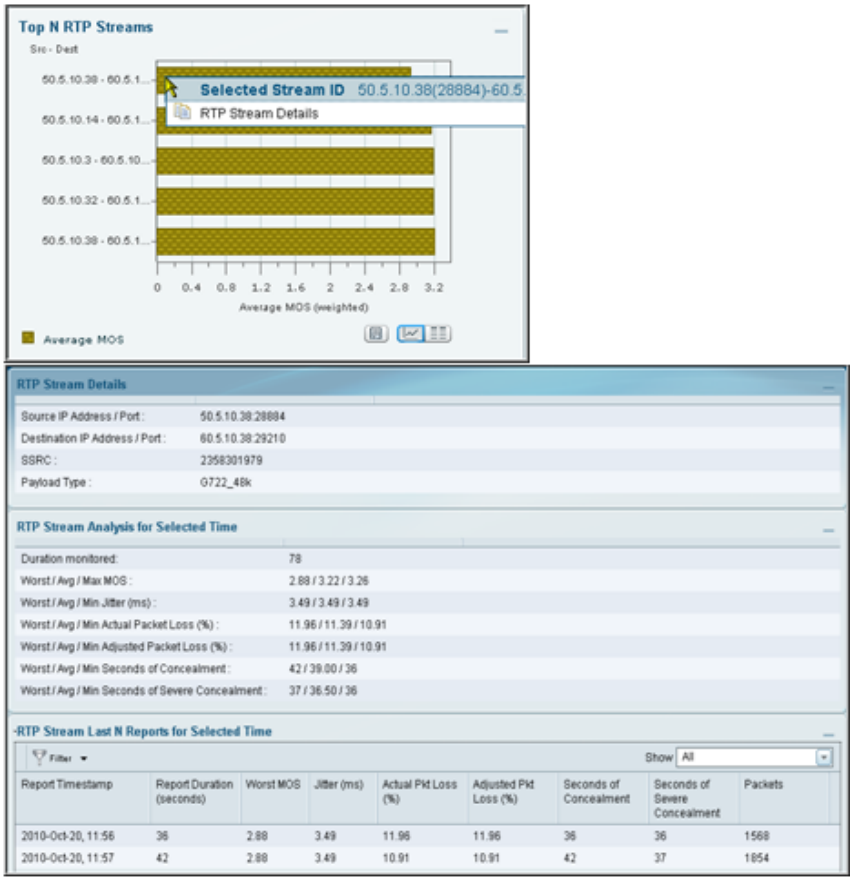
Note The data center is typically not an appropriate location for RTP stream analysis because calls will seldom go through the data center. However, the data center is a good location to monitor signaling messages between phones and Cisco Unified Communications Manager. NAM decodes signaling messages to track call history, caller names, phone numbers, and other relevant call details.

Use the following steps to monitor the network to make sure 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**. 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). The figure below displays the Top N RTP Source and Destination endpoints. Notice that there are calls that are in the poor range.

Step 2 To isolate calls that had a poor MOS, scroll down to Top N RTP Streams and click on the chart to drill down into the RTP Stream Details. As shown in Figure 6-1, notice that the MOS value for the calls listed on top is 2.88, which is low. Further, looking at the other metrics provided in the same row (for example, row one), notice that jitter is 3.49 and the packet loss rate is 11 percent, resulting in the low MOS value. This information tells you that jitter is the root cause of the poor calls; instead, it is packet loss somewhere in the network.

Figure 6-1 Top N RTP Streams by MOS



Step 3 With the endpoints' IP addresses, you can look at the network topology to identify where in the network the 50.5.10.38 subnet is located. For the purposes of this use case, this subnet is in Building 3 of the main campus. You know that the Building 3 distribution switch has a NAM located in it.

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 Building 3 and connects to the core. That interface is likely the source of the packet loss. Check the interface for faults and fix as needed.

See Analyzing Traffic, RTP Streams, page 3-30 and Setting Voice Signaling Thresholds, page 7-35.

Autodiscovery Capabilities of NAM

If you are an existing NAM 4.x or NAM 6 user, you will not need to configure the SPAN sessions, and they will be automatically created on the NAM (not on the device). If you are a new NAM 5.x user, you will need to configure SPAN or NetFlow.

SPAN or NetFlow must be already configured on the device to forward traffic to NAM for auto creating the data source. See Setting Up Prime NAM Data Sources, page 7-5.

Creating Custom Applications

NAM identifies applications/protocols based on the TCP/UDP port number, so if there are applications using custom ports, the NAM can be configured to identify those applications by name instead of the port.

See Creating Deeper Visibility Into Application Traffic, page 7-48.

Integrating NAM with Prime Infrastructure

Cisco Prime supports integrated lifecycle management of networks, services, and endpoints for Cisco borderless network, data center, and collaboration architectures with end-to-end assurance. You can use Cisco Prime Infrastructure to centrally manage the Cisco Prime NAM platforms such as the NAM appliance to track inventory, view configurations, and perform image and fault management. Prime Infrastructure also rolls up the performance intelligence from NAMs deployed across the network into a consolidated dashboard.

The following overview describes the steps to complete in Prime Infrastructure to set up NAM to view multiple NAMs on your dashboard. For details steps, see the *Prime Infrastructure User Guide* on Cisco.com.

Step 1 Ensure you configure NTP and DNS for all the NAMs in your network. You can now configure those without going to the CLI or logging in to the individual NAM web GUI. Use the Cisco Prime Infrastructure Device Work Center to perform this task. For detailed steps, see your Prime Infrastructure product documentation.

Step 2 Add the NAM HTTPS credentials from the Prime Infrastructure's Device Work Center Edit Device window so that Prime Infrastructure can retrieve data from them. You must add them only after the discovery process is complete or the modules have been added to the Prime Infrastructure inventory.

If you have licensed Assurance features, most Assurance features depend on NAM data to work so this is a required step.

You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

Step 3 To ensure that you can collect data from your NAMs using Prime Assurance, you must enable NAM data collection and configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to Prime Infrastructure. You can do this for each discovered or added NAM, or for all NAMs at the same time.

Step 4 To manage and troubleshoot a network problem such as a suspected network attack, you can use multiple NAMs to create packet captures, save them as files, and then decode them to inspect the suspicious traffic.

For other troubleshooting tips on how to use NAM with Prime Infrastructure, see the *Prime Infrastructure User Guide.* For application developers who want to use the NAM REST API to connect with Prime NAM, ask your Cisco representative about using the Cisco Prime Network Analysis Module REST API.

Integrating NAM with Third Party Reporting Tools

Prime NAM integrates with the CA NetQoS SuperAgent for the purpose of aggregating Application Response Times. Prime NAM also integrates with CompuWare Vantage and InfoVista 5View for Host, Conversation, RTP, and Response Time.

Ask your Cisco representative about the *Prime NAM API Programmer's Guide* to find out more about the NAM Northbound Interface, also referred to as the REST API (Application Programming Interface). The API enables you to provision Prime NAM and extract performance data.

You can write your own scripts based on the Prime NAM Northbound API, but you must perform some setup in the GUI.

For details on what data can be collected, see Using Response Time Summary.

Point to the Design Guide

Monitoring Cisco WAAS and Measuring Its Impact

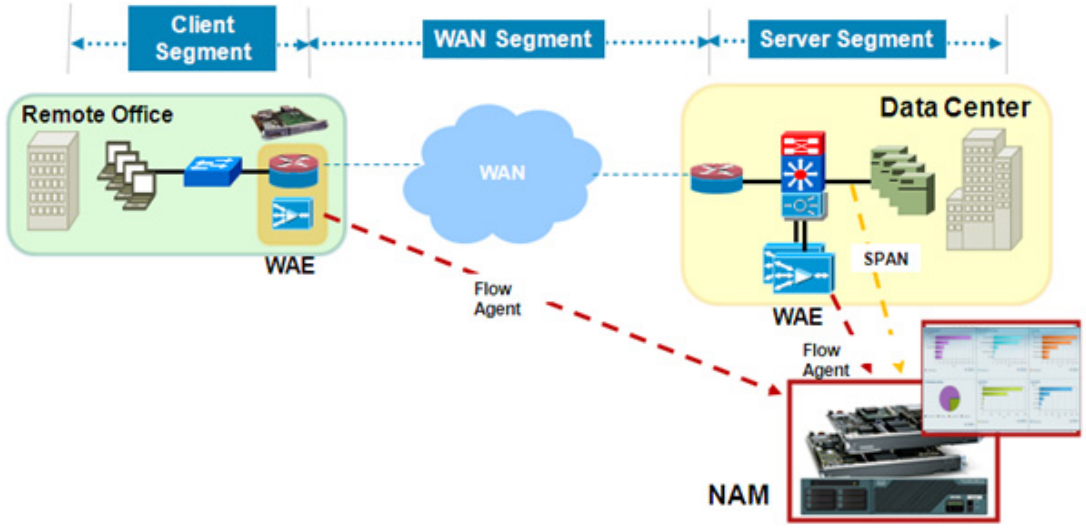
Cisco Wide Area Application Services (WAAS) is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to the branch office, and provides local hosting of branch-office IT services. Cisco WAAS allows IT departments to centralize applications and storage in the data center while maintaining LAN-like application performance and provides locally hosted IT services while reducing the branch-office device footprint.

One of the challenges facing IT personnel who deploy WAAS is to measure and report on the benefits provided by their WAN optimization deployment. Accurate measurement provides many benefits: IT can show return on investment; IT can assess whether the improvement gained meets originally advertised expectations from the solution; and finally, IT can use WAAS ongoing for monitoring, troubleshooting, and planning information for expanding the deployment.

The NAM can monitor WAAS-optimized flows by using WAE devices as the data source. Using this capability, the NAM is able to provide visibility into optimization-related metrics for the three distinct segments that are created by WAAS: the branch, the WAN, and the data center segments.

Placing a Cisco NAM appliance at the edge of the data center is recommended for WAAS deployments. From this location in the network, the NAM can measure local metrics using SPAN technology, and for information on the remote branch segment, it relies on flow agent exports from the remote WAE device. If SM-SREs are available, deploying one at the remote branch site is very useful. This SM-SRE can provide user experience at the site before WAAS is enabled and then contrast it to user experience after WAAS is enabled. See Figure 6-2.

Figure 6-2 Cisco NAM's Ability to Analyze from Multiple Data Sources



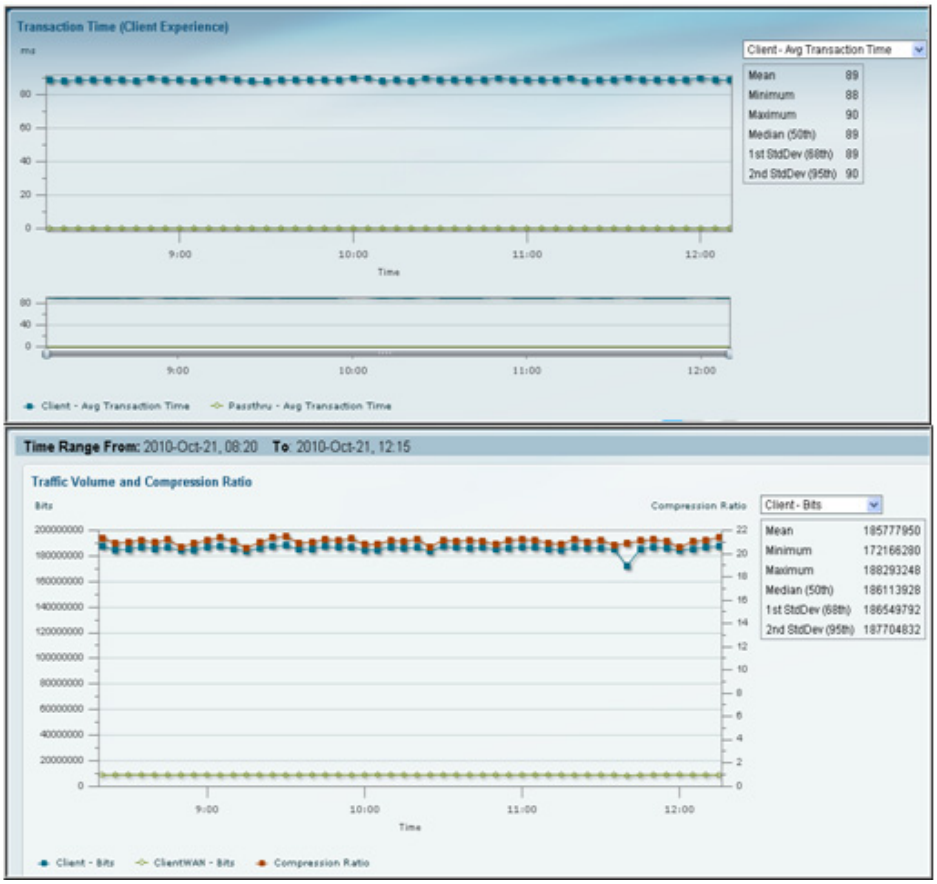
To deploy this solution:

Step 1 Using a NAM 2x20 deployed at the data center, measure application response time before WAAS is enabled using **Analyze > WAN Optimization > Top Talker Detail**. The Top Talker display includes such data as utilization, concurrent connections, and average transaction time for top applications, network links, clients, and servers that are possible candidates for optimization.

Step 2 Create a WAAS Client Side and WAAS Server Side for the WAAS flows from the DC and Branch WAEs.

Step 3 The NAM provides an interactive dashboard to view the analyzed data. Figure 6-3 displays Client Transaction Time, Traffic Volume and Compression Ratio, Number of Concurrent Connections (Optimized vs. Passthru), and Multi-Segment Network Time (Client LAN - WAN - Server LAN). As you can see in the first graph, all non-optimized traffic is displayed as Passthru.

Figure 6-3 Application Performance Analysis -- Optimized



The screen shot above illustrates the significant improvement experienced by users in the branch when WAAS is turned on. Such reports are very useful to justify an investment in WAN optimization technologies and to show returns on those investments in terms of increase in employee productivity and improved user experience from remote sites.

Figure 6-4

Step 4 From the perspective of the NAM located in the data center, there are two sources of information for response time measurements. SPAN provides measurement at the data center and exports from the branch; WAAS flow or PA via Prime Infrastructure provides measurements from the branch. Using these two sources of information, the NAM at the data center can continuously monitor current response times for each branch and help IT personnel keep user experience within known bounds. When abnormal response times are detected, the NAM can be configured to send alerts to appropriate personnel with information relevant to troubleshooting the problem.

Note The NAM 2x20 in the above scenario can be substituted with the NAM Virtual Blade on the WAVE-574 and WAE-674 to obtain the same type of reports.

Monitoring

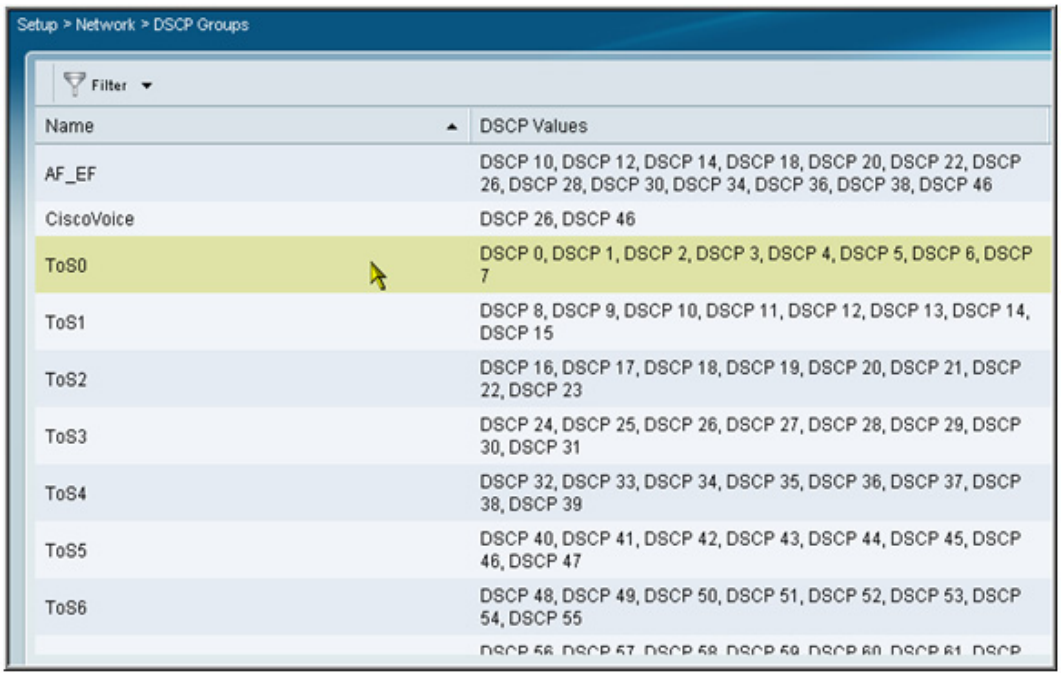
Using NAM to Monitor QoS/DiffServ (DSCP)

Differentiated Services (DiffServ) provides insight into how traffic is being classified by QoS and detects incorrectly marked or unauthorized traffic. The NAM identifies the application/protocol based on the type of service (ToS) bits setting. The administrator can configure DSCP Groups or use the ones provided (as shown in Figure 6-5). The voice template can be used to monitor whether voice traffic is marked properly. Figure 6-7 displays the DiffServ application statistics for all DSCP value. Looking at this, you will notice that RTP and Session Initiation Protocol (SIP) are listed, which indicates that they are not being correctly marked throughout its path.

In the following scenario, IT has deployed QoS to prioritize VoIP traffic to improve voice quality across the network. The NAMs are deployed in the data center and branches and utilized to monitor the DSCP to validate QoS policies.

Step 1 Choose **Setup > Media > DSCP Groups** to display the default groups.

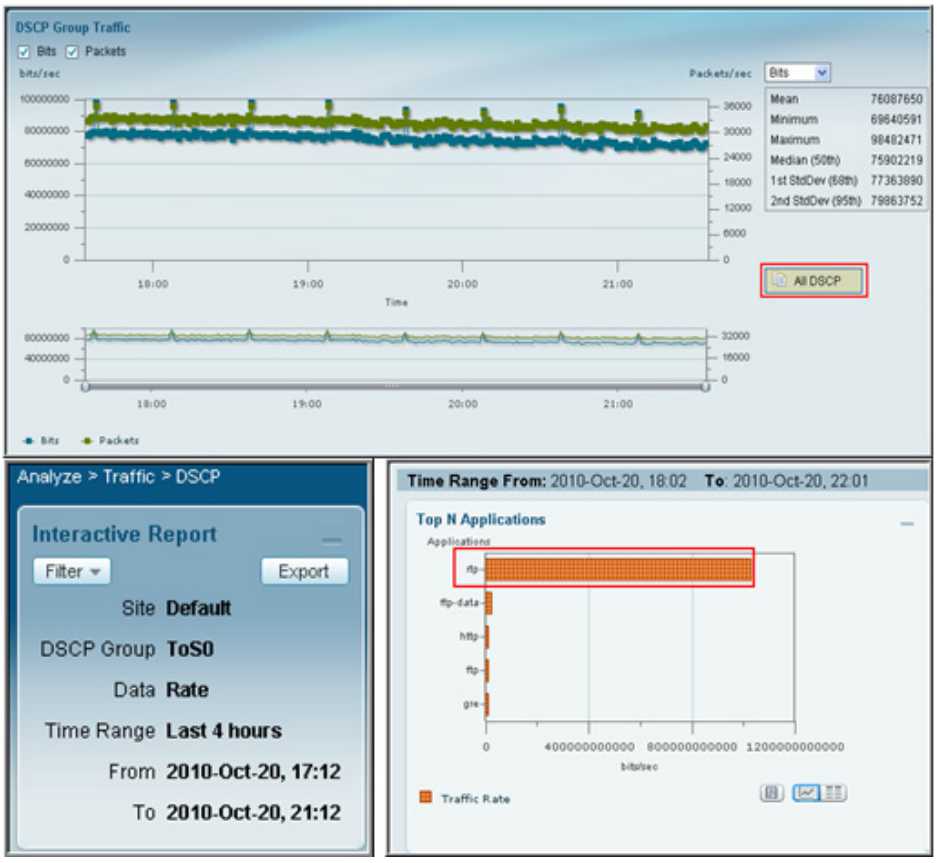
Figure 6-5 Default DSCP Groups



Step 2 Choose **Administration > System > Preferences** to turn the IP TOS Flow Key on. Use caution since this option affects ART and other flow-based traffic. See Table C-59 for details.

Step 3 Choose **Analyze > Traffic > DSCP** to find any misclassified traffic. In Figure 6-6, the RTP protocol is displayed for ToS0 classification.

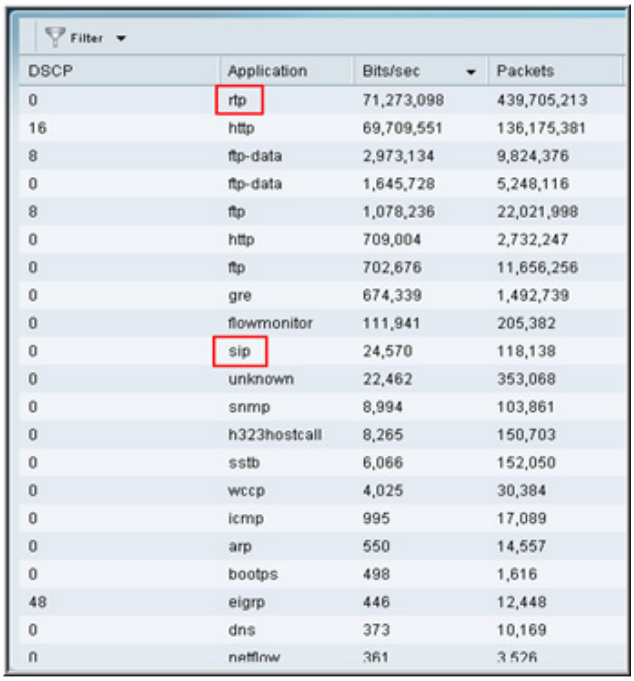
Figure 6-6 DSCP Group - ToS0



Step 4 Click on the **All DSCP** button to view all DSCP and applications.

Step 5 In Figure 6-7, RTP and SIP are highlighted. The protocols are listed for DSCP 0, which is incorrect since the standard classification for voice traffic is DSCP 46 and 24. This means that some of the voice traffic is misclassified on the network. You can also view the branch NAMs to investigate whether voice traffic is being misclassified.

Figure 6-7 All DSCP Table

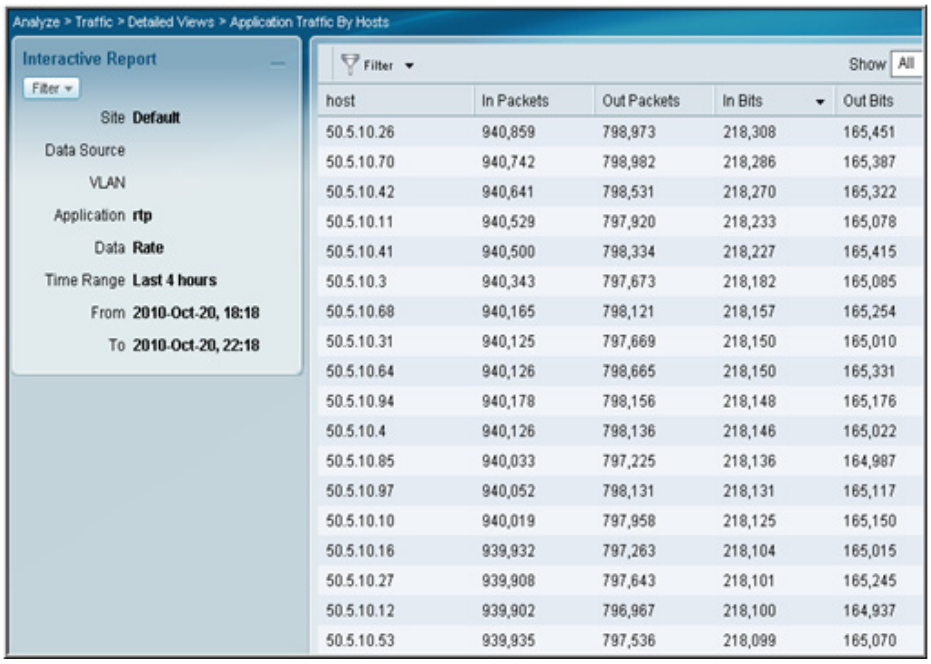


Filter

DSCP	Application	Bits/sec	Packets
0	rtp	71,273,098	439,705,213
16	http	69,709,551	136,175,381
8	ftp-data	2,973,134	9,824,376
0	ftp-data	1,645,728	5,248,116
8	ftp	1,078,236	22,021,998
0	http	709,004	2,732,247
0	ftp	702,676	11,656,256
0	gre	674,339	1,492,739
0	flowmonitor	111,941	205,382
0	sip	24,570	118,138
0	unknown	22,462	353,068
0	snmp	8,994	103,861
0	h323hostcall	8,265	150,703
0	sstb	6,066	152,050
0	wccp	4,025	30,384
0	icmp	995	17,089
0	arp	550	14,557
0	bootps	498	1,616
48	eigrp	446	12,448
0	dns	373	10,169
0	netflow	361	3,526

Step 6 Left-click on the RTP graph and select **Application Traffic by Host** to display the clients using those protocols. This helps to troubleshoot why RTP or SIP traffic from these clients is not marked correctly. As shown in Figure 6-8, the NAM displays the IP addresses of the phones using those protocols. This helps you review the QoS policy implemented on the routers and switches between the clients.

Figure 6-8 RTP Host Table



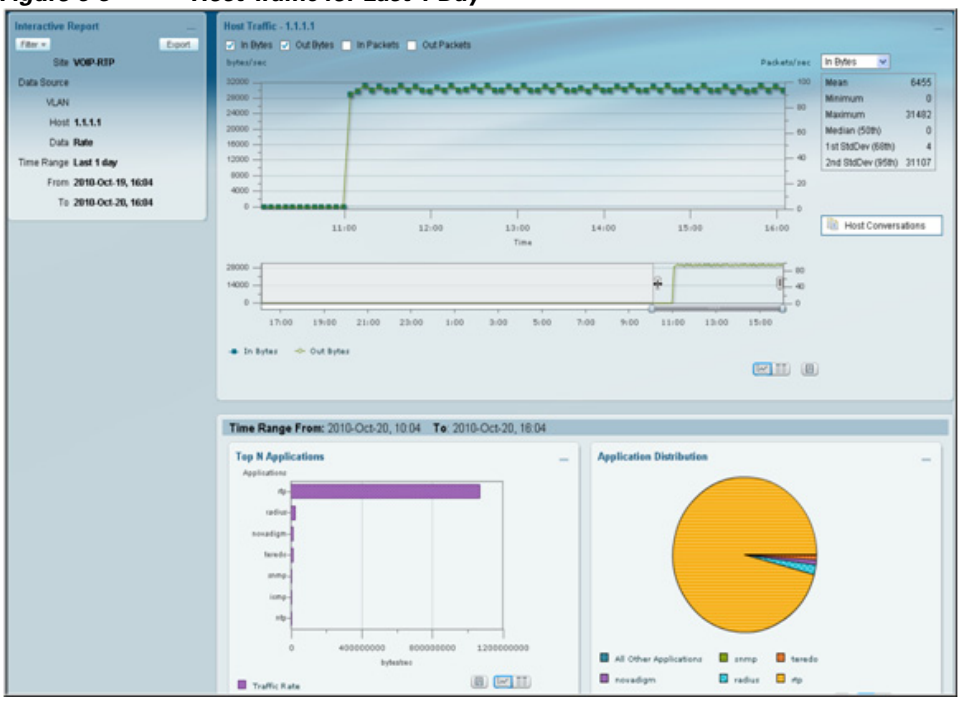
Using NAM for Historical Trends via Interactive Report

Historical trending is an important component of network performance management. While real-time analysis provides information about events, historical trending provides visibility into event sequences. Such sequences offer valuable information about various aspects of the network such as changes in network traffic behavior, anomalies and unusual activities, and network usage in peak times versus low times. It is also helpful in planning future network upgrades, application roll outs, and hardware buildouts. Here are some things to take note of regarding NAM's historical trending capabilities:

- Use the Interactive Report > **Filter** button (located on the left side of the NAM window) to look at short term and long term trends by changing the Time Range. The interactive reports can be exported or the filter setting saved for quick view in the future. The exported data can be sent via e-mail in CSV or PDF format.

- Figure 6-9 displays host traffic for the last day, and using the middle graph you can zoom down to the time range of 10:00 - 16:00 to view what other application this host is using.

Figure 6-9 Host Traffic for Last 1 Day

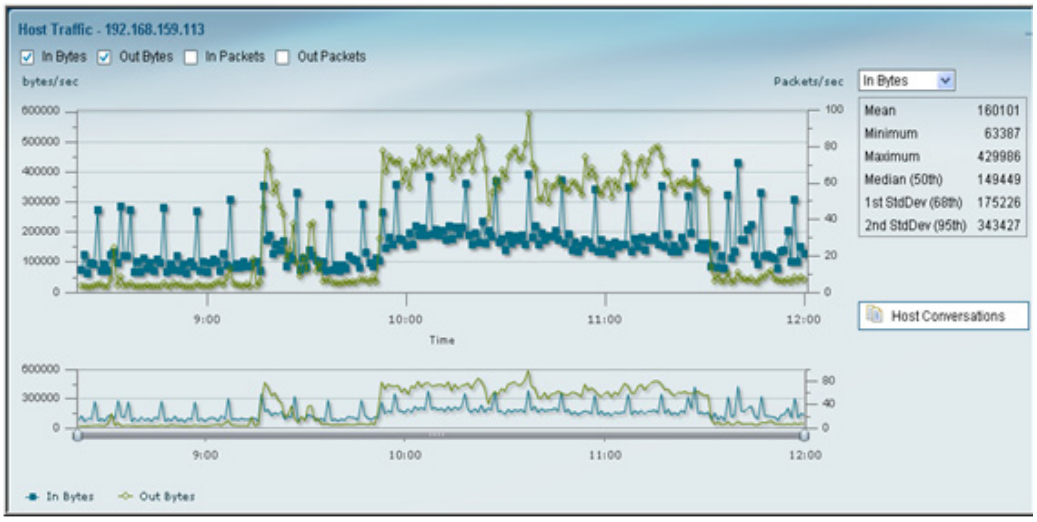


In the following deployment scenario, you will predict the capacity needed for a new branch build out due in six months by studying the usage of an existing branch office of a similar size. To deploy a NAM located in the branch router (ISR) of the existing branch:

Step 1 Start capturing traffic rates between the branch and the data center. View the traffic for the last month from **Interactive Report > Filter > Time Range > Custom** (enter a date covering a month).

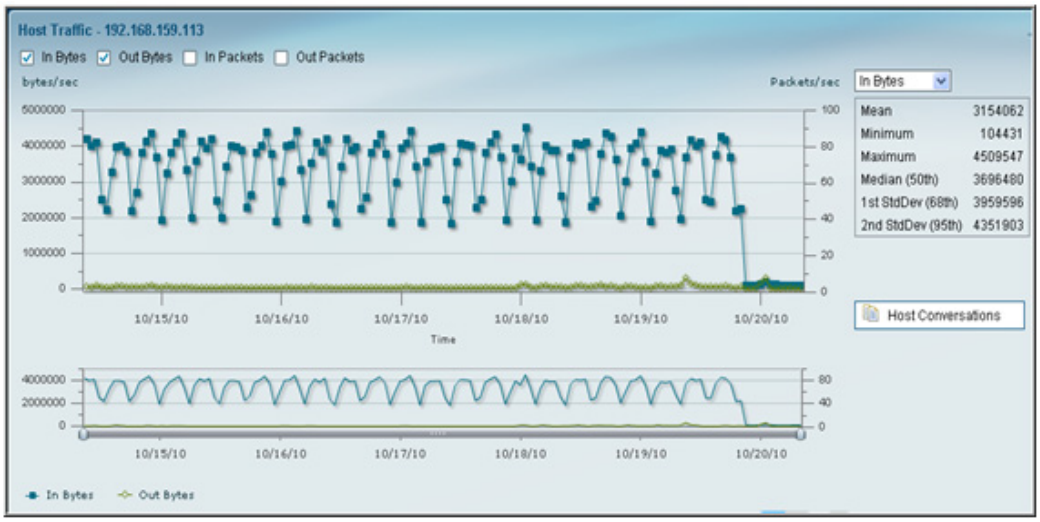
Step 2 Open a conversation report from today and find a stream that has a mildly increasing trend but is unable to confirm the rate at which it is increasing (see Figure 6-10).

Figure 6-10 A Stream with a Mildly Increasing Trend



Step 3 Change the Time Range dynamically in the Interactive Report to study the trend with a granularity of one month. You may find that the pattern does show periodic increases, but it always hits a ceiling between 4.5 Kbps and 5.x Kbps (see Figure 6-11). You are then able to conclude that the ISP link needed at the new site would be similar, and so a standard T1 line would be more than sufficient for the needs of the new remote office.

Figure 6-11 The Trend Shown with a Granularity of 1 Month



Studying historical trends is a valuable exercise in planning and creating baselines in a network. Monitor and trend on business critical applications and servers. These trends should provide handy information in a variety of day-to-day decisions.

Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications

Application Performance Response Time Analysis provides up to 45 metrics. You can configure thresholds based on many of these metrics, and receive an alert when the thresholds are passed. Thresholds should be set for critical applications or servers using Average Server Response Time, or Average Transaction Time, or Average Network Time and Average Server Network Time. These thresholds will help identify where the problem lies in the application performance, and show whether the problem is a server or network issue. Depending on the alarm, you can access the NAM to see the applications and clients accessing the server, or to check the devices in the traffic path monitoring device and interface utilization.

See Application Response Time, page 3-20.

See Defining Thresholds, page 7-31.

Using NAM to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications

The NAM monitors and analyzes RTP streams and voice calls statistics by intercepting the data collected by endpoints. So, when a phone call ends, the endpoints calculate the information and send it to the Unified Communications Manager (aka the Call Manager), the NAM collects the data (as log as it is along that path).

NAM uses the voice call statistics from the endpoint with the RTP stream to correlate the phone number with the IP address of the endpoint. Alerts are sent based on analysis of the RTP streams for MOS, Jitter, and Packet Loss.

To use NAM to monitor the application-level performance for UDP real-time applications:

Step 1 Set up thresholds to focus on which types of performance metrics you want to monitor at **Setup > Alarms > Thresholds**.

Step 2 View voice signaling/RTP traffic at **Analyze > Media > RTP Streams** or **Analyze > Media > Voice Call Statistics**.

See Analyzing Traffic, page 3-9, RTP Streams, page 3-30.

See Table C-29, Voice Monitor Setup Window, page C-18.

Monitoring the Nexus 1000V Switch Environment

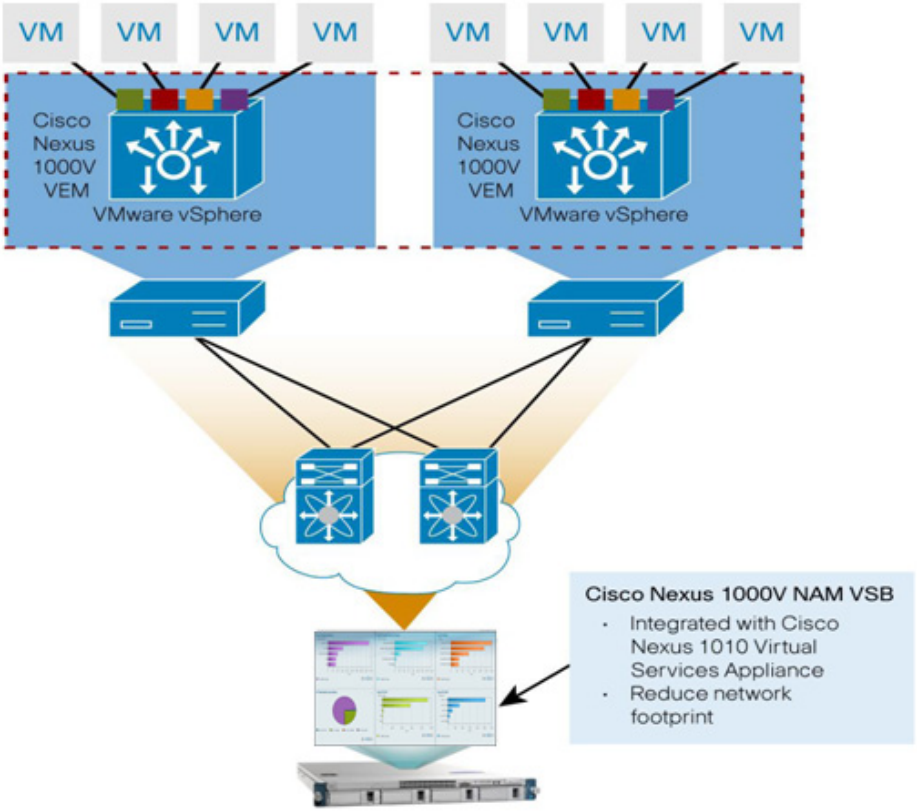
As networks and applications move into the virtualization environment, the challenge for you is to find tools to gain insight into that environment. The NAM VSB provides that function by integrating with the Cisco Nexus 1010 virtualization appliance. Using the NAM VSB, you can gain operational visibility into the virtual switching layer and is able to see virtual machine (VM) to VM statistics. See Figure 6-12.

The Nexus 1000V switch can also be monitored by other NAM platforms running the Prime NAM software.

You are deploying applications in the ritualized environment and the Nexus 1000V switch is providing the network connectivity. The NAM VSB installed on the Nexus 1010 Virtual Services Appliance is used to monitor the environment.

Note If Nexus 1000V switches and NAMs are already deployed in the network, ERSPAN or NetFlow data source can be directed by any one of those NAMs. You should directly connect the 1000V switch and NAM to the same physical switch.

Figure 6-12 Cisco Nexus 1000V NAM Virtual Service Blade Deployment



To monitor the Nexus 1000V environment:

Step 1 Install and configure either the NAM VSB on the Nexus 1110 Virtual Services Appliance. See the Installation and Configuration Guides for the NAM on Cisco.com.

Step 2 For the NAM VSB:

1. Verify that ERSPAN or NetFlow are configured on the Cisco 1000V Switch Virtual Supervisor Module (VSM) that is providing data to NAM.
2. Configure the ERSPAN or NetFlow data source, depending on your NAM:
3. Enable all applicable monitoring parameters in NAM for ERSPAN and NetFlow. Use the Traffic Summary window to display Top N information such as applications, hosts, protocol, and server response time. You can view and display details for each of the categories listed.
4. Using the Interactive Report, configure reports for trending on the application response time, hosts, and conversation traffic patterns.

The physical and virtual interfaces table provides VM-to-VM traffic utilization. Because one virtual interface connects to one VM, the data shows which VMS are utilizing the switch resources. You can then view the hosts and conversations tables to identify the culprit utilizing the resources.

Note NAM VSB provides the same complement of features except that it supports only ERSPAN and NetFlow data sources and performs no voice monitoring and packet capture.

Troubleshooting

Using NAM for Problem Isolation

The alarm details (found in the Cisco Prime Network Analysis Module Software under **Monitor > Overview > Alarm Summary**) provides information you can use to drill down on the threshold that was violated. You may also receive this alarm in e-mail (**Setup > Alarms > E-mail**). An example of the alarm is:

```
2013 SEPT 28 9:17:0:Application:Exceeded rising value(1000);packets;60653;Site(San Jose),
Application)
```

After receiving this alarm, you can access the NAM GUI to view the application in your specific site to determine why there was a spike. Click on **Analyze > Traffic > Application**; in the Interactive Report window on the left, change Site to “San Jose,” Application to “HTTP,” and Time Range to the range when the alert was received. This will display all the hosts using this protocol. You can see the Top hosts and verify there are no unauthorized hosts accessing this application. You can also access **Analyze > Traffic > Host** to view which conversations are chatty, and therefore causing the increase traffic for this application.

If the alarm is for an Application Response Time issue, you can access **Monitor > Response Time Summary** or **Analyze > Response Time > Application** to drill down on what hosts are accessing the application. Identify the application server and view what other applications are hosted and all the clients accessing that server.

See Monitor: Using Response Time Summary, page 3-5.

See Analyze: Measuring Response Time, page 3-18.

Using NAM for SmartGrid Visibility

The NAM will not recognize the IEC 60870 protocol out of the box (this is one of the main protocols used by power distribution companies). You will have to add a custom protocol, because it is a specific port you will be using. When you choose **Setup > Classification > Application Configuration**, you will see all hosts using that application. It will be identified as a Telnet application.

Customizing Cisco Prime NAM

This chapter provides set up details for advanced tools and customization. You can use these tools to take your network monitoring to another level. It provides information about functions that will begin automatically, optional tasks, and other setup tasks you will need to perform for advanced feature configuration.

This chapter contains the following sections:

For information about how to install the product, configure it, and log in, see the installation guide for your specific Cisco NAM platform.

Advanced Configuration Overview

Table 7-1 leads you through the advanced configuration steps you can follow for Prime NAM. See the description to understand why or when to perform these tasks.

Table 7-1 Advanced Configuration Overview

Action	Description	GUI Location	User Guide Location
Configure the Managed Device information	If you want to monitor an extended level of your managed device's data (health and interface information), you can set up your managed device using Cisco NAM. If you do not set up this feature, your data collection is limited. Depending on your NAM platform, managed device health and interface information will display in **Analyze > Managed Device** GUI. For service module NAM blades such as NAM-3, NAM-NX1, and SM-SRE NAM, the NAM managed device is the switch or router where NAM is located. Managed device SNMP credentials are automatically synchronized to the NAM upon NAM boot up. For other NAM platforms, the NAM managed device IP address, SNMP, and/or NetConf interface credential must be provided for NAM to get managed device health and interface information.	**Setup > Managed Device > Device Information**	See Accessing Device Interface and Health Details, page 7-39.
Configure sites	A *site* is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems. If you want to limit the view of your network data to a specific city, a specific building, or even a specific floor of a building, you can use the sites function. We recommend that sites are configured using prefix-based subnets instead of based on data source.	**Setup > Network > Sites**	See Configuring Sites, page 7-41.
Define alarms and thresholds	Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose for what types of events you want the software to notify you, and how you want to be notified. Create alarms that will be used for thresholds, then create the thresholds.	**Setup > Alarms > Actions** and **Setup > Alarms > Thresholds**	See Viewing Alarm Actions, page 7-31. See Defining Thresholds, page 7-31.

Table 7-1 Advanced Configuration Overview (continued)

Action	Description	GUI Location	User Guide Location
Configure capture	Capture allows you to configure up to ten sessions for capturing, filtering, and decoding packet data, manage the data in local or remote storage, and display the contents of the packets. Per file location, you can have only one capture session. We support up to ten capture sessions. **Note** NAM virtual blades do not support capture.	**Capture > Packet Capture/Decode**	See Capturing and Decoding Packets, page 4-1.
Configure scheduled export	You can set up scheduled jobs that generate daily reports at a specified time, in a specified interval, and then e-mail it to a specified e-mail address or addresses. Some windows may not support data export.	In the Interactive Report (left side of the dashboard), click **Export**. Scheduled Export can only be done from a Monitor or Analyze window.	See Scheduling Data Report Exports, page 7-37.
Set up TACACS+ server	TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization. When a user logs into Prime NAM, TACACS+ determines if the username and password are valid and what the access privileges are. For TACACS+ to work, both NAM and the TACACS+ server has to be configured.	**Administration > Users > TACACS+**	See Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 5-16.
Change system preferences	You can change many preferences, such as refresh interval, Top N Entries, Data Displayed, and enabling Audit Trail, as needed.	**Administration > System > Preferences**	See Performing User and System Administration

Setting Up Traffic Configurations

To set up Prime NAM traffic, you should perform the following:

- Configuring Traffic to Monitor, page 7-3
- (Optional) Setting Up Prime NAM Data Sources, page 7-5
- (Optional) Configuring Hardware Deduplication, page 7-28 (For specific NAM appliances only)

To view which traffic sources are supported on specific NAM platforms, see the *NAM Compatibility Matrix*.

Configuring Traffic to Monitor

Prime NAM can monitor your network traffic to perform many tasks including helping you to optimize your network resources and troubleshoot performance issues. Before you can monitor data, you must direct specific traffic flowing through a switch or router to the Prime NAM software for monitoring purposes.

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic.

The following sections describe SPAN sessions on devices running **Prime NAM**:

- Understanding How the Prime NAM Uses SPAN, page A-3
- Creating a SPAN Session, page 7-4
- Editing a SPAN Session, page 7-4

Note This functionality is only available when working with devices that support the CISCO-RMON-CONFIG-MIB. If you are using a switch that does not support this MIB, the SPAN screen may not show the existing SPAN sessions and will not allow SPAN configuration.

Creating a SPAN Session

To create a SPAN session on a switch:

Step 1 Choose **Setup > Traffic > SPAN Sessions**. The SPAN window displays.

Step 2 Click **Create**.

The Create SPAN Session Dialog displays. DataPort is the default for the SPAN Type. Contents of this window may be different depending on your NAM platform.

Step 3 Fill in the appropriate information on the Create SPAN Session window. See Table C-1.

Step 4 To create the SPAN session, click **Submit**. The Active Sessions window displays.

Step 5 To save the current active SPAN session in the running-configuration to the startup-configuration for switches running Cisco IOS software only, click **Save** in the active SPAN session window.

Note For switches running Cisco IOS software, *all* pending running-configuration changes will be saved to the startup-configuration.

Step 6 To verify the SPAN session was created and to view the data, go to the Top N charts on the Traffic Analysis dashboard (**Monitor > Overview > Traffic Summary**).

Editing a SPAN Session

You can only edit SPAN sessions that have been directed to the NAM. You can only delete certain SPAN sessions using the user interface.

Note Editing an existing SPAN session that has multiple SPAN destinations will affect all destinations.

To edit a SPAN session:

Step 1 Choose **Setup > Traffic > SPAN Sessions**.

The Active SPAN Sessions dialog box displays.

Step 2 Select the SPAN session to edit, then click **Edit**.

The Edit SPAN Session Dialog Box displays. The fields are described in Table C-2. Depending on your NAM platform, there may be different fields that display.

Step 3 Make the appropriate changes on the Edit SPAN Session window.

Setting Up Prime NAM Data Sources

Data sources are where the traffic sent to Prime NAM originates. Some examples are: physical dataports of the Prime NAM where you get SPAN data, a specific router or switch that sends NetFlow to the NAM, a WAAS device segment that sends data to Prime NAM, or ERSPAN and which goes to NAM management port.

Caution If you have configured sites (see Configuring Sites, page 7-41), you can assign data sources to that particular site. If you do this, and you also configure data sources, the two could overlap since sites can also be a primary "view" into data sources. If there is a mismatch between the two, you will not see any data.

Note We recommend that you configure a site using subnets instead of selecting a data source. For examples on how to specify a site using subnets, see Configuring Sites Using Subnets, page 7-43.

The following sections contains setup steps and specific information about the types of data sources available:

- Data Source Overview, page A-1
- Forwarding SPAN Traffic, page 7-5
- Forwarding ERSPAN Traffic, page 7-6
- Forwarding VACL Traffic, page 7-13
- Forwarding NetFlow Traffic, page 7-14
- Managing WAAS and WAN Traffic, page 7-20
- Ports and Hardware Details, page A-3

Forwarding SPAN Traffic

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. Depending on your platform, you can configure multiple SPAN sessions. For details on what platforms support SPAN, see the *NAM Compatibility Matrix*.

For more information about SPAN sessions, see Configuring Traffic to Monitor, page 7-3 or your platform operating system documentation.

Forwarding ERSPAN Traffic

This section describes how to configure Encapsulated Remote Switched Port Analyzer (ERSPAN) on your remote device as a Prime NAM data source. You configure ERSPAN as a Prime NAM data source from the remote device command line interface, not the Prime NAM GUI.

For details on which NAM platforms support ERSPAN, see the *NAM Compatibility Matrix*.

As an ERSPAN consumer, **Prime NAM** can receive ERSPAN packets on its management port from devices such as Cisco routers and switches. Those packets are analyzed as if that traffic had appeared on one of the Prime NAM dataports. Prime NAM supports ERSPAN versions 1 and 3. Incoming ERSPAN data is parsed by **Prime NAM**, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

Before You Begin

For the Prime NAM to receive ERSPAN from an external switch or router, that device must be configured to send ERSPAN packets to the IP address of the Cisco NAM.

To enable ERSPAN as a data source:

Note Depending on the Cisco IOS/Nexus OS version on the managed device, the CLI format for configuring an ERSPAN session may be different than what appears in this document. For details on using ERSPAN as a data source, see your specific OS product documentation.

Enabling Autocreation of ERSPAN Data Sources Using the Web GUI

There is a convenient autocreate feature for data sources, which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device that sends ERSPAN traffic to the NAM, after the first packet is received. Manual creation of ERSPAN data sources using the **Prime NAM** GUI or the CLI is typically not necessary. When manually creating a data source, you may specify any name you want for the data source. A data source entry must exist on the **Prime NAM** in order for it to accept ERSPAN packets from an external device.

Autocreated ERSPAN data sources will be assigned a name in the format *ERSPAN-<IP Address>-ID-<Integer>*, where *IP Address* is the IP address of the sending device, and *Integer* is the Session-ID of the ERSPAN session on that device. For example, device 192.168.0.1 sending ERSPAN packets with the Session ID field set to 12 would be named *ERSPAN-192.168.0.1-ID-12*. You can edit these autocreated data sources and change the name if desired.

One device can be configured to send multiple separate ERSPAN sessions to the same NAM. Each session will have a unique Session ID. **Prime NAM** can either group all sessions from the same device into one data source, or have a different data source for each Session ID. When data sources are autocreated,

they will be associated with one particular Session ID. When manually created, you can instruct **Prime NAM** to group all traffic from the same device into one data source. If you check the **Session** check box, and enter a Session ID in the Value field, the data source will only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

To configure **Prime NAM** to automatically create data sources when it receives ERSPAN packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Auto Create** on the bottom left of the window.

Step 3 Check the **ERSPAN** check box to toggle autocreation of ERSPAN data sources to "on".

Step 4 Click **Submit**.

Enabling Autocreation of ERSPAN Data Sources Using the CLI

Configuration of the autocreate feature is also possible using the **Prime NAM** CLI. Because the autocreate feature is turned on by default, in most cases these steps are not necessary.

To configure **Prime NAM** to automatically create data sources when it receives ERSPAN packets from an external device, use the **autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# autocreate-data-source erspan

ERSPAN data source autocreate successfully ENABLED
```

Prime NAM will now automatically create a ERSPAN data source for each device that sends ERSPAN packets to it. The data source will have the specific Session ID that is populated by the device in the ERSPAN packets sent to the NAM. If the same device happens to send ERSPAN packets to the Prime NAM with different Session ID values, a separate data source will be created for each unique Session ID sent from the device.

Disabling Autocreation of ERSPAN Data Sources Using the Web GUI

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Auto Create** on the bottom left of the window.

Step 3 Uncheck the **ERSPAN** check box to toggle autocreation of ERSPAN data sources to "off".

Step 4 Click **Submit**.

Disabling Autocreation of ERSPAN Data Sources Using the CLI

To disable autocreation of ERSPAN data sources, use the **no autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# no autocreate-data-source erspan
ERSPAN data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

Creating ERSPAN Data Sources Using the Web GUI

To manually configure a ERSPAN data source on the GUI, for example if the autocreation feature is turned off, use the following steps:

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Create** along the bottom of the window.

Step 3 From the Type drop-down list, choose **ERSPAN**.

Step 4 Enter the IP address of the device that will export ERSPAN to the NAM.

Step 5 Give the Data Source a name. This name will appear anywhere there is a Data Source drop-down list.

Step 6 (Optional) Check the **Session** check box and enter an Session ID into the Value field if the data source should only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

Devices can be configured with multiple ERSPAN Sessions. The packets exported may have the same source IP address, but the Session ID exported will be a different for each session. If you want to include only one Session in the data source, you must check the “Session” box and provide the value of that Session ID.

Step 7 Click **Submit**.

Creating ERSPAN Data Sources Using the CLI

To manually configure a ERSPAN data source on the **Prime NAM** using the CLI (for example if the autocreation feature is turned off), use the following steps. Note that when using the CLI, there are two separate phases involved: First, you must create a “device” entry on the **Prime NAM** and remember the device ID, and then you must create a data source entry using this device ID. In the **Prime NAM** GUI, these two phases for creating ERSPAN data sources are combined together.

Step 1 Enter the command **device erspan**. You will now be in erspan device subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# device erspan

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@172-20-104-107.cisco.com(sub-device-erspan)#
```

Step 2 Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                         - display help
address                   - device IP address (*)
cancel                    - discard changes and exit from subcommand mode
exit                      - create device and exit from sub-command mode
help                      - display help
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

Step 3 Enter the IP address of the device as shown in this example (required):

```
root@172-20-104-107.cisco.com(sub-device-erspan)# address 192.168.0.1
```

Step 4 Type **show** to look at the device configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-device-erspan)# show

DEVICE TYPE         : ERSPAN (Encapsulated Remote SPAN)
DEVICE ADDRESS      : 192.168.0.1


root@172-20-104-107.cisco.com(sub-device-erspan)#
```

Step 5 Type **exit** to come out of the subcommand mode and create the device. Remember the ID value that was assigned to the new device (you will need it to create the data source).

```
root@172-20-104-107.cisco.com(sub-device-erspan)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#
```

Step 6 Enter the command **data-source erspan**. You will now be in erspan data source subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# data-source erspan

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

Step 7 Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# ?
?                          - display help
cancel                     - discard changes and exit from subcommand mode
device-id                  - erspan device ID (*)
exit                       - create data-source and exit from sub-command mode
help                       - display help
name                       - data-source name (*)
session-id                 - erspan Session ID
show                       - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

Step 8 Enter the device ID from Step 4.

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# device-id 1
```

Step 9 Enter the name you would like for the data source (required):

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# name MyFirstErspanDataSource
```

Step 10 If desired, supply the specific Session ID for this ERSPAN data source (optional):

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# session-id 123
```

Step 11 Enter **show** to look at the data source configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show

DATA SOURCE NAME : MyFirstErspanDataSource
DATA SOURCE TYPE : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID        : 1
DEVICE ADDRESS   : 192.168.0.1
```

```
SESSION ID       : 123

root@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

Step 12 Enter **exit** to come out of the subcommand mode and create the data source:

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# exit
Data source created successfully, ID = 3
```

The data source is now created, and ERSPAN records from the device will be received and accepted by Prime NAM as they arrive.

Deleting ERSPAN Data Sources Using the Web GUI

To delete an existing ERSPAN data source, use the following steps. Note that if the autocreation feature is turned on, and the device continues to send ERSPAN packets to the NAM, the data source will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Choose the data source you would like to delete.

Step 3 Click **Delete** along the bottom of the window.

Deleting ERSPAN Data Sources Using the CLI

To delete a ERSPAN data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.

Step 1 Show all data sources so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show data-source

DATA SOURCE ID   : 1
DATA SOURCE NAME : DATA PORT 1
TYPE             : Data Port
PORT NUMBER      : 1
-----------

DATA SOURCE ID   : 2
DATA SOURCE NAME : DATA PORT 2
TYPE             : Data Port
PORT NUMBER      : 2
-----------

DATA SOURCE ID   : 3
DATA SOURCE NAME : MyFirstErspanDataSource
TYPE             : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID        : 2
DEVICE ADDRESS   : 192.168.0.1
```

```
ENGINE ID        : 123
-----------

root@172-20-104-107.cisco.com#
```

Step 2 Use the **no data-source** command to delete the data source:

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

Step 3 Show all devices so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show device

DEVICE ID            : 1
DEVICE TYPE          : ERSPAN (Encapsulated Remote SPAN)
IP ADDRESS           : 192.168.0.1
INFORMATION          : No packets received
STATUS               : Inactive
------

root@172-20-104-107.cisco.com#
```

Step 4 Use the **no device** command to delete the device:

```
root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#
```

Note that if the autocreation mode is on, and the device continues to send ERSPAN packets to the NAM, the data source (and device entry) will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

Configuring ERSPAN on Devices

There are two ways to configure ERSPAN so that the Prime NAM receives the data:

- Sending ERSPAN Data to Layer 3 Interface, page 7-11
- Sending ERSPAN Data Directly to the Cisco NAM Management Interface, page 7-12

Note Depending on the Cisco IOS or NX-OS version on your managed device, the CLI format for configuring an ERSPAN session may be different than what appears in this document. For details on using ERSPAN as a data source, see your specific OS product documentation.

Sending ERSPAN Data to Layer 3 Interface

To send the data to a layer 3 interface on the Switch housing the NAM, configure the ERSPAN source session. The ERSPAN destination session then sends the traffic to a Prime NAM data-port. After performing this configuration, you can select the DATA PORT X data source to analyze the ERSPAN traffic.

Note This method causes the ERSPAN traffic to arrive on one of the NAM dataports, which is the most efficient method and will not have any adverse effect on the NAM's IP connectivity. Therefore, we recommend this method. The configuration below may be different depending on your platform and OS version. See your OS product documentation for additional help.

Sample Configuration of ERSPAN Source

```
monitor session 48 type erspan-source
    erspan-id N
    vrf default
    destination ip aa.bb.cc.dd
    source interface Ethernet7/47
    no shut
monitor erspan origin ip-address ee.ff.gg.hh global
```

Where:

- *erspan-id N* is the ERSPAN ID
- *aa.bb.cc.dd* is the IP address of the destination switch (loopback address or any routable IP address)
- *ee.ff.gg.hh* is the source IP address of the ERSPAN traffic

Sample Configuration of ERSPAN Destination

```
monitor session 48 type erspan-destination
    erspan-id N
    vrf default
    source ip aa.bb.cc.dd
    no shut
```

Where:

- erspan-id *N* matches the ERSPAN ID at the source switch
- *aa.bb.cc.dd* is the IP address defined at the destination

You can now connect to the Prime NAM to monitor and capture traffic of the Data Port 2 data source.

Sending ERSPAN Data Directly to the Cisco NAM Management Interface

To send the data directly to the Cisco NAM management IP address (management-port), configure the ERSPAN source session. No ERSPAN destination session configuration is required. After performing this configuration on the Catalyst 6500 switch, when ERSPAN packets are sent to the NAM, it will automatically create a data source for that packet stream. If the autocreate feature is not enabled, you will have to manually create the data source for this ERSPAN stream of traffic (see Creating ERSPAN Data Sources Using the Web GUI, page 7-8).

Note This method causes the ERSPAN traffic to arrive on the Cisco NAM management port. If the traffic level is high, this could have negative impact on the NAM's performance and IP connectivity.

Sample Configuration

```
monitor session 1 type erspan-source
no shut
source interface Fa3/47
    destination
        erspan-id  Y
        ip address aa.bb.cc.dd
        origin ip address ee.ff.gg.hh
```

Where:

- Interface fa3/47 is a local interface on the erspan-source switch to be monitored
- *Y* is any valid span session number
- *aa.bb.cc.dd* is the management IP address of the NAM
- *ee.ff.gg.hh* is the source IP address of the ERSPAN traffic

Forwarding VACL Traffic

You can use VLAN access control (VACL) lists to filter packet data and expand your device's capability beyond the two SPAN session limitation. For details on which devices support VACL, see the *NAM Compatibility Matrix*.

VACL can forward traffic from either a WAN interface or VLANs to a dataport on some of the NAM platforms. A VACL provides an alternative to using SPAN; a VACL can provide access control based on Layer 3 addresses for IP and IPX protocols. The unsupported protocols are access controlled through the MAC addresses. A MAC VACL cannot be used to access control IP or IPX addresses.

Configuring VACL on a WAN Interface

Because WAN interfaces do not support the SPAN function, you must use the switch CLI to manually configure a VACL in order to monitor WAN traffic with the NAM. This feature only works for IP traffic over the WAN interface.

VACL can also be used if there is no available SPAN session to direct traffic to the NAM. In this case, a VACL can be set up in place of a SPAN for monitoring VLAN traffic.

The following example shows how to configure a VACL on an ATM WAN interface and forward both ingress and egress traffic to the NAM. These commands are for switches running Cisco IOS version 12.1(13)E1 or higher. For more information on using these features, see your accompanying switch documentation.

```
Cat6509#config terminal
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface AM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

To monitor egress traffic only, get the VLAN ID that is associated with the WAN interface by using the following command:

```
Cat6509#show cwan vlan
Hidden      VLAN    swidb->i_number    Interface
1017        94                         ATM6/0/0.1
```

After you have the VLAN ID, configure the Cisco NAM dataport using the following command:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017
```

To monitor ingress traffic only, replace the VLAN number in the capture configuration with the native VLAN ID that carries the ingress traffic. For example, if VLAN 1 carries the ingress traffic, you would use the following command:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
```

Configuring VACL on a LAN VLAN

For VLAN Traffic monitoring on a LAN, traffic can be sent to Cisco NAM by using the SPAN feature of the switch. However, in some instances when the traffic being spanned exceeds the monitoring capability of the NAM, you might want to pre-filter the LAN traffic before it is forwarded. This can be done by using VACL.

The following example shows how to configure VACL for LAN VLAN interfaces. In this example, all traffic directed to the server 172.20.10.221 on VLAN 1 is captured and forwarded to the Cisco NAM located in slot 3.

```
Cat6509#config terminal
Cat6509#(config)#access-list 100 permit ip any any
Cat6509#(config)#access-list 110 permit ip any host 172.20.10.221
Cat6509#(config)#vlan access-map lan 100
Cat6509#(config-access-map)match ip address 110
Cat6509#(config-access-map)#action forward capture
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan access-map lan 200
Cat6509#(config-access-map)#match ip address 100
Cat6509#(config-access-map)#action forward
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan filter lan vlan-list 1
Cat6509#(config)#analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509#(config)#analysis module 3 data-port 1 capture
Cat6509#(config)#exit
```

Forwarding NetFlow Traffic

NAM functions as a NetFlow consumer. You can configure NetFlow on the device side so that Prime NAM can receive NetFlow packets from devices such as Cisco routers and switches. Those records are stored in its collection database as if that traffic had appeared on one of the Cisco NAM dataports. **Prime NAM** understands NetFlow version 5 and version 9. Incoming NetFlow data is parsed by **Prime NAM**, stored in its internal database, and presented in the user interface in the same way as traffic from other data sources.

For **Prime NAM** to receive NetFlow packets from an external switch or router, you must configure that device to forward export flow records to the NAM's IP address and the correct UDP port number. The default port number on which Prime NAM listens for NetFlow packets is port 3000. This port can be modified using the **Prime NAM** CLI, but it is critical that the same port be configured on the Cisco NAM and the exporting device or devices. Depending on the external device, you may need to enable the NetFlow feature on a per-interface basis.

See the following sections about NetFlow as a data source:

- Understanding NetFlow Interfaces, page A-6
- Understanding NetFlow Flow Records, page A-7
- Managing NetFlow Data Sources, page A-7
- Configuring NetFlow on Devices, page 7-15

Configuring NetFlow on Devices

The configuration commands for NetFlow devices to export NetFlow packets to Prime NAM are platform and device specific. The example configuration commands provided here are the ones most commonly found for devices running Cisco IOS. For more detailed NetFlow configuration information, see your device documentation.

Enabling Autocreation of NetFlow Data Sources Using the Web GUI

To configure **Prime NAM** to automatically create data sources when it receives NetFlow packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Auto Create** on the bottom left of the window.

Step 3 Check the **Netflow** check box to toggle autocreation of NetFlow data sources on.

Step 4 Click **Submit**.

Enabling Autocreation of NetFlow Data Sources Using the CLI

Configuration of the autocreate feature is also possible using the **Prime NAM** CLI. Remember that the autocreate feature is turned ON by default, so in most cases these steps are not necessary.

To configure the **Prime NAM** to automatically create data sources when it receives NetFlow packets from an external device, use the following steps:

Use the **autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# autocreate-data-source netflow
NetFlow data source autocreate successfully ENABLED
```

Prime NAM will now automatically create a NetFlow data source for each device that sends NetFlow packets to it. The data source will have the specific Engine ID that is populated by the device in the NetFlow packets sent to the NAM. If the same device happens to send NetFlow packets to the NAM with different Engine ID values, a separate data source will be created for each unique Engine ID sent from the device.

Disabling Autocreation of NetFlow Data Sources Using the Web GUI

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Auto Create** on the bottom left of the window.

Step 3 Uncheck the **Netflow** check box to toggle autocreation of NetFlow data sources off.

Step 4 Click **Submit**.

Disabling Autocreation of NetFlow Data Sources Using the CLI

To disable autocreation of NetFlow data sources, use the **no autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# no autocreate-data-source netflow
NetFlow data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

Creating NetFlow Data Sources Using the Web GUI

To manually configure a NetFlow data source using the **Prime NAM** GUI, for example if the autocreation feature is turned OFF, use the following steps:

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Create** along the bottom of the window.

Step 3 Give the Data Source a name. This name will appear anywhere there is a Data Source drop-down list.

Step 4 From the Type drop-down list, choose **NetFlow**.

Step 5 Enter the IP address of the device that will export NetFlow to Prime NAM (required).

Step 6 (Optional) If you know the specific value of the Engine ID on the device you would like to monitor, check the **Engine** check box, and enter the value of the Engine ID. If the **Engine** check box is left unchecked, then all NetFlow records exported by the device will be grouped into the same data source, regardless of the Engine ID populated in the NetFlow packets (in most cases the **Engine** check box can be left blank and you don't have to worry about the Engine ID value).

Some devices have multiple Engines which independently export NetFlow records. For example, on some Cisco routers, NetFlow records can be exported by the Supervisor module as well as individual line cards. The packets exported may have the same source IP address, but the Engine ID exported by the Supervisor will be a different value than the Engine ID(s) exported by the line card(s). If you want to include only one Engine in the data source, you must check the “Engine” box and provide the value of that Engine ID.

Step 7 (Optional) SNMP v1/v2c RO Community String: If SNMP v1 or v2c will be used to communicate with the device, enter the community string that is configured on the device that is going to export NetFlow packets to the NAM.

Step 8 (Optional) “Enable SNMP v3”: If SNMP v3 will be used to communicate with the device, fill in the fields within the v3-specific dialog.

Step 9 (Optional) If desired, fill in the SNMP credentials for the device. If valid SNMP credentials are provided, **Prime NAM** can upload readable text strings from the device to describe the interfaces on that device rather than just displaying the interfaces as numbers. You may specify either SNMPv2c or SNMPv3 credentials. See Table C-3.

Step 10 Click **Test Connectivity** to see if the information you provided is accurate.

Step 11 Click **Submit**.

Creating NetFlow Data Sources Using the CLI

To manually configure a NetFlow data source on the Prime NAM using the CLI, for example if the autocreation feature is turned off, use the following steps. Note that when using the CLI, there are two separate phases involved. First you must create a “device” entry on the Prime NAM and remember the device ID. Then you must create a data source entry using this device ID. For convenience, these two phases are combined together when using the GUI to create NetFlow data sources.

Step 1 Enter the command **device netflow**. You will now be in netflow device subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# device netflow

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

Step 2 Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                         - display help
address                   - device IP address (*)
cancel                    - discard changes and exit from subcommand mode
community                 - SNMPv2c community string
exit                      - create device and exit from sub-command mode
help                      - display help
show                      - show current config that will be applied on exit
snmp-version              - SNMP version to use to communicate with device
v3-auth-passphrase        - SNMPv3 authentication passphrase
v3-auth-protocol          - SNMPv3 authentication protocol
v3-priv-passphrase        - SNMPv3 privacy passphrase
v3-priv-protocol          - SNMPv3 privacy protocol
v3-sec-level              - SNMPv3 security level
v3-username               - SNMPv3 username

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

Step 3 Enter the IP address of the device as shown in this example (required):

```
root@172-20-104-107.cisco.com(sub-device-netflow)# address 192.168.0.1
```

Step 4 If desired, enter the SNMP credentials for the device, as in the example below. If you specify snmp-version v2c, then you should enter the community string for the device. If you specify snmp-version v3, then you should enter the security level, username, authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase.

```
root@172-20-104-107.cisco.com(sub-device-netflow)# snmp-version v2c
root@172-20-104-107.cisco.com(sub-device-netflow)# community public
```

Step 5 Enter **show** to look at the device configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# show

DEVICE TYPE         : NDE (Netflow Data Export)
DEVICE ADDRESS      : 192.168.0.1
SNMP VERSION        : SNMPv2c
V2C COMMUNITY       : public
V3 USERNAME         :
V3 SECURITY LEVEL   : No authentication, no privacy
V3 AUTHENTICATION   : MD5
V3 AUTH PASSPHRASE  :
V3 PRIVACY          : DES
V3 PRIV PASSPHRASE  :

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

Step 6 Enter **exit** to come out of the subcommand mode and create the device. Remember the ID value that was assigned to the new device, you will need it to create the data source!

```
root@172-20-104-107.cisco.com(sub-device-netflow)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#
```

Step 7 Enter the command **data-source netflow**. You will now be in netflow data source subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# data-source netflow

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

Step 8 Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# ?
?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - netflow device ID (*)
engine-id                 - netflow Engine ID
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

Step 9 Enter the device ID from Step 4 (required):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# device-id 1
```

Step 10 Enter the name you would like for the data source (required):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# name MyFirstNdeDataSource
```

Step 11 If desired, supply the specific Engine ID for this NetFlow data source (optional):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# engine-id 123
```

Step 12 Enter **show** to look at the data source configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show

DATA SOURCE NAME : MyFirstNdeDataSource
DATA SOURCE TYPE : NDE (Netflow Data Export)
DEVICE ID       : 1
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123

root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

Step 13 Enter **exit** to come out of the subcommand mode and create the data source:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# exit
Data source created successfully, ID = 3
```

The data source is now created, and NetFlow records from the device will be received and accepted by the Prime NAM as they arrive.

Deleting NetFlow Data Sources Using the Web GUI

To delete an existing NetFlow data source, use the following steps. If the autocreation feature is turned on, and the device continues to send NetFlow packets to the NAM, the data source will be recreated again automatically as soon as the next NetFlow packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click on the data source you would like to delete.

Step 3 Click **Delete**.

Deleting NetFlow Data Sources Using the CLI

To delete a NetFlow data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.

Step 1 Show all data sources so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show data-source

DATA SOURCE ID   : 1
DATA SOURCE NAME : DATA PORT 1
TYPE             : Data Port
PORT NUMBER      : 1
-----------

DATA SOURCE ID   : 2
DATA SOURCE NAME : DATA PORT 2
TYPE             : Data Port
PORT NUMBER      : 2
-----------

DATA SOURCE ID   : 3
DATA SOURCE NAME : MyFirstNdeDataSource
TYPE             : NDE (Netflow Data Export)
DEVICE ID        : 2
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123
-----------

root@172-20-104-107.cisco.com#
```

Step 2 Use the **no data-source** command to delete the data source:

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

Step 3 Show all devices so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show device

DEVICE ID            : 1
DEVICE TYPE          : NDE (Netflow Data Export)
IP ADDRESS           : 192.168.0.1
SNMP VERSION         : SNMPv2c
V2C COMMUNITY        : public
V3 USERNAME          :
V3 SECURITY LEVEL    : No authentication, no privacy
V3 AUTHENTICATION    : MD5
V3 AUTH PASSPHRASE   :
V3 PRIVACY           : DES
V3 PRIV PASSPHRASE   :
INFORMATION          : No packets received
STATUS               : Inactive
------

root@172-20-104-107.cisco.com#
```

Step 4 Use the **no device** command to delete the device:

```
root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#
```

Note that if the autocreation mode is on, and the device continues to send NetFlow packets to the NAM, the data source (and device entry) will be re-created again automatically as soon as the next NetFlow packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

Testing NetFlow Devices

You can test the SNMP community strings for the devices in the Devices table. To test a device, select it from the Devices table, then click **Test**. The Device System Information Dialog Box displays. See Table C-4 for a description of the fields.

If the device is sending NetFlow Version 9 (V9) and the **Prime NAM** has received the NetFlow templates, then a V9 Templates button appears below the Device System Information window.

Note NetFlow v9 templates do not appear in all NetFlow packets. When there are no templates, the **V9 Templates** button does not appear.

Managing WAAS and WAN Traffic

This section contains the following topics about using the **Prime NAM** GUI to manage WAAS data sources:

- Understanding WAAS, page 7-21
- Considering Deployment Scenarios, page 7-22
- Using the WAAS Central Manager, page 7-22
- Monitoring Response Time from WAAS Data Sources, page 7-23

Understanding WAAS

Cisco Wide Area Application Services (WAAS) software optimizes the performance of TCP-based applications operating in a wide area network (WAN) environment and preserves and strengthens branch security. The WAAS solution consists of a set of devices called Wide Area Application Engines (WAEs) that work together to optimize WAN traffic over your network.

When client and server applications attempt to communicate with each other, the network devices intercept and redirect this traffic to the WAEs to act on behalf of the client application and the destination server.

WAEs provide information about packet streams traversing through both LAN and WAN interfaces of WAAS WAEs. Traffic of interest can include specific servers and types of transaction being exported. **Prime NAM** processes the data exported from the WAAS and performs application response time calculations and enters the data into reports you set up.

The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network not optimized.

You can use the WAAS Top Talkers Detail Dashboard to analyze the traffic for optimization. See Analyzing Traffic for Optimization Using the Top Talkers Detail, page 3-17 for more information.

Cisco WAAS helps enterprises to meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
  - Low data rates (constrained bandwidth)
  - Slow delivery of frames (high network latency)
  - Higher rates of packet loss (low reliability)

For more information about WAAS and configuring the WAAS components, see the *Cisco Wide Area Application Services Configuration Guide*.

Considering Deployment Scenarios

Table 7-2 lists six different deployment scenarios you might consider to monitor the optimized traffic on your WAAS network. Scenario #1 is typical when using NAM-3 blades.

Table 7-2 WAAS Data Source Configurations

	Deployment Scenario	Edge WAE Data Source	Core WAE Data Source
1	• Clients in the edge (branch) • Servers in the core (data center) • NAM in the core	Client	Server Server WAN
2	• Clients in the edge (branch) • Servers in the core (data center) • NAM in the edge	Client Client WAN	Server
3	• Servers in the edge (branch) • Clients in the core (data center) • NAM in the core	Server	Client Client WAN
4	• Servers in the edge (branch) • Clients in the core (data center) • NAM in the edge	Server Server WAN	Client
5	• Clients and servers in the edge (branch) and the core (data center) • NAM in the core	Client Server	Client Server Client WAN Server WAN
6	• Clients and servers in the edge (branch) and the core (data center) • NAM in the edge	Client Server Client WAN Server WAN	Client Server

Using the WAAS Central Manager

The Cisco WAAS is centrally managed by a scalable, secure, and simple function called the Cisco WAAS Central Manager, which runs on Cisco WAE Appliances. The Cisco WAAS Central Manager provides a centralized mechanism for configuring features, reporting, and monitoring, and can manage a topology containing thousands of Cisco WAE nodes.

Prime NAM is accessible from within the Central Manager interface. Prime NAM integration with WAAS Central Manager provides for easier viewing of **Prime NAM** reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments.

Below is a standard configuration workflow that you can follow.

Prerequisites are that the WAAS Central Manager is installed and functional, and the Cisco NAM (device or virtual blade) is installed and functional.

Step 1 From the WAAS Central Manager, configure the Cisco NAM IP address and login credentials.

Step 2 From the router or switch, configure the data source(s) for baseline (SPAN).

Step 3 From the WAAS Central Manager, configure the Site definition. See Configuring Sites, page 7-41 for more information.

Step 4 In the Monitor section of WAAS Central Manager, one can observe the Top Talkers under the Network Analysis tab. See Analyzing Traffic for Optimization Using the Top Talkers Detail, page 3-17 for more information.

Step 5 From the WAAS Central Manager, configure the WAAS Flow Agent and branch/data center WAEs.

Step 6 Create Device Groups for the branch and data center on the WAAS Central Manager, and assign a device to the Device Groups.

Step 7 Enable the Flow Agent on the WAAS, pointing to the Cisco NAM IP. Segments are automatically selected (enabled only if Cisco NAM is configured). **Prime NAM** will start to compute baseline ART, protocol distribution, and Top Talkers. See Enabling WAAS Flow Agent, page 7-25.

Step 8 Turn on WAAS optimization. See Optimizing WAN, page 3-16 for more information.

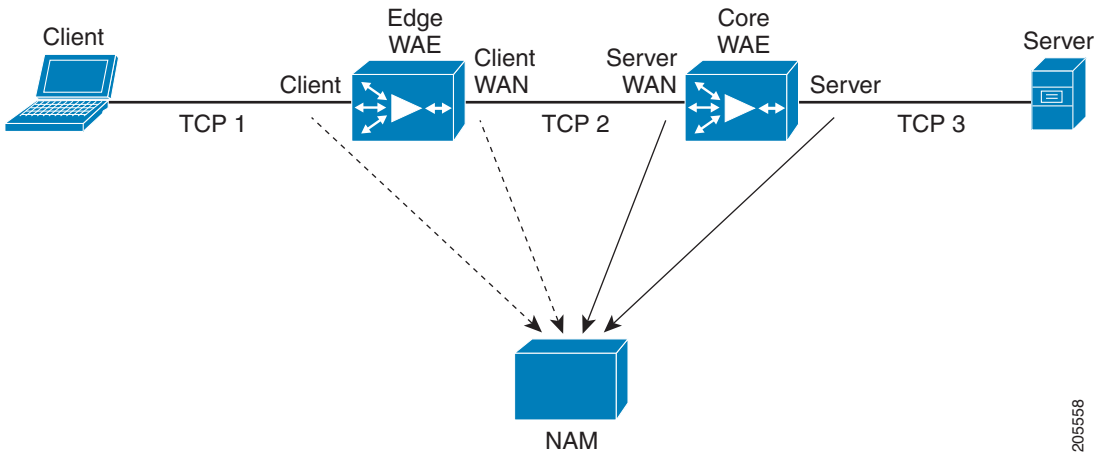
Step 9 Turn on the Flow Agent and identify the servers to monitor to get ART improvements. See Editing WAAS Data Sources, page 7-26.

Monitoring Response Time from WAAS Data Sources

Prime NAM processes the TCP flow data exported from the WAAS and performs application response time (ART) calculations and reports. You use the **Prime NAM** GUI to create a WAAS data source to monitor WAAS traffic statistics. In addition to ART, Prime NAM monitors and reports other traffic statistics of the WAAS data sources including application, host, and conversation information.

Prime NAM provides different ART metrics by collecting data at different points as packets flow along their paths. **Prime NAM** provides five different collection points, each represented by a WAAS data source. Figure 7-1, WAAS Data Sources (Data Collection Points), shows an example of the data collection points. The solid line represents data exported from a WAAS device and/or directly monitored traffic like SPAN. The broken line represents data exported from a WAAS device only.

Figure 7-1 WAAS Data Sources (Data Collection Points)



You can use the **Prime NAM** GUI to configure data sources at the locations in the network described in Table 7-3.

Table 7-3 WAAS Data Collection Points

Setting	Description
Client	This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to **Prime NAM** for monitoring. To monitor this point, configure a Client data source.
Client WAN	This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to **Prime NAM** for monitoring. To monitor this point, configure a Client WAN data source.
Server WAN	This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to **Prime NAM** for monitoring. To monitor this point, configure a Server WAN data source.
Server	This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to **Prime NAM** for monitoring. To monitor this point, configure a Server data source.
Passthrough	This setting configures the WAE device to export the TCP flows that are passed through unoptimized.

You can also configure a data source to use Export Passthrough data. For more information about configuring WAAS data sources, see Editing WAAS Data Sources, page 7-26.

Monitoring Client Data Sources

By monitoring the TCP connections between the client and the WAE device (Client segment in Figure 7-1), you can measure the following ART metrics:

- Total Response Time as experienced by the client
- Total Transaction Time as experienced by the client
- Bandwidth usage (bits/packets) before optimization
- Number of transactions and connections.

- Network Time broken down into two segments: client-edge and edge-server

To view detailed views of this data, select the **Analyze > Response Time**. > **Detailed Views** submenu.

Monitoring WAN Data Sources

By monitoring the TCP connections between the edge and core WAE devices (Client WAN and Server WAN segments in Figure 7-1), you can measure the following:

- Bandwidth usage (bits/packets) after optimization
- Network Time of the WAN segment

Monitoring Server Data Sources

By monitoring the TCP connections between the core WAE devices and the servers (Server segment in Figure 7-1), you can measure the following ART metrics:

- Server Response Time (without proxy acceleration/caching server)
- Network Time between the core WAE device and the servers

Note **Prime NAM** measures Network Time by monitoring the TCP three-way handshake between the devices.

Enabling WAAS Flow Agent

Before you can monitor WAAS traffic, you must first configure the WAAS device to export WAAS flow record data to the **Prime NAM.** Use the following WAAS command-line interface (CLI) **flow monitor** command to enable the Flow Agent on the WAAS:

flow monitor tcpstat-v1 host <*nam IP address*>

flow monitor tcpstat-v1 enable

After you enable flow export to the **Prime NAM** using WAAS CLI commands like those above, WAAS devices will be detected and automatically added to the NAM's WAAS device list.

You must then configure the WAAS segments you want to monitor as WAAS data sources: Client, Client WAN, Server WAN, and/or Server. See Editing WAAS Data Sources, page 7-26, for more detailed information.

You can also use the WAAS Central Manager to centrally issue WAAS CLI commands to configure a large number of WAEs at one time. **Prime NAM** is accessible from within the WAAS Central Manager interface. For more information about WAAS Central Manager, refer to the WAAS technical documentation.

Note In addition to configuring the WAAS devices, you must specify which application servers you want to monitor among the servers being optimized by WAAS devices. See Configuring WAAS Monitored Servers, page 7-59, for more detailed information.

For more information about WAAS and configuring the WAAS components, see the *Cisco Wide Area Application Services Configuration Guide*.

This section contains the following topics:

- Editing WAAS Data Sources, page 7-26
- Deleting a WAAS Data Source, page 7-27

Adding Data Sources for New WAAS Device

Prime NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up **Prime NAM** to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

Note This step is not usually necessary because export-enabled WAAS devices are detected and added automatically. See Enabling WAAS Flow Agent, page 7-25, for more information about how to enable WAAS export to the NAM.

To manually add a WAAS device to the list of devices monitored by **Prime NAM**:

Step 1 Choose **Setup > Traffic > NAM Data Sources**.

Step 2 Click **Create**.

The Prime NAM Data Source Configuration Dialog appears.

Step 3 Choose “WAAS” from the list of Types.

Step 4 Enter the device IP address in the IP field.

Step 5 Check the check boxes for the appropriate WAAS Segments. See Table 7-3.

Step 6 Click **Submit** to add the new WAAS custom data source.

Editing WAAS Data Sources

Prime NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up **Prime NAM** to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

To edit a WAAS device’s custom data source:

Step 1 Choose **Setup > Traffic > NAM Data Sources**. The data sources are displayed.

Step 2 Choose the WAAS device you want to modify, and then click **Edit**.

You can configure the WAAS data sources to monitor the following WAAS segments as shown in Figure 7-1, WAAS Data Sources (Data Collection Points):

- Client—This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to **Prime NAM** for monitoring.
- Client WAN— This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to **Prime NAM** for monitoring.
- Server WAN—This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to **Prime NAM** for monitoring.

- Server—This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to **Prime NAM** for monitoring.

SPAN data sources might take the place of the WAE Server data sources listed in Table 7-2. For example, if you already configure SPAN to monitor the server LAN traffic, it is not necessary to enable the Server data source on the WAE device.

Note The following step is optional and applies only when **Prime NAM** is configured to export data to an External Response Time Reporting Console, such as the NetQos Super Agent.

Deleting a WAAS Data Source

To delete a WAAS custom data source:

Step 1 Choose **Setup > Traffic > NAM Data Sources**. The data sources are displayed.

Step 2 Choose the WAAS custom data source you want to delete, then click **Delete**.

A dialog box displays the device address and asks if you are sure you want to delete the device.

Auto Create of New WAAS Devices

If you have numerous WAE devices, you can set up **Prime NAM** to configure newly discovered WAE devices using a predefined configuration template using the **Prime NAM** auto configuration option.

Note If most of your WAE devices are edge WAE, you might want to set the auto configuration to be that of the edge device, then manually configure the data center WAE. For example, select the Client segment for monitoring.

To configure WAAS autoconfiguration:

Step 1 Choose **Setup > Traffic > NAM Data Sources**. The data sources are displayed.

Step 2 Click **Auto Create**.

The Prime NAM Data Source Configuration Dialog displays.

Step 3 Check the **WAAS** check box.

Step 4 Check the check boxes for the desired Segments. See Editing WAAS Data Sources, page 7-26, for more information.

Configuring Hardware Deduplication

Note This section applies only to Cisco NAM 2320, 2220, and 2204 appliances.

Prime NAM supports hardware-based detection of duplicate packets and allows you to configure a single deduplication filter that reduces the amount of duplicate traffic across all adapter ports.

You can use deduplication to eliminate redundant data. This can help to significantly shrink storage requirements and improve bandwidth efficiency on tasks like backup and recovery.

After you enable deduplication, the NAM appliance detects and filters the duplicated packets. The packet is identified as duplicated if all inspected segments match another packet within the specific time window.

In addition to the duration-based timeout, there is also a fixed packet-count timeout. There cannot be more than 7 packets between the duplicate packets. If packets 0 and 8 are identical, packet 8 *will* be dropped. If packets 0 and 9 are identical, packet 9 *will not* be dropped.

To configure packet deduplication:

Step 1 Choose **Setup > Traffic > Hardware Deduplication**.

Step 2 Check the **Enabled** check box to enable packet deduplication.

Enter a value in the Time Window (1-127 in microseconds (µs)) for the search or buffer period.

The value you set in the Time Window indicates the length of time (n microseconds) in which two packets can be considered duplicates. If the Time Window is 100 µs but two identical packets arrive 120 µs apart, the second packet would not be dropped. If the identical packets arrive 80 µs apart, the second packet would be dropped.

Step 3 Click to choose a segment of the packet to inspect for deduplication.

The default inspects the entire packet. The second option inspects all segments except the ISL portion of the packet. The third option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The fourth option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The final (bottom) option inspects only the UDP/TCP and payload segments of the packet.

Note Regardless of the option you choose, the packet checksum is ignored.

Step 4 Click **Submit** to enable the settings you have entered, or click **Reset** to cancel any change.

Setting Up Alarms and Alarm Thresholds

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose what types of events for which you want Prime NAM to notify you, and how you want to be notified. Monitoring alarms enables you to watch problem areas and collect data on areas such as increased utilization, severe application response delays, and voice quality degradation.

This is the order that you typically follow for setting up alarms and alarm thresholds:

Step 1 Define the way you would like to be notified when an alarm occurs (by e-mail, trap, trigger capture, or syslog).

- For e-mail server settings: Choose **Administration > System > E-Mail Setting**
- For trap settings: Choose **Administration > System > SNMP Trap Setting**
- For capture session settings: Choose **Capture > Packet Capture/Decode > Sessions**
- For syslog settings: Choose **Administration > System > Syslog Setting**

Step 2 Define the Alarm Action at **Setup > Alarms > Actions**.

Step 3 Define the Threshold for this alarm at **Setup > Alarms > Thresholds**.

The tasks for setting up alarms are:

- Configuring Alarm Actions, page 7-29
- Viewing Alarm Actions, page 7-31
- Defining Thresholds, page 7-31

Configuring Alarm Actions

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both.

When a threshold's rising water mark is crossed, the alarm condition is met. This triggers the alarm action to take effect.

To configure an alarm action:

Step 1 Choose **Setup > Alarms > Actions**.

The Alarm Action page displays any configured actions. If none of the four actions (e-mail, trap, capture, or syslog) are configured, you will see `No data available`.

Step 2 Click **Create**.

Step 3 Enter a Name for the action (up to 63 characters).

Step 4 Choose the type of alarm action. Prime NAM supports any combination of these four actions in one alarm condition:

Alarm Action	Description	Important Notes
E-mail syslog	An alarm action that e-mails the syslog content of the alarm condition. To avoid e-mail flooding the network, **Prime NAM** does not send more than five e-mails in any given hour.	Configure the e-mail address in **Administration > System > E-Mail Setting**. Prime NAM alarm mail is sent as a result of Prime NAM alarms, not router or switch alarms. Prime NAM sends up to five e-mails per hour per function (traffic and NetFlow, voice signaling, RTP, and application response time). Also, in each e-mail, there could be up to five alarm messages. These limits are in place to avoid e-mail overload. If you have configured e-mail alarms and do not receive e-mail, then your Prime NAM does not have any alarms. If Prime NAM sends you many alarm messages, the e-mail may state, for example, "5 of 2,345 alarm messages."
Trap	An alarm action that sends Prime NAM trap messages to one or more trap servers. Any trap server that has the same community string will receive the trap message. Prime NAM uses Cisco Syslog MIB in the trap message. To avoid trap flooding, the limit is ten trap messages per interval.	Choose the SNMP community where you would like traps to be sent. Configure the community string in **Administration > System > SNMP Trap Setting**. After the "Community field appears, choose the community string from the drop-down list.
Trigger capture	An alarm action to start or stop a pre-defined capture session or stop a capture to save it to a file.	From the Session drop-down, choose the session (the list will be empty if there is no capture session configured in **Capture > Packet Capture/Decode > Sessions**). Click the **Start Capture**, **Stop Capture**, or **Stop Capture and Save to File** radio button. For more details, see Understanding Trigger Capture, page 7-31.
Remote syslog	An alarm action that sends syslog messages to remote syslog servers. The limit is ten syslog messages per interval to avoid flooding the network.	This will log syslog messages. The default setting is to log syslog messages locally to Prime NAM. If you want to log syslog messages to remote servers, set up the destination information at **Administration > System > Syslog Setting**.

Step 5 To edit or delete alarm actions, select the alarm and use the appropriate button.

Step 6 Click **Submit**.

The Alarm Action table displays the newly configured action in its list.

Viewing Alarm Actions

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation and be alerted to potential problems.

Prime NAM supports IPv6 for all alarm functionality.

Note You could see two alarms for the same occurrence if both the source and the destination are in the same site.

To see events that have been created, choose **Setup > Alarms > Actions**. See Table C-5 for descriptions of the fields on the Alarm Configuration window.

To configure alarm actions, see Configuring Alarm Actions, page 7-29.

Understanding Trigger Capture

This section describes how to use a trigger capture to start a capture session based on the alarm parameters you set. For example, you can set alarm parameters on various thresholds to start a capture session which can be used to investigate some kind of questionable network activity.

You must set your alarm threshold parameters so that Prime NAM has defined rising or falling numbers that will cause an action, or trigger, to start a capture session. You can also use the stop-and-save option. The actions are defined below:

- Trigger Capture **Start**—An alarm condition occurs based on threshold parameters you have set; the capture session starts automatically.
- Trigger Capture **Stop**: An alarm condition occurs based on the threshold parameters you have set; the capture session stops automatically.
- Trigger Capture **Stop Capture and Save to File**—An alarm condition occurs, stopping the capture session. If the captured packet data is in memory, it is saved to a file. The buffer memory is then clear to wait for next alarm event.

When an event occurs that you have defined as an alarm threshold, NAM stops any existing capture session and saves the captured packets from memory into a file. The capture session then restarts. NAM can save up to five files, depending on your local hard disk storage.

NAM monitors for threshold parameters every minute. For real-time data, the default is 5 minutes.

Defining Thresholds

Prime NAM can inspect incoming performance records and apply a configured set of thresholds to the most recent interval of data. Using thresholds allows you to target specific network traffic issues and set up notifications that are triggered when certain thresholds are crossed. For example:

- if a server's CPU load exceeds 90%
- if a device or the whole network uses more bandwidth than usual, or
- if the remaining file size on a disk drive is less than 15% or 100 MB.

In general, you should set thresholds so that only severe traffic problems that impact quality of service generate events. These critical events are intended to provide actionable notification of problems to network operators. When setting thresholds try to identify a traffic level that will have a noticeable effect

on network service levels. Set a duration that corresponds to an unacceptable period of poor service. The goal is to generate very few, significant events indicating severe problems that require immediate attention. Thresholds are not intended as a reporting tool to generate statistical information about network traffic.

To set up alarm thresholds for variables with values that trigger alarms, see Viewing Alarm Actions, page 7-31.

Note You could receive two alarms for the same occurrence if both the source and the destination are in the same site.

You can also decide whether you want to be notified **if the threshold is being crossed just once**, or whether you only want an alarm to be triggered if this state p**ersists for a certain time**. This helps you to ensure an effective network monitoring system, which will not bombard you with unnecessary notifications.

Prime NAM Threshold Alarms window (**Setup > Alarms > Thresholds**) displays thresholds you have configured. If you hover over the arrow next to the threshold Name a detailed view of the selected threshold displays.

For descriptions of the fields on the Threshold window, see Table C-6.

You can set up alarm thresholds by defining threshold conditions for monitored variables on the NAM.

You can configure the following thresholds:

- Setting Host Thresholds, page 7-32
- Setting Conversation Thresholds, page 7-33
- Setting Application Thresholds, page 7-33
- Setting Response Time Thresholds, page 7-34
- Setting DSCP Thresholds, page 7-34
- Setting RTP Stream Thresholds, page 7-34
- Setting Voice Signaling Thresholds, page 7-35
- Setting NetFlow Interface Thresholds, page 7-36

Related Topics

- Configuring Alarm Actions, page 7-29
- Viewing Alarm Actions, page 7-31

Setting Host Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **Host** tab.

Step 3 The Host Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-7 describes the fields available on this window.

Note If you leave a selection blank, it means that the parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting Conversation Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **Conversation** tab.

Step 3 The Conversation Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-8 describes the fields available in this window.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting Application Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **Application** tab.

Step 3 The Application Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-9 describes the fields available in this window.

Note If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting Response Time Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **Response Time** tab.

Step 3 The Response Time Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-10 describes the fields available in this window.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting DSCP Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **DSCP** tab.

Step 3 The DSCP Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-11 describes the fields available in this window.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting RTP Stream Thresholds

Prime NAM sends syslog, trap, e-mail, and trigger captures for RTP streams that violate stream statistics thresholds on the following metrics:

- Number of Consecutive Packet Loss

  Each RTP packet has an RTP header that contains a sequence number. The sequence number increments by one for each RTP packet received in the same RTP stream. A gap in the sequence numbers identifies a packet loss. If the gap in sequence numbers jump is more than the threshold, the software raises an alarm condition.

- Packet Loss percent

  There are two types of percent packet loss percent: Adjusted Packet Loss and Actual Packet Loss. Actual Packet Loss indicates expected packets that never appear in **Prime NAM**. Adjusted Packet Loss includes actual packets lost and packets that arrive with large delay beyond the expected buffer capacity of the endpoint.
- Jitter: Packets delay compare to the expected receiving time
- Concealment Seconds: Seconds in which there is one or more packets lost
- Severe Concealment Seconds: Seconds in which there is more than 5% of packet lost

To set thresholds for RTP streams:

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **RTP Streams** tab.

Step 3 The RTP Stream Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-12 describes the fields available in this window.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting Voice Signaling Thresholds

You can set up software to monitor voice call quality. When Cisco Unified Communication Manager's call detail records option is enabled, Cisco IP phones, both SCCP and SIP, will report the call's jitter and packet loss at the end of the call. Prime NAM intercepts this information and raises an alarm when the alarm condition crosses the rising threshold.

To set up a voice signaling threshold:

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose **Voice Signaling** tab.

Step 3 The Voice Signaling Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table C-13 describes the fields available under the Voice Signaling Metrics drop-down menu.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the voice signaling thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit.**

Setting NetFlow Interface Thresholds

Step 1 Choose **Setup > Alarms > Thresholds**.

Step 2 Click **Create** and choose the **NDE Interface** tab.

The NDE Interface Alarm Threshold Configuration window displays. The fields are described in Table C-14.

Note If you leave a selection blank, it means that that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

Step 3 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Editing or Deleting an Alarm Threshold

You can edit alarm thresholds on an as-needed basis. You can delete thresholds when you no longer need them. Any changes take effect immediately.

To edit or delete an alarm threshold:

Step 1 Choose **Setup > Alarms > Thresholds**.

The Thresholds table displays.

Step 2 Select the alarm, then click **Edit** or **Delete**.

Step 3 Depending on your selection:

- If you selected to edit, the dialog box displays for the type of alarm; for example, **Host Threshold**. Make the necessary changes. Then
  - click **Submit** to save your changes
  - click **Reset** to reset the thresholds to the values set before you edited them, or
  - click **Cancel** to cancel the edit and return to the previous page.
- If you selected to delete, click **OK** to confirm deletion, or click **Cancel** to leave the configuration unchanged.

Scheduling Data Report Exports

You can use Prime NAM to schedule data collection over a period of time for trend analysis and troubleshooting activities and then export the reports to be viewed at your convenience. For example, if you see a spike in application response time on a certain day or time you can set up a scheduled report. The report exports collected data from a specific range of time so that you have a snapshot of what might be causing issues.

You can set up scheduled jobs that will generate a daily report at a specified time, in a specified interval, and e-mail it to a specified e-mail address or addresses.

You can also obtain a report immediately by clicking the **Preview** button, rather than wait for the scheduled time. This report can also be sent after you preview it.

Tip Prime NAM displays time in this report based on the browser that initiated the report. So if your browser is in San Jose, CA, the time zone displayed in the report is based on the time zone of that machine. The data is not based on the Cisco NAM server time if the two machines are not synchronized. To synchronize your time, see Synchronizing Your System Time, page 5-5.

This section covers the following topics:

Creating a Scheduled Report Export

Scheduled export of data reports is a convenient way to collect traffic of interest in Prime NAM. We strongly recommend you to define your data report time range first and then set your export time right after your report end time. This is the most straight-forward way to use this feature.

To set up a scheduled report and export it to an e-mail address or addresses:

Step 1 From any Monitor or Analyze window, click **Export** in the Interactive Report pane to select your export preferences. If you want the report to contain filtered data, enter the filters before selecting **Export**.

Step 2 Choose the Report Time by selecting a time range for the interval of time you want data measured. The time range is limited to a 24 hour period. Any time range that includes midnight will have a *from* time larger than *to* time.

Step 3 Choose the Export Time (which is the day of the week on which to generate the weekly report and hour that report will be sent). Multiple days are supported. You can also specify what time to start the export.

The actual data time range used to generate the report for export is always the last available and complete time span specified in the Report Time step above. Prime NAM does not generate reports using data in any future time. For example:

Export Time	Report Time	Data Reported and Exported
If Every Day and Hour is 09:00	07:00 to 08:00	07:00 to 08:00 the same day (recommended use case)
If Monday and Friday and Hour is 03:00	05:00 to 05:59	Sunday and Thursday 05:00 to 05:59
If Every Day and Hour is 00:00	18:00 to 01:00	Previous day from 18:00 to 01:00

Tip Set your Export Time to occur right after the end of Report Time. This gives you the most recent data and is the easiest way to use this feature.

Step 4 Enter the e-mail address to which you would like the report delivered.

Step 5 Choose the delivery option (CSV or PDF).

Step 6 Enter the Report Name and Report Description, which appear at the end of the report delivered to you.

Step 7 Click:

- **Submit** to submit the request for the scheduled job.
- **Preview** to generate the report immediately.

Note Remember that report results are based on the local time of the browser that initiated the report.

Editing a Scheduled Export Job

Step 1 Choose **Setup > Data Export > Scheduled Exports**.

Step 2 Click the job you want to edit.

Step 3 Click **Edit**.

Step 4 Modify the information as desired.

Step 5 Click **Submit** to submit the request for the scheduled job.

Deleting a Scheduled Export Job

Step 1 Choose **Setup > Data Export > Scheduled Exports**.

Step 2 Click the job you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** to confirm, or click **Cancel** to return to the previous window without deleting the job.

Accessing Device Interface and Health Details

You can enable your NAM to access interface and health device details if they are available on the device you identify using the Prime NAM Managed Device feature.

This section contains the following topics:

Understanding How Platform-Specific NAMs Handle Managed Device Data

A managed device can represent a router or switch being monitored by Prime NAM. Depending on your Cisco NAM platform, the managed device is accessed by the NAM differently and may support different MIBs based on the device support.

The following details list how NAM accesses the managed device:

- For a physical or virtual blade or service module, the managed device is the device in which NAM software or hardware is located. The managed device information is automatically updated without user intervention and cannot be modified on the NAM. One of the benefits of having a blade or service module is that there is no configuration required for this feature.
- For a physical appliance, you identify the managed device as a switch or router that shares its traffic using SPAN or user credentials. You must enter the device address and either the SNMP credentials or NetConf credentials to configure the NAM SPAN session on the managed device. On certain platforms, NetConf is an alternative for NAM to configure a NAM SPAN session on a managed device which does not support configuring NAM SPAN sessions using SNMP. If you choose to use NetConf, you must enable NetConf on the managed device interface and enable SSH to support the SPAN session. This enables you to monitor managed device information such as interface statistics.
- All supported NAM platforms, except NAM-NX1 and vNAM, require *if-mib* (ifTable) to provide the managed device interface data. NAM-NX1 gets this data by exchanging messaging with the Supervisor card (SUP) on the EOBC channel. SPAN session configuration from a managed device is not allowed on Cisco Prime vNAMs.
- All supported NAM platforms, except for NAM-NX1, vNAM, and NAM appliance platforms, require *entity-mib* and *if-mib* to get and configure SPAN sessions. NAM-NX1 uses EOBC and proprietary messages with SUP on EOBC to get and configure SPAN sessions. Appliances have two options to get and configure SPAN sessions: SNMP (which use the MIBs required by the other NAM platforms) or NetConf interface (which require no MIBs). SPAN session configuration from a managed device is not allowed on Cisco Prime vNAMs.

To see a list of the available platforms and supported devices, see the *NAM Compatibility Matrix*. For MIB support, see Table C-63 on page C-43.

Configuring Managed Device Information

The managed device information that is required is dependent on your platform device type. For details, see Understanding How Platform-Specific NAMs Handle Managed Device Data, page 7-39.

For details on how to ensure NAM is managing your device interface and other traffic, see:

- Configuring Managed Device Information on Blades or Modules, page 7-40
- Configuring Managed Device Information on Appliances and other Virtual Platforms, page 7-40

Configuring Managed Device Information on Blades or Modules

You are not required to configure NAM blades or modules on the NAM side.

Note NAM-3 platform requires SNMP MIBS (SNMPv3 is not required). SNMP requests and responses are communicated over an internal interface within the chassis and SNMPv3 is not used. NAM-NX1 requires some SNMP MIBs.

Ensure you follow the configuration instructions in your platform documentation so that your managed device communicates network traffic to NAM.

Once NAM automatically updates your managed device details, you can view that information using **Setup > Managed Device > Device Information**. For details, see Viewing Managed Device Information, page 7-41.

For details about how NAM treats managed devices, see Accessing Device Interface and Health Details, page 7-39.

Configuring Managed Device Information on Appliances and other Virtual Platforms

For appliances and some virtual NAM platforms, you must set up your managed device using the NAM **Setup > Managed Device > Device Information** window. Enter your device address and credentials to allow NAM SPAN session configuration. You will need to configure SNMP credentials to receive details about managed device interface statistics. You may need to configure NetConf credentials to enable a NAM SPAN session to and from the managed device. To use NetConf, your managed device must support the NetConf interface and have SSH enabled. You can use NetConf as an alternative to configuring a NAM SPAN session on your managed device if your device does not support configuring NAM SPAN sessions via SNMP.

Note This section applies to all Cisco NAM platforms *except* the NAM-NX1 and NAM-3 blades. SPAN session configuration via managed device is not allowed on vNAMs.

To set your managed device parameters:

Step 1 Choose **Setup > Managed Device > Device Information**.

Depending on your managed device, either the Router System Information displays as show in Table C-15 or the Switch System Information displays as shown in Table C-16.

Step 2 Click **Test Connectivity** to perform an SNMP test. Click **Close** when finished.

Step 3 Click **Submit** to submit the information and close the window.

Viewing Managed Device Information

To view the switch information, choose **Setup > Managed Device > Device Information**.

Depending on your platform, the System Information may display some or all of the fields shown in Table C-15 or Table C-16.

Configuring Network Parameters

This section describes how to set up the network parameters including:

- Configuring Sites, page 7-41
- Setting Interface Speed using NetFlow Interface Capacity, page 7-44
- Configuring DSCP Groups, page 7-45

Configuring Sites

Cisco Prime Network Analysis Module makes it easier to monitor traffic and identify issues across your network by providing a way to manage large campuses using different views of your network, referred to as *sites*.

A *site* is a collection of hosts (network endpoints) partitioned into views. You can limit the view of your network analysis data to a specific city, a specific building, or even a specific floor of a building, and can use sites to focus collection and analysis of data. Sites are optional, but recommended.

See the following sections to set up sites:

- Defining a Site, page 7-41
- Viewing Defined Sites, page 7-42
- Configuring Sites Using Subnets, page 7-43

Defining a Site

A site can be defined as a set of subnets specified by an address prefix and mask, or using other criteria such as a remote device data source (for example, remote WAE device and segment information).

Configuring Sites Using Subnets, page 7-43 gives specific information about various scenarios.

To set up a site or sites:

Step 1 Choose **Setup > Network > Sites** and click **Create**.

Step 2 The Site Configuration window appears. Enter a Name, Description, Subnet, and Data Source as appropriate.

See Table C-18 for field descriptions.

Step 3 Enter the subnet and data source, then click **Detect** to tell the software to look for subnets in the traffic. See Detecting Site Subnets, page 7-42.

Step 4 Click **Submit**.

Note The "Unassigned" site (with a description of "Unclassified hosts") includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.

Detecting Site Subnets

When you click the **Detect** button at **Setup > Network > Sites > Sites Configuration**, Prime NAM looks for subnets detected within in the past hour. See Table C-19 for information about the fields.

When you click **Detect**, Prime NAM finds those subnets that meet the criteria that you entered.

Viewing Defined Sites

To view already-defined sites:

Step 1 Choose **Setup > Network > Sites**.

Step 2 The Sites window appears. Defined sites will be listed in the table.

The fields are described in Table C-20.

Editing a Site

You can edit sites that have been created. The Unassigned site cannot be edited or deleted.

Step 1 Choose **Setup > Network > Sites**.

Step 2 Highlight the site that you have configured.

Step 3 Click **Edit** and edit the desired field.

The fields are described in Table C-20.

Step 4 Click **Submit** to save the changes, or click **Reset** and **OK** to reinstate the site's previous settings, or click **Cancel** to cancel any changes and return to the main Sites page.

Configuring Sites Using Subnets

The site definition is very flexible and can accommodate various scenarios. Prime NAM uses the site definition not only for viewing of data, but for data export and data retention as well. The same rule cannot be defined in multiple sites. That is why the preferred way is to define a site using its subnets. See Table 7-4 for examples of site definitions.

Note VLAN option is removed from the Site definition.

For details on how Prime NAM resolves overlapping IP addresses, see Resolving Ambiguity (Overlapping Site Definitions), page 7-44

Table 7-4 Site Definition Details

Site Definition	Example	Notes
Subnet (IP address prefix)	*Site Data-Center = subnet 172.20.0.0/16*	Preferred. Normally, subnets alone are sufficient to define a site.
Overlapping IP addresses (subnet from data source)	*Site NewYork = subnet 10.11.0.0/16* from *"NetFlow-NewYork"* data source. *Site LosAngeles = subnet 10.11.0.0/16* from *"NetFlow-LosAngeles"* data source. *Site Sale-Dept = subnet 10.11.0.0/16* from *"DATA PORT 1"* data source. *Site Finance-Dept = subnet 10.11.0.0/16* from *"DATA PORT 1"* data source.	In certain scenarios when there are overlapping IP address spaces in the networks (for example, in private networks where hosts from different sites have the same IP addresses), then data sources can be used to differentiate the subnets.
WAE device serving the site	For WAAS traffic, you can define a site associated with a WAE device without specifying the site's subnets. Simply select all of the WAAS data sources coming from the WAE device(s) serving that site. *Site SanJose = WAE-SJ-Client, WAE-SJ-CltWAN, and WAE-SJ-Passthrough data sources.*	We recommend that you use subnets to specify WAAS-optimized sites. Use this method only if the site's subnets cannot be determined. If you are configuring a WAAS device, you will need to add WAAS servers to Prime NAM. See Auto Create of New WAAS Devices, page 7-27.

Table 7-4 Site Definition Details

Site Definition	Example	Notes
Multiple Rules	You can define a site using a combination of multiple rules described in this table. For example, if a site has both optimized and non-optimized traffic, it can be defined using a combination of WAAS data sources and a subnet from a NetFlow data source.	When defining a site using multiple data sources, be careful to make sure that those data sources do not have duplicated traffic to avoid double counting the site traffic statistics.
Unassigned site	The Unassigned site includes hosts that do not match any of your site configurations. Sites are classified at the time of packet processing.	Cannot be edited or deleted.

Resolving Ambiguity (Overlapping Site Definitions)

Conflicting rules are not allowed in site definitions. Of the following two scenarios, the second one is not allowed.

1.2.3.0/24 from DATASOURCE1 = SiteA

1.2.3.0/24 from DATASOURCE1 = SiteB

Using a prefix is the preferred method. Data source is secondary. In the following two scenarios, the first would receive the higher priority.

1.2.3.0/24 = Site D

WAE1-Client datasrc = Site E

The longest prefix has higher priority (same data source). In the following two scenarios, the first would receive the higher priority.

1.2.3.0/24 from DATASOURCE1 = Site A

1.2.0.0/16 from DATASOURCE1 = Site C

The more refined (specific) rule has higher priority. In the following two scenarios, the first would receive the higher priority.

1.2.3.0/24 from DATASOURCE1 = Site A

1.2.3.0/24 (any datasrc) = Site D

Setting Interface Speed using NetFlow Interface Capacity

After you have set up NetFlow data sources (see Forwarding NetFlow Traffic, page 7-14), you can go to the NDE Interface Capacity window at **Setup > Network > NDE Interface Capacity** to specify the speed of each interface. This allows the software to calculate interface utilization on the NDE Interface Traffic Analysis window (**Analyze > Traffic > NDE Interface**). Otherwise, the Prime NAM software can only display the throughput of the interface, but cannot show its utilization.

The interface name and speed will be automatically discovered by the Prime NAM if you configure the device SNMP credentials in **Setup > NAM Data Sources > Create > Type: NETFLOW**.

To add a new or edit an existing interface, continue to Creating or Editing a NetFlow Interface, page 7-45.

Creating or Editing a NetFlow Interface

To add a new interface if it has not been automatically discovered, at the NetFlow Data Export (NetFlow) Interface Capacity window (**Setup > Network > NDE Interface Capacity**), click **Add**. Then fill in the fields as described in Table C-21.

Note It is normally not necessary to manually create NetFlow interfaces. They should be discovered automatically when the device sends NetFlow packets to the NAM.

To edit an existing interface, choose the device, then click **Edit**. Fill in the fields as described in Table C-21.

Configuring DSCP Groups

Differentiated services monitoring (DiffServ) is designed to monitor the network traffic usage of Differentiated Services Code Point (DSCP) values. To monitor DSCP, you must configure at least one aggregation profile, and one aggregation groups associated with each profile. This section describes how to set up the DSCP groups.

You can define two or three different groups of traffic, and assign the various DSCP values to each group. Or you can assign one particular value for the first group and give it a name, and then assign all the rest to the other (or default) group and give that a name.

For detailed information about setting DSCP values, see *Implementing Quality of Service Policies with DSCP*:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

The following tasks help you set up and manage the DSCP groups:

- Creating a DSCP Group, page 7-45
- Editing a DSCP Group, page 7-46
- Deleting a DSCP Group, page 7-46

Creating a DSCP Group

To create a DSCP Group:

Step 1 Choose **Setup > Network > DSCP Groups**.

The DSCP Groups table displays.

Step 2 Click **Create**.

The DSCP Group Configuration window displays.

Step 3 Fill in the fields as described in Table C-22.

Table C-23 shows the available formats and associated values.

Step 4 Click **Submit** to save your changes.

Editing a DSCP Group

To edit a DSCP group:

Step 1 Choose **Setup > Network > DSCP Groups**.

The DSCP groups window displays.

Step 2 Select the profile to edit, then click **Edit**.

Step 3 Make the necessary changes, then click **Submit** to save your changes, or click **Reset** to cancel.

Deleting a DSCP Group

To delete a DSCP group, select the profile from the DSCP Groups table, then click **Delete**.

Configuring Application Classification

Prime NAM provides two ways of enhancing how your traffic is displayed in the dashboard and reports. Prime NAM uses application classification to:

- Expand the number of application's for which Prime NAM can provide down to Layer 7 application details. See Adding More Detail into Dashboard and Application Reports.
- Create custom applications using a list of rules based on HTTP URL or Server /Port definition. This is referred to as the *classic* application classification model. See Creating Deeper Visibility Into Application Traffic, page 7-48.

You can use one or both of these methods to ensure Prime NAM provides the level of traffic detail you need.

Adding More Detail into Dashboard and Application Reports

You can add more detail enable deep packet inspection to see Layer 7 application visibility by using application classification. To understand more about application classification and Layer 7 application visibility, see About Deeper Application Classification.

In order to enable application classification for deep packet inspection in Prime NAM:

Step 1 Choose **Setup > Classification > Applications Settings**. Then select the Deep Packet Inspection checkbox in order to enable your Prime NAM dashboards to display key critical details, such as hostname and port, in your traffic captures and reports.

Step 2 If necessary, select **New** in the Protocol Pack pane to download the latest NBAR2 Protocol Pack (PP). Prime NAM stores the default plus one additional PP.

You can download PP files under the **Cisco Prime Network Analysis Module** product links at the CCO software download location at following URL:

http://software.cisco.com/download/navigator.html

Timesaver Use **Downloads Home >Products > Cloud and Systems Management > Network Analysis Module (NAM) Products > Cisco Prime Network Analysis Module Software** to locate the protocol pack.

Step 3 To revert back to the default protocol when a previous protocol pack is no longer needed, choose **Restore Default**.

About Deeper Application Classification

This release of Prime NAM supports a more comprehensive, or deeper, application classification method. This method allows you to see more details in your monitoring dashboards and packet captures (including application names, interface details, and so on).

To expand the level of application information your Prime NAM can monitor and analyze, enable the deeper level of application classification and download application signature updates when you need them.

In addition to providing the application name, this method also brings attributes to simplify application management for both classification and reporting. Application categorization, for example, allows the grouping of similar applications.

When this method is enabled you can view extracted information from applications such as HTTP URL, HTTP User Agent, and SIP URL, for export or classification.

Note Depending on your installation or upgrade method you may need to enable deep packet inspection.

You can use protocol packs to add new and update existing application signatures. NAM support of protocol packs allows you to see any new and updated application signatures in Prime NAM traffic monitoring. For more details on Protocols Packs, see About Protocol Packs and Application Classification, page 7-47.

You can also use the Prime NAM CLI to change the classification status to use the deeper application classification method and check which classification setting your NAM is using.

For details about what application signatures are in specific protocol pack versions, see Network-Based Application Recognition Q&A on Cisco.com.

For details on enabling deep application classification and updating protocol packs using the CLI, see the *Cisco Prime Network Analysis Module Command Reference Guide*.

About Protocol Packs and Application Classification

Prime NAM uses Cisco's Network-Based Application Recognition to recognize and classify a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments. The support of Protocol Packs (PP) allow you to update your application signatures so that dashboard and traffic data provide the most detailed information available. Prime NAM Protocol Packs can be found in the CCO software download location. These are the only protocol packs you should use with Prime NAM.

You do not need a license to download a protocol pack for Prime NAM. For this release, updating the protocol pack may cause a temporary interruption of operation for several seconds, similar to changing the system time.

To view the Prime NAM Protocol Pack version, choose **Setup > Classification > Applications Settings**.

To turn on deep application classification in Prime NAM, choose **Setup > Classification > Applications Settings** and select **Deep Packet Inspection**. For details, see Adding More Detail into Dashboard and Application Reports, page 7-46.

If you choose not to use the deep application classification method, Prime NAM defaults to a less comprehensive classification method that may not include all applications or protocols.

About NAM Classic Deep Packet Application Classification

This section covers how you can customize your Prime NAM to provide a deeper level of visibility into the application data presented in the dashboard and reports.

Prime NAM uses the application ID classification system. When defining applications, you can view and select from a list of protocols and port numbers, and candidate IP addresses and port numbers for the traffic being analyzed. You can also create URL-based application classifications. For an in depth overview of application types, see Understanding Application Traffic, page 7-50.

You can also configure custom applications using the Application Programming Interface (API), also referred to as the North Bound Interface (NBI). This is needed to ensure uniform application classification across a number of NAMs. See your customer service representative for details on how to get access to the NBI documentation.

To set up classifications use the following tasks:

- Creating Deeper Visibility Into Application Traffic, page 7-48
- Configuring Application Groups, page 7-52
- Filtering Encapsulations, page 7-53

Creating Deeper Visibility Into Application Traffic

This section provides details into the application classification method known as Network Based Application Recognition (NBAR) classic.

You can use Prime NAM to monitor pre-determined or custom applications in your Data Center so that your traffic analysis is more focused and therefore optimal.

Without configuring application classification, applications running on a certain servers or specific ports are classified as *unknown*. This means that you may not have enough insight into the monitoring traffic. After configuring your application or ports, you can gain visibility into those application details on the monitoring screens. Similarly for the URL-based applications, instead of having all web traffic being grouped under the HTTP URL, you can specify a more granular layer of monitoring by using the application and port.

This section describes the following tasks:

- Creating Custom Applications, page 7-49
- Editing Custom Application Classifications, page 7-50
- Adding More Detail into Dashboard and Application Reports, page 7-46
- Deleting an Application Rule, page 7-50
- Understanding Application Traffic, page 7-50

To find out more about Layer 7 visibility and deep packet inspection, see Adding More Detail into Dashboard and Application Reports, page 7-46.

Creating Custom Applications

You can create a custom applications using the list of rules based on HTTP URL, Protocol, or Server IP addresses. If you create a custom application, you can later edit it if you choose. Standard, pre-defined applications cannot be edited.

For details on application types or other options, see Understanding Application Traffic, page 7-50.

To create a new application classification:

Step 1 Choose **Setup** > **Classification** > **Applications** and select **Create**..

For a description of the Applications window, see Table C-25.

Step 2 Enter an application classification name.

Step 3 (Optional) Enter an application description that gets displayed in the view table. There is a 75 character limit.

Step 4 (Optional) You can skip the Selector value. This is an arbitrary number, unique within an engine-id. It will be automatically assigned if left blank.

Step 5 Select the application classification rule type drop-down menu.

a. To choose a Server/Port application rule, select **Server/Port** in the Application Classification Rule drop-down menu.

   Then select the definition drop-down menu to enter the following required information.

   - To choose a Server, Protocol, and Port or Port Range, select the drop-down menu then enter the required information.
   - To choose a protocol, select **Any**, **TCP**, **UDP**, or **Both TCP & UDP**.
   - To choose a port or port range, enter the required information.

b. To choose the URL-based application rule, select **HTTP URL** in the Application Classification Rule drop-down menu then enter the required information. (See Understanding URL-Based Application Classification, page 7-51 for additional field details.)

Tip You can also add or remove multiple rule definitions to this application classification by clicking the gear icon and selecting **Insert new rule** or **Delete**.

Step 6 Click **Submit** to create the new application classification signature.

You can now monitor the new applications using the Interactive Report filter with the application dashboards.

Editing Custom Application Classifications

In Prime NAM you can only modify the custom, or user-defined, applications, and not the preconfigured system applications. You can only edit an application for which it states *Custom* in the Engine ID column.

To edit an application:

Step 1 Choose **Setup > Classification > Applications**.

Step 2 Select the application to edit, and click **Edit**.

The Application configuration window displays.

Step 3 Make the desired changes.

Step 4 Do one of the following:

- To accept the changes, click **Submit**.
- To leave the configuration unchanged, click **Cancel**.
- To delete the application rule, click **Delete**.

Deleting an Application Rule

You may want to delete an application rule when you are no longer using it in your network.

To delete an application rule, simply select it from the Application list, then click **Delete**.

You cannot delete preconfigured system applications, only custom applications.

Understanding Application Traffic

This section contains information on application types, rules, and other details you may find helpful.

There are two types of application classification rules:

1. *Server/Port* rules defines a a server IP address. For server-based application classification, Prime NAM analyzes traffic for the candidate IP addresses and port number or numbers you specify. You can also define port or protocol-based application (for example, based on a TCP port). You can create additional ports to enable Prime NAM to handle additional traffic for standard applications. Port ranges for IP are 1-255 for IP. TCP and UDP port ranges are1-65535.
2. *HTTP-based URL* rules define URL-based application extensions to the existing list of supported applications. When the URL in an HTTP request matches the criteria of a URL-based application, the traffic is classified as that protocol. The HTTP request is a URL on any port that is part of the iana-l4:http protocol, or protocol named http under the *iana-l4* engine ID.

Tip To create Protocol or Server IP Address applications, you can check the Application Configuration table in **Analyze > Traffic > Application**. To create an HTTP URL-based application, you can analyze the incoming URLs on **Analyze > Traffic > URL Hits**. NBAR is enabled through CLI.

Prime NAM recognizes an application based on either:

- An application which resides on a specific server IP address—You can filter using an IP address, a protocol, and a port or range of port numbers. After configuring the server information, the monitoring dashboard displays more detailed application information instead of just the *unknown* grouping.
- A set list of application IDs—The protocol, port number, or port number range, along with the focused inspection of traffic (for example, voice signaling traffic or FTP), heuristics (for example, DCE-RPC or SUN-RPC), or standardized application identifiers exported by Cisco platforms with NetFlow.

  If Prime NAM is not able to recognize an application using any of these mechanisms, the application type of the traffic is reported as ***unknown***. You can configure the application reported as unknown to create custom applications.
- A custom application based on a URL-based HTTP request—You can include URL Host, URL Path, or a Prime NAM Content Type. This allows you to gain additional visibility instead of grouping all web traffic HTTP. For details, see Understanding URL-Based Application Classification, page 7-51.

To add custom applications and view or edit any user-defined applications, choose **Setup > Classification > Applications**.

Caution There is no limit on the number of URL-based applications that can be created. It is important to consider that these types of applications use large amounts of CPU bandwidth and may impact your performance if too many are defined.

Table C-24 describes the fields on the Applications view page.

Understanding URL-Based Application Classification

URL-based applications are extensions to the list of applications. When the URL in an HTTP request (a URL on any port that is part of the iana-l4:http protocol, or protocol named *http* under the *iana-l4* engine ID) matches the criteria of a URL-based application, the traffic is classified as that protocol. The device interface statistics are collected by regularly (once a minute) polling the ifTable statistics of all interfaces on the managed device.

A URL-based application can be used the same way as any other application. For example, a URL-based application can be used in collections, captures, and reports.

An incoming URL is matched against the criteria of the configured URL-based applications in the order of the selector in ascending order. When a match is found, the remaining URL-based applications are not considered.

A URL consists of the following parts:

- a host (host.domain.com)
- a path (dir_nam/dir_name)
- an argument/content type

Tip Content-type argument should rarely be used in combination with the other two fields. It can be used alone, for example to identify WAP traffic you could define an application with a content type of **wap.**. In almost all other cases, we recommend you use host and path only.

Example—Creating an URL-Based Application

This example provides steps on how to create a URL to allow you to control the displayed traffic data. For example, the URL *www.cisco.com/go/nam* are broken down when sent to the web server into two fields: a host field (*www.cisco.com*) and a path field (*/go/nam*). By defining different values for the fields in the application, you can control the granularity of URLs that are classified as this new application. If you want to group all traffic to *www.cisco.com* together and only define the host part, then use the host only part. If you have multiple hosts that map to the same end resource and only want to define the path part., then use only the path entry (*go/nam*).

To collect traffic for a particular host and path for the URL **http://cisco.com/go/nam** enter:

- the *host* part is **host.domain.com**, for example, **Cisco.com**
- the *path* part is **/go/nam**
- the *argument* part is **null/empty**

In the configuration of an URL-based application, the path part and the argument path are combined and called the *path part*. For detailed descriptions, see Table C-29.

Note The host, path, and argument parts of a URL are matched against the corresponding POSIX regular expressions specified in the application definition. For details on regular expression syntax, refer to the IEEE Std.

Configuring Application Groups

An application group is a set of applications that can be monitored as a whole. The following topics help you set up and manage the application group:

- Creating an Application Group, page 7-52
- Editing or Deleting an Application Group, page 7-53
- Deleting an Application Group, page 7-53

Creating an Application Group

To create an application group:

Step 1 Choose **Setup >Classification > Application Groups**.

The Application Groups window displays.

Step 2 Click **Create** and enter the name in the Application Group Name field.

Step 3 Use the next Application field and the **Filter** button to narrow the list of selectable applications. For example, if you enter *bittorrent*, all applications with that name appear in the list below.

Step 4 Select an application and click **Add**. Applications appear in the Selected Applications box.

You can select multiple applications at once by using the Shift button, and then click **Add.**

Step 5 Click **Submit** to save your changes.

Editing or Deleting an Application Group

To edit or delete an application group:

Step 1 Choose **Setup > Classification > Application Groups**.

Step 2 Select the Application Group by clicking the radio button, then click **Edit** or **Delete**.

Note You can only delete one application group at a time.

Deleting an Application Group

To delete an application group, simply select the application and then click the **Delete** button.

Filtering Encapsulations

Using encapsulation gives you increased flexibility when trying to view different types of application traffic (such as counting or grouping). The encapsulation settings affect how traffic of certain IP-based tunneling protocols are treated.

You can use this software to set up the way you want to view different types of encapsulations in network traffic for the following protocols:

- CAPWAP Data—Control And Provisioning of Wireless Access Points
- ERSPAN—Encapsulated Remote Switched Port Analyzer
- FabricPath
- GRE—IP over GRE tunneling (Generic Routing Encapsulation)
- GTP—GPRS (General Packet Radio Service) Tunneling Protocol
- IP.IP4—IP4 over IP4/IP6
- IP.IP6—IP6 over IP6
- IPESP—IP with Encapsulating Security Payload
- L2TP Data—Layer 2 Tunneling Protocol
- LISP Data—Locator/ID Separation Protocol
- LWAP Data—Lightweight Access Point Protocol
- MPLS—Multiprotocol Label Switching
- OTV—Overlay Transport Virtualization
- PPPoE—Point to Point Protocol over Ethernet
- Segment ID—Rule to match one or more fields with a regular expression.
- SGT—Security Group Tag

- VNTAG—Virtual Network Tag
- VxLAN—Virtual Extensible LAN

To filter encapsulations:

Step 1 Select **Analyze > Traffic > Encapsulation**.

Step 2 From the Interactive Report pane, click **Filter** to display the filter options,

Step 3 Use the available options to select filtering for the encapsulation traffic reports. Unavailable options will be grayed out.

Step 4 Enter whether you want to include filtering on the site and specify the data source.

Step 5 Select encapsulation options to filter on including the time range.

Step 6 If you add a filter name, the filter is saved below the Interactive Report pane for reuse.

Step 7 Click **Submit** to run the filter and update the Encapsulation Traffic graphs and Top N dashboards based on your filter settings.

If you want to revert to the previous settings since your last submission, click **Reset**.

Setting Up Prime NAM Monitoring

This section discusses how to set up monitoring over and above the default monitoring parameters. You can customize these monitoring parameters.

To set up Prime NAM monitoring perform these tasks:

- Setting Aggregation Intervals, page 7-54
- Configuring Response Time, page 7-56
- Setting Up Voice Monitoring, page 7-56
- Creating RTP Filters, page 7-57
- Configuring URL Collections, page 7-57
- Configuring WAAS Monitored Servers, page 7-59

Setting Aggregation Intervals

Prime NAM has short-term and long-term aggregation intervals (this was referred to as long-term reporting in earlier NAM releases). Aggregated data is displayed in the dashboards if the query is longer than one day.

The purpose of gathering short term aggregation interval data is for troubleshooting. It has a finer granularity than long term data (by default, the short term aggregation interval for Traffic/Media is one minute, and short term response time interval is five minutes).

The purpose of gathering long term interval data is for trending analysis. The smallest aggregation interval for long term data is one hour (60 minutes).

Caution If you modify the aggregation intervals, existing collected data that is not in the same aggregation interval will be completely removed. Data will then start being collected from the beginning again at the moment the intervals are modified and applied.

Traffic and Media refer to applications, hosts, RTP streams, and voice calls monitoring. Response Time refers only to application response time. Prime NAM does not support long term aggregations of data for the following media: conversations, RTP streams, and voice signaling calls monitoring.

To set up aggregation intervals:

Step 1 Choose **Setup > Monitoring > Aggregation Intervals**.

Step 2 Choose the desired durations for Short Term Interval and Long Term Interval.

Step 3 Check the **Collect only hosts from user-defined sites (exclude hosts from Unassigned site)** check box if you want the Prime NAM long term data to contain information only for hosts classified to the user-defined sites. This check box only applies to the long term data; short term always collects all hosts.

Note Enabling the "Collect only hosts from user-define sites" option can significantly speed up report queries, because it excludes unclassified hosts' statistics from the database.

When you first start the NAM, in monitoring windows that show site information, you will see a site named "Unassigned" and with a description of "Unclassified Hosts." The Unassigned site includes any that do not match the site configurations. By default, long-term storage will include data for all sites, including the Unassigned site. In some cases, you may not want to view long term data of hosts that are not in your network, in which case you would check the check box.

Step 4 Click **Submit**.

The aggregation intervals determine how much data can be stored in the Prime NAM database. See Table 7-5 for information about short and long-term data retention. This calculation is based on a worst case scenario where tables are full or almost full. It is based on recommended database sizes.

Table 7-5 Data Retention

	Short-Term Aggregated Data (Normal)	Short-Term Aggregated Data (Minimum)	Long-Term Aggregated Data (Normal)[1]	Long-Term Aggregated Data (Minimum)
All supported platforms	72 hours	14 hours	100 days (with default polling interval)	30 days (with default polling interval)

1. Can depend on how the user configures the LT polling interval. The more frequent polling, the shorter the duration.

Configuring Response Time

To configure the timing parameters for response time data collections:

Step 1 Choose **Setup > Monitoring > Response Time**.

The Response Time Configuration page displays. The settings you make on this window comprise the time distribution in microseconds for the detailed Server Application Response Time data collection.

Step 2 Check the **Enable Response Time Monitor** check box.

Step 3 After Monitored Server Filter, you will see **Disabled** or **Enabled**. If a WAAS server has been configured under **Setup > Monitoring > WAAS Servers**, you will see **Enabled**. Click **Configure Filter** to configure a filter if you need to enable your monitor server filter.

Step 4 Enter the Response Time values as described in Table C-28.

Step 5 Accept the default settings or change the settings to the values you want to monitor. Click **Submit** to save your changes.

Setting Up Voice Monitoring

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.

After you set up the software to monitor voice data, you will be able to view the collected voice data under **Analyze > Media**. For more information on viewing the voice data, see Analyzing Media, page 3-30.

Note Voice monitoring features are supported with Cisco IP telephony devices only.

To set up voice monitoring:

Step 1 Choose **Setup > Monitoring > Voice**.

The Voice Monitoring page displays.

Step 2 Check the **Enable Call Signal Monitoring** check box.

Step 3 Accept the default MOS Score value range or modify the values as you prefer. See Table C-28.

Note To report jitter and packet loss for the SCCP protocol, you must enable CDR on Cisco Unified Communications Manager. For more information on Cisco Unified Communications Manager, see the Cisco Unified Communications Manager documentation.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Step 4 Click **Submit** to save your changes, or click **Reset** to cancel and revert to the previous settings.

Creating RTP Filters

When the software is initially started, RTP stream traffic will automatically start being monitored. Prime NAM enables you to monitor all RTP stream traffic among all SPAN traffic, without having to know the signaling traffic used in negotiating the RTP channels. RTP Stream Monitoring is enabled by default under **Setup > Monitoring > RTP Filter**. To disable it, uncheck the **Enable RTP Stream Monitoring** check box and click **Submit** to apply the change.

To create an RTP filter:

Step 1 Choose **Setup > Monitoring > RTP Filter**.

Step 2 Click **Create**.

Step 3 From the drop-down menu, choose the protocol (IP or IPv6).

Step 4 Enter the Source Address, Source Mask, Destination Address, and Destination Mask.

Step 5 Click **OK**.

Configuring URL Collections

The URL collection listens to traffic on TCP port 80 of a selected data source and collects URLs. Any protocol which has its master port set to TCP port 80 can be used for URL collections. Only one collection on a single data source can be enabled at a time.

A URL, for example: ***http://host.domain.com/intro\?id=123***, consists of a host part (**host.domain.com**), a path part (**intro**), and an arguments part (**?id=123**).

Note Since the argument is matched against a regular expression, a literal *?id=123* is not a valid regular expression. The ? needs to be escaped with a backslash character, \ , so the actual regular expression needed is *\?id=123*.

The collection can be configured to collect all parts or it can configured to collect only some of the parts and ignore others.

This section contains the following procedures:

- Enabling a URL Collection
- Changing a URL Collection
- Disabling a URL Collection

Enabling a URL Collection

To enable a URL collection:

Step 1 Choose **Setup > Monitoring > URL.**

Step 2 Check the **Enable** check box to initiate URL Collection.

Note The collection will not begin until you click **Submit**.

Step 3 Provide the information described in Table C-29.

You can enter a partial name of a data source and click **Filter** to find data sources that match. Choose **Clear** to return to the entire list of data sources.

Note Depending on which radio button option is collected, the format of the URL varies. For example, the leading *http:* part is only present if the *host* part is collected. Keep this variable in mind, when configuring a *match only* expression.

Step 4 Check the **Recycle Entries** check box to recycle entries.

Step 5 Select the check box for one of the following:

- Collect complete URL (Host, Path and Arguments)—You might use this if you are a network security engineer and suspect a virus infection may be caused by a website. This information could be used to identify which web page has the virus embedded and how it may have spread. It can also be shared for further analysis to help create a solution to stop the spread.
- Collect Host only (ignore Path and Arguments)—You might use this if your network administrator changed your firewall policies to block certain hosts.
- Collect Host and Path (ignore Arguments)
- Collect Path and Arguments (ignore Host)
- Collect Path only (ignore Host and Arguments)

Step 6 Click **Submit** to save your changes, or click **Reset** to cancel.

Changing a URL Collection

To change a URL collection:

Step 1 Choose **Setup > Monitoring > URL**.

Step 2 Change the URL Collection Configuration field information as described in Table C-29.

Note Changing any parameters and applying the changes flushes the collected URLs and restarts the collection process.

Step 3 Click **Submit** to save your changes, or click **Reset** to cancel.

Disabling a URL Collection

When you disable URL collection monitoring, all collection stops immediately and any collection that was in progress is deleted.

To disable a URL collection:

Step 1 Choose **Setup** > **Monitoring > URL**.

Step 2 Uncheck the **Enable** check box.

Step 3 Click **Submit**.

Configuring WAAS Monitored Servers

WAAS monitored servers specify the servers from which WAAS devices export traffic flow data to the Prime NAM monitors. To enable WAAS monitoring, you must list the servers to be monitored by Prime NAM using the WAAS device's flow monitoring.

You must configure WAAS monitored servers to enable Prime NAM to monitor WAAS traffic. Prime NAM displays status of WAAS devices as *pending* until you set up WAAS monitored servers.

To configure a WAAS monitored server:

Step 1 Choose **Setup > Monitoring > WAAS Servers**. The WAAS Servers page displays.

Step 1 Check the **Filter Response Time for all Data Sources by Monitored Servers** check box if you want Prime NAM to compute response time data only for the servers from this list for all data sources, including non-WAAS data sources. All other servers will be ignored in response time monitoring views. This enables you to reduce Prime NAM workload and to improve its overall performance.

Step 2 Click **Add** and enter the server IP address in the Server Address field. You can paste multiple IP addresses here as well.

Tip Specify the WAAS monitored servers from which WAAS devices export traffic flow data to the Prime NAM monitors. Do ***not*** use the WAE device IP address.

Step 3 Click **Submit**.

Understanding Prime NAM Traffic Sources

Before you can monitor data using Prime NAM software, you must direct specific traffic flowing through a switch or router to the **Prime NAM**. This appendix explains the various data sources that you can configure for **Prime NAM**.

This appendix contains the following topics:

For details on supported data sources, see the *NAM Compatibility Matrix*.

Data Source Overview

Prime NAM uses various data sources to deliver its performance troubleshooting functionality:

To understand which methods to use to direct specific traffic to the **Prime NAM** software, see Table A-1.

Table A-1 Methods of Directing Traffic

Method	Usage Notes
Switch SPAN[1]	You can direct a set of physical ports, a set of VLANs, or a set of EtherChannels to the NAM. Selecting an EtherChannel as a SPAN source is the same as selecting all physical ports comprising the EtherChannel as the SPAN source. On some NAM platforms, using SPAN allows for NAM configuration without having to use the switch.Forwarding SPAN Traffic, page 7-5.
Switch Remote SPAN (RSPAN)[1]	You can monitor packet streams from remote switches, assuming that all traffic from a remote switch arrives at the local switch on a designated RSPAN VLAN. Use the RSPAN VLAN as the SPAN source for the NAM.

Table A-1 Methods of Directing Traffic (continued)

Method	Usage Notes
Encapsulated Remote Switched Port Analyzer (ERSPAN)[1]	You can monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports using ERSPAN. ERSPAN sends traffic to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different routers or switches, which provides remote monitoring of multiple routers or switches across your network. See Forwarding ERSPAN Traffic, page 7-6.
NetFlow Data Export (NDE)	Prime NAM analyzes NetFlow from Managed Devices (Routers/Switches) You can monitor NetFlow records directly from remote switches or routers. You must configure the NetFlow packet source to the NAM from a local switch or remote router using the device CLI. For received NetFlow traffic, a default site will be created including all interfaces from that device. See Configuring Sites, page 7-41. SPAN and NetFlow sources can be in effect simultaneously. See Forwarding NetFlow Traffic, page 7-14.
WAAS	You can access Prime NAM from within the Central Manager interface. Prime NAM integration with WAAS Central Manager provides for easier viewing of **Prime NAM** reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments. See Configuring WAAS Monitored Servers, page 7-59.
SNMP	Used as a southbound interface for configuration and data retrieval from switches and routers. Prime NAM uses web services as the northbound interface for data objects. The software continues to support baseline manageability features of SNMP such as MIB-2 and IF-TABLE for the NAM, and the health status and interface statistics that can be used by external products like Fault and Configuration Management offerings (for example, CiscoWorks LMS and Prime Infrastructure).
Network Tap Device	Applies to NAM appliances only. For details, see your appliance installation guide.

1.Prime NAM can analyze Ethernet VLAN traffic from the following sources: Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN, RSPAN, or ERSPAN source port.

The Data Sources page (**Setup > Traffic > NAM Data Sources**) lists the data sources configured for your NAM. Table C-2 describes the fields in the NAM Data Sources window.

Table A-2 summarizes the traffic sources that are used for Prime NAM monitoring.

Table A-2 Summary of Traffic Sources for Prime NAM Monitoring

Traffic Source	LAN		WAN	
	Ports	**VLANs**	**Ports**	**VLANs**
VACL capture	Yes	Yes	Yes	N/A
NetFlow Data Export NDE (local)	Yes	Yes	Yes	Yes
NetFlow Data Export NDE (remote)	Yes	Yes	Yes	Yes

Table A-2 Summary of Traffic Sources for Prime NAM Monitoring (continued)

Traffic Source	LAN		WAN	
	Ports	VLANs	Ports	VLANs
SPAN	Yes	Yes	No	No
ERSPAN	Yes	Yes	No	No

Ports and Hardware Details

NAM-3 and NAM-NX1 each have two dataports. Each dataport can accept one SPAN session. Depending on the managed device operating system (OS) version, the number of SPAN sessions allowed may vary. Most IOS versions support two SPAN sessions. Nexus OS may support more than two SPAN sessions.

Depending on the IOS running on the Supervisor, port names are displayed differently. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the VSS, a port name might be displayed as Gi1/2/1 to represent a Gigabit port on switch 1, module2, port 1. On NAM-NX1, a port name might be displayed at Ethernet1/1/1.

On NAM hardware, one of the two interfaces must be selected as the Prime NAM management port for IP traffic (such as HTTP and SNMP). Prime NAM can monitor traffic for analysis on the internal interface, the external interface, or both simultaneously. A typical configuration is to monitor LAN and WAN traffic on the internal interface. However, the external interface can be used to monitor LAN traffic.

Some Cisco switches do not support SNMP MIB objects that are required by NAM when configuring SPAN sessions. On these switches, you can use the switch device CLI command to configure the SPAN session for NAM. Alternatively, for the NAM appliances only, if the NAM managed device supports NetConf interface over SSH, you can configure the NAM to use NetConf to configure SPAN sessions on the managed device.

Understanding How the Prime NAM Uses SPAN

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure up to two SPAN sessions in a Catalyst 6500 chassis. Newer Cisco IOS images may support more than two SPAN sessions. Consult the Cisco IOS document for the number of SPAN sessions supported per switch or router.

Table A-3 describes the types of SPAN sources and the possible ways to configure them.

Table A-3 SPAN Sources

SPAN Source	Configured with one of the following:
Any set of physical ports	• **Prime NAM** (the GUI)[1] • Switch CLI
Any EtherChannel	• **Prime NAM** (the GUI) • Switch CLI
Any set of VLANs configured on the local switch	• **Prime NAM** (the GUI) • Switch CLI

1. See the *NAM Compatibility Matrix* for detailed list of NAM devices that can be configured using the GUI.

See Table C-3 for a description of the fields on the SPAN Sessions window.

Table A-4 lists the possible SPAN states. The SPAN state displays in parenthesis in the Source - Direction column.

Table A-4 Possible SPAN States

State	Description
Active	SPAN source is valid and packet traffic from the source is copied to the SPAN destination (NAM Dataport).
Inactive	Packet traffic from the source is not copied to the SPAN destination (NAM Dataport).
Up	For NAM-NX1 only, the Supervisor displays this when packets are forwarded to the NAM.
Down	For NAM-NX1 only, the Supervisor displays this when packets are not forwarding to the NAM.

The NAM-3 platform provides two possible destination ports for SPAN and VLAN access control list (VACL) sessions. Multiple SPAN sessions to the Prime NAM are supported, but they must be destined for different ports. The Prime NAM destination ports for use by the SPAN graphical user interface (GUI) are named DATA PORT 1 and DATA PORT 2 by default. In the CLI, NAM-3 SPAN port is named dataport1 and dataport2.

For more information about SPAN and how to configure it on the various NAM platforms, see your device documentation on Cisco.com.

Note Due to potentially very high volume of ERSPAN traffic from the source, we recommend that you do not terminate the ERSPAN session on the NAM management port. Instead, you should terminate ERSPAN on the switch, and use the switch's SPAN feature to SPAN the traffic to NAM dataports.

Understanding How the Prime NAM Uses VACLs

A VLAN access control list can forward traffic from either a WAN interface or VLANs to a dataport on the NAM. A VACL provides an alternative to using SPAN; a VACL can provide access control based on Layer 3 addresses for IP and IPX protocols. The unsupported protocols are access controlled through the MAC addresses. A MAC VACL cannot be used to access control IP or IPX addresses.

There are two types of VACLs: one that captures all bridged or routed VLAN packets and another that captures a selected subset of all bridged or routed VLAN packets. Catalyst operating system VACLs can only be used to capture VLAN packets because they are initially routed or bridged into the VLAN on the switch.

A VACL can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN or, with Release 12.1(13)E or later releases, a WAN interface. Unlike regular Cisco IOS standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, the VACLs apply to all packets and can be applied to any VLAN or WAN interface. The VACLs are processed in the hardware.

A VACL uses Cisco IOS access control lists (ACLs). A VACL ignores any Cisco IOS ACL fields that are not supported in the hardware. Standard and extended Cisco IOS ACLs are used to classify packets. Classified packets can be subject to a number of features, such as access control (security), encryption, and policy-based routing. Standard and extended Cisco IOS ACLs are only configured on router interfaces and applied on routed packets.

After a VACL is configured on a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VACL. Packets can either enter the VLAN through a switch port or through a router port after being routed. Unlike Cisco IOS ACLs, the VACLs are not defined by direction (input or output).

A VACL contains an ordered list of access control entries (ACEs). Each ACE contains a number of fields that are matched against the contents of a packet. Each field can have an associated bit mask to indicate which bits are relevant. Each ACE is associated with an action that describes what the system should do with the packet when a match occurs. The action is feature dependent. Catalyst 6500 series switches and Cisco 7600 series routers support three types of ACEs in the hardware: IP, IPX, and MAC-Layer traffic. The VACLs that are applied to WAN interfaces support only IP traffic.

When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet coming into the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL applied to the routed interface and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny.

When configuring VACLs, note the following:

- VACLs and context-based access control (CBAC) cannot be configured on the same interface.
- TCP Intercepts and Reflexive ACLs take precedence over a VACL action on the same interface.
- Internet Group Management Protocol (IGMP) packets are not checked against VACLs.

Note You cannot set up VACL using the Prime NAM interface.

For details on how to configure a VACL with Cisco IOS software, see Cisco.com.

For details on how to configure a VACL on a WAN interface and on a LAN VLAN, see Forwarding VACL Traffic, page 7-13.

Understanding How the Prime NAM Uses NetFlow

The Prime NAM uses NetFlow as a format for the ongoing streaming of aggregated data, based on the configured set of descriptors or queries of the data attributes in NAM. NetFlow Data Export (NetFlow) is a remote device that allows you to monitor port traffic on the NAM; the Prime NAM can collect NetFlow from local or remote switches or routers for traffic analysis.

To use an NetFlow data source for the Prime NAM, you must configure the remote device to export the NetFlow packets. The default UDP port is 3000, but you can configure it from the Prime NAM CLI as follows:

```
root@nam2x-61.cisco.com# netflow input port ?
<port>                    - input NetFlow port number
```

The distinguishing feature of the NetFlow v9 format, which is the basis for an IETF standard, is that it is template-based. Templates provide an extensible design to the record format, a feature that must allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format.

For more detailed information about Prime NAM and NetFlow, see Forwarding NetFlow Traffic, page 7-14.

For specific information about creating and managing NetFlow queries, see the *Cisco Network Analysis Module API Programmer's Guide* (contact your Cisco account representative if you need to refer to this document).

Understanding NetFlow Interfaces

To use a device as an NetFlow packet data source for the **Prime NAM**, you must configure the device itself to export NetFlow packets to UDP port 3000 on the NAM. You might need to configure the device itself on a per-interface basis. A NetFlow packet device is identified by its IP address. In the NAM, the default UDP port of 3000 can be changed with a **Prime NAM** CLI command (see Configuring NetFlow on Devices, page 7-15).

You can define additional NetFlow packet devices by specifying the IP addresses and (optionally) the community strings. Community strings are used to upload convenient text strings for interfaces on the managed devices that are monitored in NetFlow records.

Remote NetFlow packet devices may export information pertaining to any or all of their individual interfaces. The **Prime NAM** keeps track of the interface associated with any flow information received from the device. On the NDE Interface Analysis page (**Analyze > Traffic > NDE Interface**), you can view information for any selected interface on the device. This page will display the interface utilization or throughput over time, as well as show the top Applications, Hosts, and DSCP groups in both the input and output directions for the interface.

Understanding NetFlow Flow Records

A NetFlow packet contains multiple flow records. Each flow record has two fields:

- Input SNMP ifIndex
- Output SNMP ifIndex

Note This information might not be available because of NetFlow feature incompatibility with your Cisco IOS version, or because of a NetFlow flow-mask configuration.

In most cases, turning on NetFlow on an interface populates the NetFlow cache in the device with flows that are in the *input* direction of the interface. As a result, the input SNMP ifIndex field in the flow record has the ifIndex of the interface on which NetFlow was turned on. Sample NetFlow Network, Figure A-1, shows a sample network configuration with a NetFlow router.

Figure A-1 Sample NetFlow Network

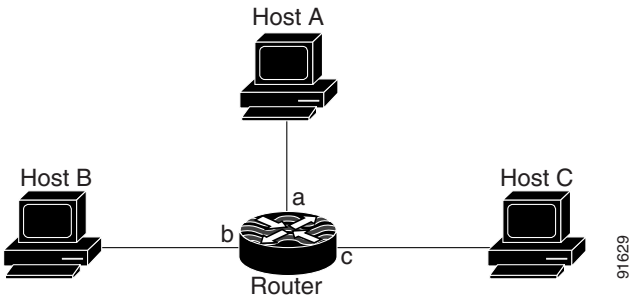


Table A-5 lists the reported flows if NetFlow is enabled on interface a.

Table A-5 Reporting Flow Records

Input Interface	Output Interface	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	No
b	a	No
c	a	No
c	b	No

Managing NetFlow Data Sources

A data source entry must exist on **Prime NAM** in order for it to accept NetFlow records from an external device. Data source entries may be created manually using the **Prime NAM** web GUI or the CLI. When manually creating a data source, you may specify any name you want for the data source.

For convenience, manual creation of NetFlow data sources is not necessary. There is an "autocreate" feature which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device which sends NetFlow packet traffic to the Prime NAM when the first packet is received.

Autocreated NetFlow data sources will be assigned a name in the format *NetFlow-<IP Address>-ID-<Integer>*, where *<IP Address>* is the IP address of the exporting device, and *<Integer>* is the Engine-ID that the device populates in the packets (part of the NetFlow Data Export standard). An example might be "NetFlow-10.10.0.1-ID-12" for device 10.10.0.1 sending NetFlow packets with the Engine ID field set to 12. You can edit these autocreated data sources and change the name if you want to, as well as optionally specifying SNMP credentials for the device, as described later in this guide.

Understanding How the Prime NAM Uses WAAS

Cisco Wide Area Application Services (WAAS) software optimizes the performance of TCP-based applications operating in a wide area network (WAN) environment and preserves and strengthens branch security. The WAAS solution consists of a set of devices called Wide Area Application Engines (WAEs) that work together to optimize WAN traffic over your network.

When client and server applications attempt to communicate with each other, the network devices intercepts and redirects this traffic to the WAEs to act on behalf of the client application and the destination server.

WAEs provide information about packet streams traversing through both LAN and WAN interfaces of WAAS WAEs. Traffic of interest can include specific servers and types of transaction being exported. Prime NAM processes the data exported from the WAAS and performs application response time and other metrics calculations and enters the data into reports you set up.

The WAEs examine the traffic and using built-in application policies to determine whether to optimize the traffic or allow it to pass through your network not optimized.

You can use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You can also use the WAAS Central Manager GUI to create new application policies so that the WAAS system will optimize custom applications and less common applications. Prime NAM is accessible from within the Central Manager interface. The Cisco Prime NAM integration with WAAS Central Manager provides for easier viewing of Prime NAM reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments. See Using the WAAS Central Manager, page 7-22.

For more information about WAAS data sources and managing WAAS devices, see Understanding WAAS, page 7-21.

Understanding Prime NAM Behavior Reference

This appendix includes details on how Cisco Prime Network Analysis Module (Prime NAM) works including how to navigate and use the control elements in the user interface.

This section includes the following topics:

For the location of the release-specific documentation for the command line interface or the application programming interface, see the *Cisco Prime NAM Documentation Overview* on Cisco.com.

Menu Bar

For a description of common tasks in Prime NAM, see Table B-1.

Table B-1 Summary of Menu Tasks

Menu Name	Description
Home	Brings you to the Traffic Summary Dashboard (**Monitor > Overview > Traffic Summary**).
Monitor	View summary dashboards with network traffic, application performance, site performance, and alarms information at a glance.

Table B-1 Summary of Menu Tasks (continued)

Menu Name	Description
Analyze	See various views for traffic over a time period, WAN optimization, response time, managed device, and media functions.
Capture	Configure multiple sessions for capturing, filtering, and decoding packet data, manage the data in local or remote storage, and display the contents of the packets.
Setup	Perform setup options needed to access Prime NAM features.
Administration	Set dashboard preferences, perform user and system administration tasks, and generate diagnostic information for obtaining technical assistance.

Filters

You can use the Filter feature to display specific information on the Prime NAM interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- Quick Filter
- Advanced Filter

Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option.

To launch the quick filter, choose **Quick Filter** from the Filter drop-down menu.

To clear the Quick Filter, click the Filter icon.

Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and operator from the drop-down menu. In addition, you must enter filter criteria based on the data available in the Prime NAM database.

To launch advance filtering, choose **Advanced Filter** from the Filter drop-down list.

To clear the Advanced Filter, click the Filter icon.

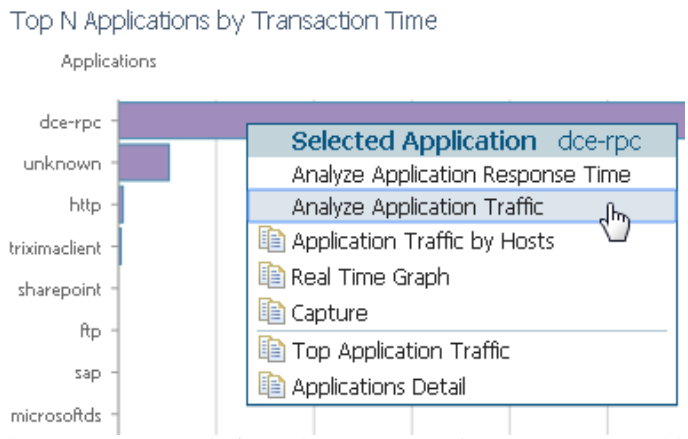
Displaying Detailed Views

You can access additional details from the Dashboard and Monitor and Analyze mega-menus that provide packet and bits per second data as well as identify host, application, DCSP, and other categories. Select a graph element and left-click to view menu options. These may include options titled **Details** or **Detailed Views**. For an example of the Applications submenu see Figure B-1 on page B-3.

Accessing Context Menus

On most charts that appear on the dashboards (except for pie charts), you can left-click on a colored bar of data to get a context menu, with which you can get more detailed information about that item. See Figure B-1 on page B-3.

Figure B-1 Context Menu Showing Application Submenus



The example above is from the Response Time Summary Dashboard, Top N Applications by Transaction Time chart. The description to the right of "Selected Application" in the menu shows what item you had clicked on (in this case, *dce-rpc*).

The menu items above the separator line are specific to the selected element of the Top N chart. The items below the separator line are not specific to the selected element, but apply to the Top N chart. The selections with no icons display in the current page. Selections with icons open in a separate page.

Performing a Quick Capture

From the Context menu of many of the bar charts that show Applications or Hosts or VLANs. you can start a Capture. For example, when you click on an Application in a bar chart (as in Figure B-1 on page B-3) and choose Capture, the following is done automatically:

- A memory-based capture session is created
- A software filter is created using that application
- The capture session is started
- The decode window pops open and you can immediately see packets being captured.

Note Quick Capture does not use site definition/filter.

From both the selectors in the upper left of the dashboards and from the item the user clicks on in the barchart, the following are carried into the context for the capture session:

- Application
- VLAN
- Host
- Data Source (if it is a DATA PORT)

If you open up the associated Capture Session and its associated Software Filter, the above settings will be shown.

Determining How to Use Sites to View Data

A *site* is an optional collection of hosts, or network endpoints, partitioned into views that help you monitor traffic and troubleshoot problems (see Configuring Sites, page 7-41 for more detailed information).

If you have set up sites, you will be able to select a particular site to view in the Interactive Report and view data relevant to that site only. In some cases, you can select both a Client Site and a Server Site to view data pertaining to interaction between hosts at different sites.

Filtering Traffic for Viewing on the Dashboards

You can use the Interactive Report on most Monitor and Analyze windows to filter the parameters of the information displayed in the dashboards. Use the Monitor windows to view *at a glance* data and the Analyze windows to view data over time.

Step 1 Click the **Filter** button to change the parameters of the information displayed in the charts. An asterisk represents required fields.

Step 2 To search for a specific site's VLAN traffic, select the Site name from the drop-down menu. Then select Encapsulation **Edit** button and enter the Layer 1 VLAN options on which you want to filter. You can select multiple values and additional layers.

To set a custom time range, select the **Custom** option from the Time Range drop-down menu. Then enter the dates and times. The From and To fields are only enabled when the Time Range is set to **Custom**.

You may need to enter the time range filter several times before seeing the data that you need. The default filter time range is for the last hour.

The reporting time interval selection changes depends upon both the dashboard you are viewing and your NAM platform.

Step 3 To view your updated filter results in the dashboard, click **Apply**.

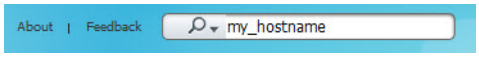
Step 4 To save your filter for future use, enter a Filter Name and click **Submit**.

The software supports up to five saved filters. Saved reports display at the bottom of the Interactive Report panel. You can also edit or delete filters after creating them using the icons in the saved filter dialog box.

Filtering Data Using Global Search

You can use the global search filter to limit your overall view to specific host data. The global search tool appears in the top-right corner of the user interface.

Step 1 From your Monitor or Analyze dashboard enter your IPv4, IPv6, and Layer 2 traffic MAC addresses. You may also search using hostnames if you have enabled hostname (DNS lookup) in Prime NAM.



Specified host filters are also in effect for context menu charts. For example, if you specify a hostname filter in Monitor > Response Time Summary, the dashboard refreshes with only data specific to this host (including the IP address and site, if applicable). You can hover over table data for instant details. drill down menus also reflect this host's data.

Step 2 To change the time range, select one of the default ranges or create a custom range.

Switching Chart Formats Using the Chart View / Table View

Using the Chart view lets you see an overview of the data in an integrated manner, and can show you trending information. To get the exact value of any data in the graphical view, hover over a data point to see the tool tip. The chart view may be To toggle between the two views, use the Chart and Table icons at the bottom of the panel:

Accessing Other Tasks Using Mouse-Over for Details

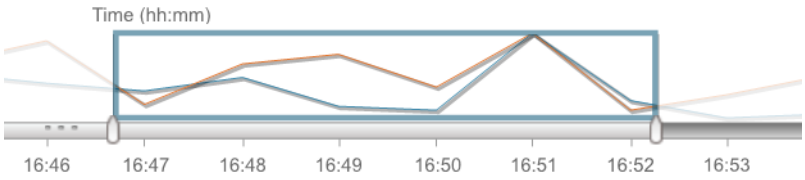
When in Chart view, you can mouse over the chart to get more detailed information about what occurred at a specific time.

Many of the line charts in Prime NAM are dual-axis, meaning there is one metric shown on the left axis of the chart and another metric shown on the right axis of the chart.

For example, in the DCSP Group Traffic chart, Megabits per second is shown on the left axis, and Packets per second is shown on the right axis.

Changing the Time Interval Using Zoom/Pan Charts

For many charts, you can drag the beginning or end to change the time interval, as shown below.

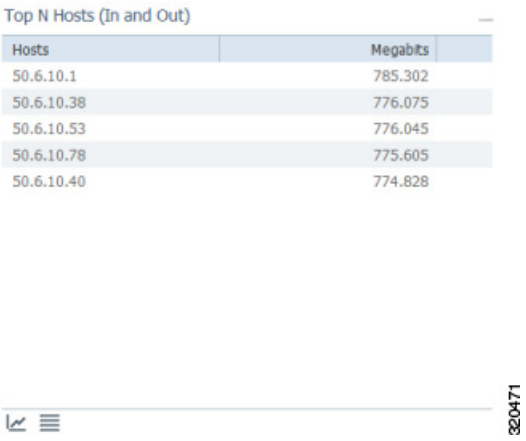


The time interval change on the zoom/pan chart affects the data presented in the charts in the bottom of the window. The zoom/pan time interval also affects the drill down navigations; if the zoom/pan interval is modified, the context menu drill downs from that dashboard will use the zoom/pan time interval.

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.

Using Sort Grid to Change Sort Order

When looking at information in Grid view, you can sort the information by clicking the heading of any column. Click it again to sort in reverse order.



Displaying Bits or Bytes or Packets in Charts

To change the display on most Monitor and Analyze charts from bits to bytes, you can use the Bits and Bytes radio buttons to specify which information you would like the chart to display. To change this preference to display bytes use the **Administration > System > Preferences**.

On most Monitor and Analyze charts, you can use the Bits and Packets check boxes at the top to specify which information you would like the chart to display. To change this preference to display bytes use the **Administration > System > Preferences**.

Statistics

The Statistics legend gives you the minimum, maximum, and average statistics of the data. This will display the initial data retrieved for the selector.

Context-Sensitive Online Help

Click the **Help** link on the top-right corner of the Prime NAM interface to bring you to the Help page for that particular window of the GUI.

If available, the Help link appears on the top-right corner of each page; some pages also have a blue “i”, which provides help for that specific subject.

On some fields, hovering over the field displays tip information.

GUI Field Descriptions

This appendix describes critical field descriptions for the following windows. Not all fields are described as some are self-explanatory and others have tips that appear in the user interface.

Setup User Interface Windows

This section describes the field descriptions for the following dialog boxes:

- NBAR Interface Details
- Site Configuration
- Subnet Detection
- Sites Window
- Add NetFlow Interface Capacity
- Create or Edit Applications
- DSCP Group Setup Dialog Box
- Applications
- URL-Based Applications
- Response Time Configuration Window
- Voice Monitor Setup Window
- URL Collection Configuration Dialog Box

Create SPAN Session Dialog Box

Table C-1 describes the critical fields on the Create SPAN Session dialog box.

Table C-1 Create SPAN Session Dialog Box

Field	Description
Session ID	
Span Session Options	• Extended: Allows for IP extended input ACLs to receive a copy of a dropped packed on a destination port even if the actual incoming packet is dropped. • Multicast Best Effort: Multicast packets are delivered to a group using **best - effort** reliability, just like IPv6 unicast packets. • Sampling: Collects NetFlow statistics for a subset of incoming (ingress) IPv4 traffic on the interface, selecting only one out of "N" sequential packets, where "N" is a configurable parameter. • MTU Truncation: Maximum bytes allowed for each replicated packet in a SPAN session • Rate Limit: Sets Committed Access Rate and Distributed Committed Access Rates for the interface's bandwidth
SPAN Type	• Switch Port • VLAN • EtherChannel • RSPAN VLAN You can have only one RSPAN VLAN source per SPAN session.
SPAN Destination Interface	The NAM interface to which you want to send data.
Switch Module	

Table C-1 Create SPAN Session Dialog Box (continued)

Field	Description
SPAN Traffic Direction	
Available and Selected Sources	SPAN sources available for the selected SPAN type.

Prime NAM Data Sources Dialog Box

Table C-2 describes the critical fields on the Prime NAM Data Sources dialog box.

Table C-2 Prime NAM Data Sources

Field	Description
Device	DATA PORT if it is a local physical port or the IP address of the device that is sending NAM data.
Type	The source of traffic for the NAM. DATA PORT if it is a local physical port. WAAS, ERSPAN, or NETFLOW, if a data stream exported from the router or switch or WAE device.
Activity	
Status	ACTIVE or INACTIVE.
Data Source	
Data Source Details	Physical Port or information about the data source being Enabled or Disabled.

Edit SPAN Session Dialog Box

Table C-3 describes the critical fields on the Edit SPAN Session dialog box.

Table C-3 Edit SPAN Session Dialog Box

Field	Description
Session ID	
SPAN Type	
SPAN Destination Interface	The Prime NAM interface to which you want to send data.
SPAN Traffic Direction	Direction of the SPAN traffic.
Available and Selected Sources	SPAN sources available for the selected SPAN type.

SNMP Credential Options in NAM Data Sources Window

Table C-4 describes the options on the NAM Data Sources window for SNMP Credentials.

Table C-4 SNMP Credential Options in NAM Data Sources Window

Field	Description
Mode: No Auth, No Priv	SNMP will be used in a mode with no authentication and no privacy.
Mode: Auth, No Priv	SNMP will be used in a mode with authentication, but no privacy.
Mode: Auth and Priv	SNMP will be used in a mode with both authentication and privacy.
User Name	Enter a username, which will match the username configured on the device.
Auth Password	Enter the authentication password associated with the username that was configured on the device. Verify the password.
Auth Algorithm	Choose the authentication standard which is configured on the device (MD5 or SHA-1).
Privacy Password	Enter the privacy password, which is configured on the device. Verify the password.
Privacy Algorithm	Enter the privacy algorithm, which is configured on the device (AES or DES).

Device System Information Dialog Box

Table C-5 describes the critical fields on the Device System Information dialog box.

Table C-5 Device System Information Dialog Box

Field	Description
Hardware	
Device Software Version	The current software version running on the device.
System Uptime	Total time the device has been running since the last reboot.
SNMP read from device	SNMP read test result. For the local device only.

Alarm Configuration Window

Table C-6 describes the critical fields on the Alarm Configuration Window.

Table C-6 Alarm Configuration Window

Field	Description
Name	Name given to the alarm at setup.
E-mail	**Enable** if turned on. **Disable** if turned off. Choose **Administration > System > E-Mail Setting**.

Table C-6 Alarm Configuration Window (continued)

Field	Description
Trap	**Community:** ***xxxxx*** if configured. If not configured it is blank. Choose **Administration > System > SNMP Trap Setting**.
Trigger Capture	**Session:*xxxxx*** if configured. If no captures are configured it is blank. Choose **Capture > Packet Capture/Decode > Sessions**.
Syslog Remote	**Enable** if turned on. **Disable** if turned off. Choose **Administration > System > Syslog Setting**.
Status	**Missing Trap** means that the trap configured for that alarm action has been deleted. **OK** means the Alarm action was successfully created.

Threshold Configuration Window

Table C-7 describes the critical fields on the Threshold Configuration window.

Table C-7 Threshold Configuration

Field	Description
Type	You can configure eight types of thresholds.
Application	
Site	
Host	
Severity	High or Low (user-configured classification). These alarms are displayed on the Alarm Summary dashboard (**Monitor > Overview > Alarm Summary**). You can choose to view High, Low, or High and Low alarms.
Action	Rising action and Falling action (if configured). Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both.
Status	**OK** if configuration is complete. Otherwise, the issue displays (for example, **Missing Src Site**).
Add Metrics (button)	Adds another row.
Delete (button)	Removes that Metrics row.

Host Alarm Thresholds Window

Table C-8 describes the critical fields on the Hold Alarm Threshold window.

Table C-8 Host Alarm Thresholds

Field	Description
Name	
Site	Choose a site from the list. See Configuring Sites, page 7-41 for information on setting up a site.
Host	Choose a host from the list. You can enter the name of the host if the drop-down list does not contain the desired host.
Application	Choose an application from the list. You can enter the first few characters to narrow the selection in the drop-down list.
DSCP	Choose a DSCP value from the list. You can enter the first few characters to narrow the selection in the drop-down list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). During threshold creation, by default, the falling action is the same as rising action. See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
Host Metrics (per second)	Choose the type of metric from the list, and then enter a value for a Rising threshold and a Falling threshold.

Conversation Alarm Thresholds Window

Table C-9 describes the critical fields on the Conversation Alarm Thresholds window.

Table C-9 Conversation Alarm Thresholds

Field	Description
Name	
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Source Site/Host	Make a selection from the drop-down lists, or leave as **Any**. See Configuring Sites, page 7-41 for information on setting up a site.
Destination Site/Host	Make a selection from the drop-down lists, or leave as **Any**. See Configuring Sites, page 7-41 for information on setting up a site.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
Conversation Metrics (per second)	Choose from one of the six metrics, and then enter a Rising threshold and a Falling threshold.

Application Alarm Thresholds Configuration Window

Table C-10 describes the critical fields on the Application Alarm Thresholds Configuration window.

Table C-10 Application Alarm Thresholds

Field	Description
Name	
Site	Choose a site from the list. See Configuring Sites, page 7-41 for information on setting up a site.
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
DSCP	Choose a DSCP value 0-63, or Any.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Configuring Alarm Actions, page 7-29 for information on setting up alarm actions.
Application Metrics (per second)	Choose Bits or Bytes, and then enter a Rising threshold and a Falling threshold.

Response Time Alarm Threshold Configuration Window

Table C-11 describes the critical fields on the Response Time Alarm Threshold Configuration window.

Table C-11 Response Time Thresholds

Field	Description
Name	
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview > Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Client Site/Host	Make a selection from the lists. See Configuring Sites, page 7-41 for information on setting up a site.
Server Site/Host	Make a selection from the lists, or leave as "Any." See Configuring Sites, page 7-41 for information on setting up a site.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
Response Time Metrics	Choose a metric from the list, and then enter a Rising threshold and a Falling threshold. For the Packets and Bytes-related metrics, the entry is per second. For the time-related metrics, the unit is per microseconds (u).

DSCP Alarm Threshold Configuration Window

Table C-12 describes the critical fields on the DSCP Alarm Threshold Configuration window.

Table C-12 DSCP Alarm Thresholds

Field	Description
Name	Give the DSCP Alarm Threshold a name.
Site	Choose a site from the list. See Configuring Sites, page 7-41 for information on setting up a site.
DSCP	Choose a DSCP value from the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional).
DSCP Metrics (per second)	Choose one of the metric types from the list, and then enter a Rising threshold and a Falling threshold.

RTP Streams Threshold Configuration Window

Table C-13 describes the critical fields on the RTP Threshold Configuration window.

Table C-13 RTP Streams Thresholds

Field	Description
Name	
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Codec	Choose a Codec from the list.
Source Site/Host	Make a selection from the drop-down lists, or leave as “Any.” See Configuring Sites, page 7-41 for information on setting up a site.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.

Table C-13 RTP Streams Thresholds (continued)

Field	Description
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
RTP Stream Metrics	Choose a metric from the list: • Jitter: Variation of packet arrival time compare to expected arrival time. • Adjusted packet loss percent: Percent of packet loss which includes packets actually lost and packets that arrived beyond the expected buffering capability of the endpoint. • Actual packet loss percent: Percent of packets that Prime NAM has never seen. • MOS: Mean opinion score that is composed of both jitter and adjusted packet loss. • Concealment seconds: Number of seconds in which Prime NAM detected packets lost. • Severe concealment seconds: Number of seconds in which Prime NAM detected packets lost of more than 5%. Enter a Rising threshold and a Falling threshold.

Voice Signaling Threshold Configuration Window

Table C-14 describes the critical fields on the Voice Signaling Threshold Configuration window.

Table C-14 Voice Signaling Thresholds

Field	Description
Name	
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	Choose a Rising action and a Falling action from the lists (optional). See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
Voice Signaling Metrics	Choose Jitter to enable an alarm when the software detects jitter to be more than the value set here. Check Packet Loss % to enable an alarm when the software detects Packet Loss percentage to be outside of the values you entered.

NetFlow Interface Threshold Configuration Window

Table C-15 describes the critical fields on the Network Interface Threshold Configuration window.

Table C-15 NetFlow Interface Alarm Thresholds

Field	Description
Direction	Choose Ingress or Egress.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	Choose a Rising action and a Falling action from the lists (optional). See Viewing Alarm Actions, page 7-31 for information on setting up alarm actions.
Application Metrics (per second)	Choose Bytes or Packets, and enter a Rising and Falling threshold.

Router System Information Window

Table C-16 describes the critical fields on the Router System Information window.

Table C-16 Router/Managed Device System Information

Field	Description
Name	
Hardware	
Managed Device Software Version	Current software version of the router.
Managed Device System Uptime	Total time the router or switch has been running.
Location	
Contact	
Managed Device	IP address of the router.
SNMP v1/v2c RW Community String	
Verify String	
Enable SNMP V3	Check the check box to enable SNMP Version 3. If SNMPv3 is not enabled, the community string is used.
Mode: No Auth, No Priv	SNMP is used in a mode with no authentication and no privacy.
Mode: Auth, No Priv	SNMP is used in a mode with authentication, but no privacy.
Mode: Auth and Priv	SNMP is used in a mode with both authentication and privacy.
User Name	Enter a username, which will match the username configured on the device.
Auth Password	Enter the authentication password associated with the username that was configured on the device. Verify the password.

Table C-16 Router/Managed Device System Information (continued)

Field	Description
Auth Algorithm	Choose the authentication standard which is configured on the device (MD5 or SHA-1).
Privacy Password	Enter the privacy password, which is configured on the device. Verify the password.
Privacy Algorithm	Enter the privacy algorithm, which is configured on the device (AES or DES).

Switch/Managed Device System Information

Table C-17 describes the critical fields on the Switch System Information window.

Table C-17 Switch Device Information

Field	Description
SNMP Test information	Displays the IP address of the NAM and the switch on which the SNMP test occurred.
Name	
Hardware	
Supervisor Software Version	
System Uptime	Total time the device has been running.
SNMP read from chassis	SNMP read test result.
SNMP write to chassis	SNMP write test result.
Mini-RMON on chassis	For Cisco IOS devices, displays the status if there are any ports with Mini-RMON configured (Available) or not (Unavailable).
NBAR on chassis	Displays if NBAR is available on the device.
VLAN Traffic Statistics on chassis	Displays if VLAN data is Available or Unavailable. **Note** Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.
NetFlow Status	For Catalyst 6500 Series devices running Cisco IOS, if NetFlow is configured on the device, *Remote export to NAM <address> on port <number>* displays, otherwise the status displays *Configuration unavailable*.

NBAR Interfaces Window

Table C-18 describes the critical fields on the NBAR Interfaces window.

Table C-18 NBAR Interface Details

Field / Operation	Description
Enable (check box)	Check indicates that NBAR is enabled.
Interface	Depending on the IOS running on the Supervisor, port names are displayed differently. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the Virtual Switch software (VSS), a port name might be displayed as Gi1/2/1to represent a Gigabit port on switch 1, module2, port 1.
Interface Description	Description of the interface.

Site Configuration Window

Table C-19 describes the critical fields on the Site Configuration window.

Table C-19 Site Configuration

Field	Description
Name	
Description	
Disable Site (check box)	If you check this check box, the software will skip this site when classifying traffic. This is useful if the site is no longer active, but the user would still like to access historical site data in the database. Otherwise, the user should delete sites that are not needed.
Subnet	IP address subnet (IPv4/IPv6 address and mask); for example, 10.1.1.0/24. Click the blue **i** to get information about Site Rules. You can click the **Detect** button to tell the software to look for subnets in the traffic. See Configuring Sites Using Subnets, page 7-43.
Data Source	Specify the data source from where the site traffic originates. Leave this field blank if the site traffic can come from multiple data sources.

Subnet Detection Window

Table C-20 describes the critical fields on the Subnet Detection window.

Table C-20 Subnet Detection

Field	Description
Subnet Mask	Enter the subnet mask. **Note** If the bit mask is 32 or less, the software will detect an IPv4 subnet. If the bit mask is between 33 and 64, then it will detect an IPv6 subnet.
Data Source	Choose the data source in which you would like to detect subnets.
Interface	Choose the interface in which you would like to detect subnets.
Filter Subnets Within Network	Enter an IPv4 or IPv6 address
Unassigned Site (check box)	The "Unassigned" site includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.

Sites Window

Table C-21 describes the critical fields on the Sites window.

Table C-21 Sites Window

Field	Description
Name	
Description	
Rule	Lists the first rule assigned to the selected site. If you see periods next to the site rule (...), then multiple rules were created for that site. To see the list of all rules, click the quick view icon (after highlighting the site, click the small arrow on the right).
Status	Shows if the site is Enabled or Disabled.

Add NetFlow Interface Window

Table C-22 describes the critical fields on the NetFlow Interface Add window.

Table C-22 Add NetFlow Interface Capacity

Field	Description
Device	Enter the IPv4 or IPv6 address.
ifIndex	Unique identifying number associated with a physical or logical interface. Valid characters: 0-9.
ifName	Name of the interface. Valid characters are A-Z, a-z, 0-9.
ifSpeed(Mbps)	An estimate of the interface's current bandwidth in bits per second.

DSCP Group Setup Dialog Box

Table C-23 describes the critical fields on the DSCP Group Setup dialog box.

Table C-23 DSCP Group Setup Dialog Box

Field	Description	Usage Notes
Name	Name of the profile.	Enter the name of the profile you are creating. The maximum is 64 characters.
Label Format	DSCP	DSCP numbers from 0 to 63. After selecting the DSCP radio button, you can freely choose any of the 64 possible values and assign them to Groups.
	AF / EF / CS	Assured Forwarding (AF) guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, Expedited Forwarding (EF) is used for traffic that is very sensitive to delay, loss and jitter, such as voice or video traffic. Class Selector (CS) the last 3 bits of the 6-bit DSCP field, so these correspond to DSCP 0 through DSCP 7.
	Bit Field	Six bits in the IP header of a packet.

DSCP Group Label Formats

Table C-24 describes the DSCP Group label formats.

Table C-24 DSCP Group Label Formats

DSCP Format (DSCP 0 through DSCP 63)	AF/EF/CS Format	Bit Field Format
DSCP 0	-	000000
DSCP 8	CS1	001000
DSCP 10	AF11	001010
DSCP 12	AF12	001100
DSCP 14	AF13	001110
DSCP 16	CS2	010000
DSCP 18	AF21	010010
DSCP 20	AF22	010100
DSCP 22	AF23	010110
DSCP 24	CS3	011000
DSCP 26	AF31	011010
DSCP 28	AF32	011100
DSCP 30	AF33	011110
DSCP 32	CS4	100000

Table C-24 DSCP Group Label Formats (continued)

DSCP Format (DSCP 0 through DSCP 63)	AF/EF/CS Format	Bit Field Format
DSCP 34	AF41	100010
DSCP 36	AF42	100100
DSCP 38	AF43	100110
DSCP 40	CS5	101000
DSCP 46	EF	101110
DSCP 48	CS6	110000
DSCP 56	CS7	111000

Application Window

Table C-25 describes the critical fields on the Add Application Window.

Table C-25 Create or Edit Applications

Field	Description
Name	Unique 1 to 64 character descriptive name.
Description	
Selector	(Optional) Leave blank. An arbitrary number up to 4-digits, unique within an engine-id. It is automatically assigned if left blank. Identification number is autogenerated if left blank. Range is from 1 to 65535. This allows you to configure applications consistently across multiple NAMs, so that the same user-created application is exported with the same value. This should be used when configuring the same custom applications on multiple NAMs. The application tag for user-created applications is a combination of the engine ID and the Selector. The 32 bit is generated by using the engine ID as the highest order byte, and the Selector makes up the other 3 bytes. For standard application/protocols, the application tag is predefined.
Application Classification Rule	Select application type: Protocol, HTTP URL-based or Server IP Address.
Application Rule: Protocol/Port	Add the application protocol and port you want to track.
	Protocol—Lists predefined protocols. If your option is not included, you can create a custom URL-based application classification.
	Port—Enter the port number or port number range to monitor. The port is an arbitrary number you assign to handle the additional ports for the protocol family. This protocol number must be unique so it does not conflict with standard protocol/port assignments. The port number range will vary depending on the protocol type selected. You can create additional ports to enable Prime NAM to handle additional traffic for standard applications.

Table C-25 Create or Edit Applications (continued)

Field	Description
Application Rule: HTTP URL	Create custom URL-based applications by selecting this option. Enter at least one of the values below.
	URL Host—The host name identified in the header from which the traffic is originating.
	URL Path—The specific URL path that identifies the traffic.
Engine ID	Identifies the type of application (including ethertype, iana-14, iana-13, lic, L7, or custom).
Application Tag	System generated tag which can be used when multiple NAMs are being monitored.
Description	(Optional) Custom description to define your application. Limited to 75 characters.
Status	Active means that network traffic is being analyzed. Inactive means that the application is not being analyzed, possibly due to a duplication of effort. The Interactive Report filter may still list inactive applications if there is any historical data for the inactive application in the database, but it is not collecting new data.

Applications Window

Table C-26 describes the critical fields on the Applications Window.

Table C-26 Applications

Field	Description
Application	Unique 1 to 64 character descriptive name.
Rule	Displays application type: Protocol, HTTP URL-based or Server IP Address.
Selector	An arbitrary number up to 4-digits, unique within an engine-id. It is automatically assigned if left blank. This allows you to configure applications consistently across multiple NAMs, so that the same user-created application is exported with the same value. This should be used when configuring the same custom applications on multiple NAMs. The application tag for user-created applications is a combination of the engine ID and the selector. The 32 bit number is generated by using the engine ID as the highest order byte, and the selector makes up the other 3 bytes. For standard application/protocols, the application tag is predefined.
Engine ID	Identifies the type of application (including ethertype, iana-14, iana-13, lic, L7, or custom)
Application ID	System generated tag which can be used when multiple NAMs are being monitored.

Table C-26 Applications (continued)

Field	Description
Description	If a system-defined, contains system information about the application type. If user-defined, enter custom description to define your application. Limited to 75 characters.
Status	Active means that network traffic is being analyzed. Inactive means that the application is not being analyzed, possibly due to a duplication of effort. The Interactive Report filter may still list inactive applications, but it is not monitored by NAM and is therefore not classified or displayed on NAM dashboards.

URL-Based Applications Window

Table C-27 describes the critical fields on the URL-Based Applications window.

Table C-27 URL-Based Applications

Field	Description
Index	A unique number (1-64) of each URL-based application. You can define up to 64 URL-based applications in NAM.
Host	Matching criteria in the host portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression[1].
Path	Matching criteria in the path portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression[1].
Content-Type	Matching criteria in the Content-Type field of the HTTP packets. This match is a POSIX Regular Expression[1].
Protocol Description	Description of this URL-based application.

1. A regular expression provides a concise and flexible means for matching strings of text, such as particular characters, words, or patterns of characters. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification. The IEEE POSIX Basic Regular Expressions (BRE) standard (released alongside an alternative flavor called Extended Regular Expressions or ERE) was designed mostly for backward compatibility with the traditional (Simple Regular Expression) syntax but provided a common standard which has since been adopted as the default syntax of many Unix regular expression tools, though there is often some variation or additional features. Many such tools also provide support for ERE syntax with command line arguments. In the BRE syntax, most characters are treated as literals - they match only themselves (in other words, a matches "a").

Response Time Configuration Window

Table C-28 describes the critical fields on the Response Time Configuration Window.

Table C-28 Response Time Configuration Window

Field	Description	Usage Notes
Range 1 (µs)	Upper response time limit for the first container	Enter a number in microseconds. The default is 1 to 1,000 µs
Range 2 (µs)	Upper response time limit for the second container	Enter a number in microseconds. The default is 1,001 to 5,000 µs
Range 3 (µs)	Upper response time limit for the third container	Enter a number in microseconds. The default is 5,001 to 10,000 µs
Range 4 (µs)	Upper response time limit for the fourth container	Enter a number in microseconds. The default is 10,001 to 50,000 µs
Range 5 (µs)	Upper response time limit for the fifth container	Enter a number in microseconds. The default is 50,001 to 100,000 µs
Range 6 (µs)	Upper response time limit for the sixth container	Enter a number in microseconds. The default is 100,001 to 500,000 µs
Range 7 (µs)	Upper response time limit for the seventh container	Enter a number in microseconds. The default is 500,001 to 1,000,000 µs
Range 8 (µs)	Upper response time limit for the eighth container. This is the maximum interval that Prime NAM waits for a server response to a client request.	This range cannot be edited. Enter a number in microseconds. The default is 1,000,001 µs to infinity.

Voice Monitor Setup Window

Table C-29 describes the critical fields on the Voice Monitor Setup Window.

Table C-29 Voice Monitor Setup Window

Field	Description
Voice Monitoring	
Enabled	Enables voice monitoring. Ensure this check box is selected if you are interested in voice monitoring.
MOS Values	
Excellent	MOS scores listed here indicate excellent quality voice transmission (where 5.0 is the highest score). The default setting considers the range between 4.34 to 5.0 as *excellent*.
Good	MOS score listed here indicate good quality voice transmission. The default setting considers the range between 4.03 to 4.33 as *good*.

Table C-29 Voice Monitor Setup Window (continued)

Field	Description
Fair	MOS score listed here indicate fair quality voice transmission. The default setting considers the range between 3.6 to 4.02 as *fair*.
Poor	MOS score listed here indicate poor quality voice transmission. The default setting considers the range between 0.0 and 3.59 as *poor*. This default cannot be changed.

URL Collection Configuration Window

Table C-30 describes the critical fields on the URL Collection Configuration Window.

Table C-30 URL Collection Configuration Dialog Box

Element	Description	Usage Notes
Data Source	Identifies type of traffic incoming from the application.	Select one of the options from the drop-down box.
Max Entries	Maximum number of URLS to collect.	Select one of the following options from the drop-down box: • 100 • 500 • 1000
Match only	The application URL to match.	Optional parameter to limit collection of URLs that match the regular expression of this field.

Monitor User Interface Windows

This section describes field descriptions for the following windows:

- Applications Detail
- Application Groups Detail
- Client-Server Application Responses Window
- Client-Server Application Transactions Window
- Client-Server Network Responses Window
- DSCP Detail
- Host Detail
- Interfaces Stats Table
- Last 50 Alarms
- Server Application Responses Metrics
- Server Application Transactions Metrics
- Server Network Responses Window
-

Applications Detail Window

Table C-31 describes the critical fields in this window.

Table C-31 Applications Detail

Field	Description
Application	Software services classified by NAM from analyze and monitor traffic.
Application Group	The application group (set of applications that can be monitored as a whole).
Bytes/sec	Traffic rate; number of bytes per second
Packets/sec	Traffic rate; number of packets per second

Application Groups Detail Window

Table C-32 describes the critical fields in this window.

Table C-32 Application Groups Detail

Field	Description
Application Group	The application group (set of applications that can be monitored as a whole).
Site	Applicable site (or Unassigned if no site)
Bytes/sec	Traffic rate; number of bytes per second
Packets/sec	Traffic rate; number of packets per second

Application Response Time (ART) Metrics

Table C-33 describes the metrics measured for response time.

Table C-33 Application Response Time (ART) Metrics

Metric	Description
Average Response Time	Response Time is the time between the client request and the first response packet from the server, as observed at the NAM probing point. Increases in the response time usually indicate problems with server resources, such as the CPU, Memory, Disk, or I/O due to a lack of necessary resources or a poorly written application. This and other Response Time metrics are in microseconds (µs) units.
Min Response Time	
Max Response Time	
Number of Responses	Total number of request-response pairs observed during the monitoring interval
Number of Late Responses	Total number of responses that exceed the Max Response Time
Number of Responses 1	Number of responses with a response time less than RspTime1 threshold
Number of Responses 2	Number of responses with response time less than RspTime2 and larger than RspTime1
Number of Responses 3	Number of responses with response time less than RspTime3 and larger than RspTime2
Number of Responses 4	Number of responses with response time less than RspTime4 and larger than RspTime3
Number of Responses 5	Number of responses with response time less than RspTime5 and larger than RspTime4

Table C-33 Application Response Time (ART) Metrics (continued)

Metric	Description
Number of Responses 6	Number of responses with response time less than RspTime6 and larger than RspTime5
Number of Responses 7	Number of responses with response time less than LateRsp and larger than RspTime6
Client Bits	Number of TCP payload bits sent from the client(s) during the monitoring interval
Server Bits	Number of TCP payload bits sent from the server(s) during the monitoring interval
Client Packets	Number of TCP packets sent from the client(s) during the monitoring interval
Server Packets	Number of TCP packets sent from the server(s) during the monitoring interval
Average number of concurrent connections	Average number of concurrent TCP connections during the reporting interval
Number of new connections	Number of new TCP connections made (TCP 3-way handshake) during the monitoring interval
Number of closed connections	Number of TCP connections closed during the monitoring interval
Number of unresponsive connections	Number of TCP connection requests (SYN) that are not responded during the monitoring interval
Number of refused connections	Number of TCP connection requests (SYN) that are refused during the monitoring interval
Average Connection duration	Average duration of TCP connections during the monitoring interval
Average Server Response Time	Server Response Time is the time it takes an application server (for example, a web server) to respond to a request. This is the server *think time*, which is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application and/or server resources, such as the CPU, Memory, Disk, or I/O.
Min Server Response Time	
Max Server Response Time	
Average Network Time	Network time between a client and a server. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.
Min Network Time	
Max Network Time	
Average Client Network Time	Client Network Time is the network time between a client and the NAM switch or router. In WAAS monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Min Client Network Time	
Max Client Network Time	
Average Server Network Time	Server Network Time is the network time between a server and NAM probing point. In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.
Min Server Network Time	
Max Server Network Time	
Average Total Response Time	Total Response Time is the total amount of time between the client request and when the client receives the first response packet from the server. Use Total Response Time with care because it is not measured directly and mixes the server response time metric with the network time metric.
Min Total Response Time	
Max Total Response Time	
Average Transaction Time	Transaction Time is the total amount of time between the client request and the final response packet from the server. Transaction times may vary depending upon client usages and application types. Transaction Time is a key indicator for monitoring client experiences and detecting application performance anomalies.
Min Transaction Time	
Max Transaction Time	

Table C-33 Application Response Time (ART) Metrics (continued)

Metric	Description
Number of Transactions	The number of transactions completed during the monitoring interval.
Average Data Transmission Time	Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.
Average Data Time	Data Time: Average data time portion of transaction time.
Packets Retransmitted	Number of retransmitted packets detected during the monitoring interval
Bits Retransmitted	Number of retransmitted bits detected during the monitoring interval
Average Retransmission Time	Average time to retransmit lost packets per transaction
Client ACK Round Trip Time	Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point
Number of Client ACK Round Trips	Number of client ACK RTs observed during the monitoring interval

Client Server Application Responses Window

Table C-34 provides definitions of the critical fields of the Client-Server Application Responses window.

Table C-34 Client-Server Application Responses Window

Field	Description
Number of Responses	Total number of responses observed during the monitoring interval
Minimum Client Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Client Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Client Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Server Network Time (ms)	Minimum network time between a server and NAM probing point.
Average Server Network Time (ms)	Average network time between a server and NAM probing point.
Maximum Server Network Time (ms)	Maximum network time between a server and NAM probing point.
Minimum Total Response Time (ms)	The total amount of time between the client request and the final response packet from the server.
Average Total Time (ms)	Average time (ms) elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Maximum Total Time (ms)	The total amount of time between the client request and the final response packet from the server.

Client-Server Application Transactions Window

Table C-35 provides definitions of critical fields in the Client-Server Application Transactions window.

Table C-35 Client-Server Application Transactions Window

Field	Description
Number of Transactions	Total number of transactions observed during the monitoring interval.
Average Transaction Time (ms)	Average time elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Average Server Response Time (ms)	Amount of time it takes a server to send the initial response to a client request as seen by the NAM.
Average Data Transmission Time (ms)	Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.
Average Retransmission Time (ms)	Average time to retransmit lost packets per transaction
Client ACK Round Trip Time (ms)	Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point

Client-Server Network Responses Window

Table C-36 describes the critical fields of the Client-Server Network Response Time window.

Table C-36 Client-Server Network Responses Window

Field	Description
Minimum Client Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Client Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Client Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Server Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Server Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Server Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Network Time (ms)	Minimum of the network time measured by analyzing TCP three-way handshake sequence. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.

Table C-36 Client-Server Network Responses Window (continued)

Field	Description
Average Network Time (ms)	Average of the network time measured by analyzing TCP three-way handshake sequence.
Maximum Network Time (ms)	Maximum of the network time measured by analyzing TCP three-way handshake sequence.

DSCP Detail Window

Table C-37 describes the critical fields in this window.

Table C-37 DSCP Detail

Field	Description
Bytes/sec	Traffic rate; number of bytes per second. In **Administration > System > Preferences**, you can choose to display NAM data in Bits or Bytes.
Packets/sec	Traffic rate; number of packets per second

Host Detail Window

Table C-38 describes the critical fields in this window.

Table C-38 Host Detail

Field	Description
In Bits/sec	Number of bits per second incoming
In Packets/sec	Number of packets per second incoming
Out Bits/sec	Number of bits per second outgoing
Out Packets/sec	Number of packets per second outgoing

Interfaces Stats Table

Table C-39. describes the critical fields in the Interfaces Stats table.

Table C-39 Interfaces Stats 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 incoming packets collected per second.
Out Packets/s	Number of outgoing packets sent out per second.
In Bits/s	Number of bits collected per second.
Out Bits/s	Number of bits sent out per second.

Table C-39 Interfaces Stats Table (continued)

Field	Description
In Non-Unicast/s	Number of non-unicasts collected per second.
Out Non-Unicast/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.

Last 50 Alarms Table

Table C-40 describes the critical fields on the Last 50 Alarms table.

Table C-40 Last 50 Alarms

Field	Description
Site	This contains site or source and destination sites (source - destination) of the network traffic that generated the alarm message.
Alarm Triggered By	Details information of the network traffic that generated the alarm message. The format of the alarm triggered by string are: • Triggered by application threshold: application • Triggered by application with DSCP threshold: DSCP:codepoint - application • Triggered by host threshold: host • Triggered by host with application threshold: host - application • Triggered by host with application and DSCP: DSCP: code point - host - application • Triggered by host with DSCP: DSCP: code point - host • Triggered by conversation: source - destination • Triggered by conversation with application: source - application - destination • Triggered by response time: IAP: client - application - server. • Triggered by DSCP: DSCP: code point • Triggered by RTP stream: source - source port - codec(codec string) - SSRC(number) - destination - destination port • Triggered by voice signaling: Calling (address - number) Called (address - number) ID/References (id() - ref (calling:called)) • Triggered by NetFlow interfaces: NetFlow: Device (address) - If-Index(number) - Ingress/Egress
Threshold Variable	Parameter of the threshold that is used to evaluate alarm condition.
Threshold Value	User defined rising value of the threshold variable.
Triggered Time	Time when the alarm condition was found occurred.

Table C-40 Last 50 Alarms (continued)

Field	Description
Triggered Value	Parameter value when the alarm condition was raised. Note: The triggered value could be - when the viewing window does not included the alarm when it was occurring.
Clear Time	Time when the alarm condition was resolved. The alarm variable has fallen below the falling threshold value.

Server Application Responses Window

Table C-41 provides definitions of the critical fields of the Server Application Responses window.

Table C-41 Server Application Responses Metrics

Field	Description
Average Client Network Time (ms)	Client Network Time is the network time between a client and the NAM switch or router. In WAAS monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Maximum Client Network Time (ms)	
Average Server Response Time (ms)	Server Response Time is the time it takes an application server (for example, a web server) to respond to a request. This is the server *think time*, which is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application and/or server resources, such as the CPU, Memory, Disk, or I/O.
Maximum Server Response Time (ms)	
Average Total Response Time (ms)	Total Response Time is the total amount of time between the client request and when the client receives the first response packet from the server.
Maximum Total Response Time (ms)	

Server Application Transactions Window

Table C-42 provides definitions of the critical fields of the Server Application Transactions window.

Table C-42 Server Application Transactions Metrics

Field	Description
Average Transaction Time (ms)	Average time (ms) elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Average Server Response Time (ms)	Amount of time it takes a server to send the initial response to a client request as seen by the NAM.
Average Data Transfer Time (ms)	Average elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time. Data transfer time is always measured in the server-to-client direction and can be used to detect problems for a particular type of transaction of an application.
Average Retransmission Time (ms)	Average time to retransmit lost packets, per transaction.
Client ACK Round Trip Time (ms)	Average round trip time for the client to acknowledge (ACK) a server TCP packet.

Server Network Responses Window

Table C-43 provides definitions of the critical fields of the Server Network Response Times window.

Table C-43 Server Network Responses Window

Field	Description
Average Server Network Time (ms)	Average of the Server Network Time (network time between a server and NAM probing point).
Maximum Server Network Time (ms)	Maximum of the Server Network Time (network time between a server and NAM probing point).
Average Network Time	Average of the network time between client and server. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.
Maximum Network Time	Maximum of the network time between client and server.
Server Bytes	Number of TCP payload bytes sent from the server(s) during the monitoring interval.
Client Bytes	Number of TCP payload bytes sent from the client(s) during the monitoring interval.

Calls Table

Table C-44 provides definitions of the critical fields of the Calls Table.

Table C-44 Calls Table

Field	Description
Calling Number	Calling number as it appears in the signaling protocol.
Called Number	Called number as it appears in the signaling protocol.
Calling Host Address	RTP receiving address of the calling party detected by the NAM from inspecting the call signaling protocol.
Calling Port	RTP receiving port of the calling party detected by NAM from inspecting call signaling protocol.
Calling Alias	Calling party name detected by NAM from inspecting call signaling protocol.
Called Host Address	IP address of the phone receiving the call.
Called Port	Port of the phone receiving the call.
Called Alias	Alias name, MGCP endpoint ID, or SIP URI of the called party phone.
Calling Reported Jitter (ms)	Jitter value reported by calling party at the end of the call.
Calling Reported Packet Loss (%)	Percentage of packet loss reported by calling party at the end of the call.
Start Time	Time when the call was detected to start.
End Time	Time when the call was detected to end.
Duration	Duration of the call. **Note** When the call signaling's call tear down sequence is not detected by the NAM, the NAM will assume: - the call ended after 3 hours in low call volume per interval - the call ended after 1 hour in high call volume per interval (high call volume is defined as call table filled up during the interval.)
Called Reported Jitter (ms)	Jitter value reported by called party at the end of the call.
Called Reported Pkt Loss (%)	Percentage of packet loss reported by called party at the end of the call.

RTP Stream for Selected Call Report Statistics

Table C-45 provides definitions of the critical fields of the RTP stream statistics of a selected call calculated by the NAM.

Table C-45 RTP Streams for the Selected Call Table

Field	Purpose
Source Address	IP Address of the originator of the RTP stream
Source Port	UDP port of the originator of the RTP stream
Destination Address	IP address of the receiver of the RTP stream

Table C-45 RTP Streams for the Selected Call Table (continued)

Field	Purpose
Destination Port	UDP port of the receiver of the RTP stream
Codec	Encoding decoding format/algorithm of the RTP stream
SSRC	Synchronization source number as it appear in the RTP header
Duration Weighted MOS	NAM calculated score that takes into account of the duration of the stream
Duration Weighted Jitter	Jitter that takes into account of the duration of the RTP stream among all per-interval reports
Overall Adjusted Packet Loss	Percentile of adjust packets lost against total packets of all per-interval RTP reports.

RTP Conversations Table

Table C-46 provides definitions of the critical fields of the RTP Conversations Table.

Table C-46 RTP Conversations Table

Field	Purpose
Start Time	Time when the RTP stream was discovered by the NAM
Source Address	IP Address of the originator of the RTP stream
Source Port	UDP port of the originator of the RTP stream
Destination Address	IP address of the receiver of the RTP stream
Destination Port	UDP port of the receiver of the RTP stream
Codec	Encoding decoding format/algorithm of the RTP stream
SSRC	Synchronization source number as it appear in the RTP header
Duration Weighted MOS	NAM calculated score that takes into account of the duration of the stream

Capture User Interface Windows

This section includes the following topics:

Capture Analysis Window

Table C-47 describes the Capture Analysis window fields.

Table C-47 Capture Analysis Window Fields

Field	Description
Capture Overview	Provides a summary of the displayed capture including number of packets captured, bytes captured, average packet size, capture start time, duration of capture, and data transfer rate (both bytes and bits per second)
Traffic over Time	Displays a graphic image of network traffic (KB/second)
Protocol Statistics	Displays packets and bytes transferred for each protocol
Hosts Statistics	Displays packets and bytes transferred for each host address

Capture Session Fields

Table C-48 describes the critical fields on the **Capture > Packet Capture/Decode > Sessions** page.

Table C-48 Capture Session Fields

Operation	Description
Start Time	Time the capture was last started. You can stop and restart the capture as many times as necessary.
Size (MB) (Capture to Memory) **Size (MB) x No. files (Capture to Files)**	Size of the session **Note** *Capture to files* indicates the capture is being stored in one or more files and is a link to those files. The capture file size is limited to 500 MB on Nexus 1000V, SM-SRE, and vNAM. On all other NAM platforms, the capture file size limit is 2,000 MB.
State	The current status of the capture: • Running—Packet capture is in progress • Stopped—Packet capture is stopped. Captured packets remain in buffer, but no new packets are captured • Full—The memory or file is full, and no new packets will be captured.
Location	The location of the capture (Memory, Local Disk, and external storage).
Capture Operation Buttons	
Create	Create a new capture session. See Configuring Capture Sessions, page 4-6.
Edit	Edit the settings of the selected capture.
Delete	Delete a selected session. Not available if capture session is running.
Start	Start capturing to a selected session. The number in the Packets column for that session will start to rise.
Stop	Stop capturing to the selected session (no packets will go through). Capture data remains in the capture memory buffer, but no new data is stored. Click Start to resume the capture.

Table C-48 Capture Session Fields (continued)

Operation	Description
Clear	Clear captured data from memory.
Decode	Display details of the capture session.
Save to File	Save a session to a file on the NAM hard disk. See Working with Capture Files, page 4-18.

Capture Setting Fields

Table C-49 describes the Capture Settings fields.

Table C-49 Capture Settings Fields

Field	Description	Usage Notes
Packet Slice Size (bytes)	The slice size in bytes; used to limit the size of the captured packets.	Enter a value between 64 and 9000. Enter zero (0) to not perform slicing. If you have a small session but want to capture as many packets as possible, use a small slice size. If the packet size is larger than the specified slice size, the packet is *sliced* before it is saved in the capture session. For example, if the packet is 1000 bytes and slice size is 200 bytes, only the first 200 bytes of the packet is stored in the capture session.
Capture Source	Data-Ports or ERSPAN	Choose the capture source (check one or more check boxes): • Data-ports: This accepts SPAN, RSPAN, and VACL capture. For NAM on ISR G2 SM-SRE, internal, external, or both.[1] On NAM-NX1, you can select only one data-port at a time. • ERSPAN: Locally terminated is recommended. **Note** On some platforms, you may be limited to selecting only one of the dataports at a time. Most platforms allow you to select both dataports at once.
Storage Type: Memory	Check to store captures in memory	Enter values for **Memory Size** for this capture. Enter a number from 1 up to your platform maximum. If system memory is low, the actual session size allocated might be less than the number specified here. Check (if desired) **Wrap when Full** to enable continuous capture (when the session is full, older packet data is removed to make room for new incoming packets). If you do not check **Wrap when Full**, the capture will end when the amount of data reaches size of session.

Table C-49 Capture Settings Fields (continued)

Field	Description	Usage Notes
Storage Type: File(s)	File Size (MB)	Enter a value for **File Size** (file size can be from 1 MB to 500/2000 MB depending on your platform). If disk space is not available, you are not able to start new capture-to-disk sessions.
	Number of Files	Enter a value for Number Of Files to use for capture. The maximum is determined on the size of the file, numbers of files stored, and the amount of disk space available at the location where these files are stored.
	Rotate Files	Use this feature if you plan to capture sets of small files that allow you to perform instantaneous downloads, decodes, and analysis. Rotating files allows you to automatically maintain your storage space. Check the Rotate Files check box to rotate files. Available only for remote storage or NAM appliances. For information about configuring remote storage, see About Capturing to Data Storage, page 4-22. If you choose the **Rotate Files** option, when you reach the highest number file, the earliest file is overwritten. For example, if you specify **No. Files** to 10, file **CaptureA_1** is overwritten after the NAM writes capture data to file **CaptureA_10**. To determine the most recent capture, check each file's time stamp.
	File Location	If file data storage is available, choose one of the storage targets in the drop-down list. The drop-down list displays only those targets in the Ready state. Local disk is the default, or choose a previously configured remote storage location if available. Each option shows the amount of disk space available for capture packet storage. Maximum capture session size for capture to disk is determined by the available space on the capture target. You can manage these locations from the **Capture > Data Storage** page (see Utilizing Capture Data Storage, page 4-22).

1. The Nexus virtual blade (VB) does not have dataports, so this option is not supported.

Custom Decode Filter Dialog Box

Table C-50 describes the critical fields on the custom decide filter window.

Table C-50 Custom Decode Filter Dialog Box

Field	Description	Usage Notes
Protocol	The protocol to match with the packet.	Choose a protocol from the list. (Select **All** to match all packets regardless of protocol.)
Address (MAC or IP)	Indicates whether to filter by MAC or IP address.	Choose MAC to filter using the source/destination MAC address of the packets. Choose IP to filter using the source/destination addresses of the packets.
Both Directions	Indicates whether the filter is applied to traffic in both directions.	If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A. If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A.
Offset	The offset (in bytes) from the Base where packet data-matching begins.	Enter a decimal number.
Base	The base from which the offset is calculated. If you select absolute, the offset is calculated from the absolute beginning of the packet (for example, the beginning of the Ethernet frame). If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match.	Choose **absolute** or a protocol.

Table C-50 Custom Decode Filter Dialog Box (continued)

Field	Description	Usage Notes
Data Pattern	The data to be matched with the packet.	Enter *hh hh hh ...*, where *hh* are hexadecimal numbers from 0-9 or a-f. Leave blank if not applicable.
Filter Expression	An advanced feature to set up complex filter conditions. The simplest filter allows you to check for the existence of a protocol or field. For example, to see all packets that contain the IPX protocol, you can use the simple filter expression **ipx**.	See Tips for Creating Custom Decode Filter Expressions, page 4-33.

Custom Decode Subexpressions Fields

Table C-51 describes the custom decode fields and provides filter and format details.

Table C-51 Custom Decode Field Subexpressions

Field	Filter By	Format
eth.addr eth.src eth.dst	MAC address	*hh:hh:hh:hh:hh:hh*, where h is a hexadecimal number from 0 to 9 or a to f.
ip.addr ip.src ip.dst	IP address	*n.n.n.n or n.n.n.n/s*, where n is a number from 0 to 255 and s is a 0-32 hostname that does not contain a hyphen.
tcp.port tcp.srcport tcp.dstport	TCP port number	A decimal number from 0 to 65535.
udp.port udp.srcport udp.dstport	UDP port number	A decimal number from 0 to 65535.
protocol	Protocol	Click the Protocol list in the Custom Decode Filter dialog box to see the list of protocols on which you can filter.
protocol [*offset*:*length*]	Protocol data pattern	*hh:hh:hh:hh...*, where hh is a hexadecimal number fro 0 to 9 or a to f. *offset* and *length* are decimal numbers. *offset* starts at 0 and is relative to the beginning of the *protocol* portion of the packet.
frame.pkt_len	Packet length	A decimal number that represents the packet length, not the truncated capture packet length.

Error Scan Window

Table C-52 describes the Error Scan window fields.

Table C-52 Error Scan Window Descriptions

Field	Description
Severity	**Warn**: Warning; for example, an application returned an unusual error code **Error**: A serious problem, such as malformed packets
Group	**Checksum**: A checksum was invalid **Sequence**: Protocol sequence is problematic **Response Code**: Problem with the application response code **Request Code**: An application request **Undecoded**: Dissector incomplete or data can't be decoded **Reassemble**: Problems while reassembling **Malformed**: Malformed packet or dissector has a bug; dissection of this packet aborted

Hardware Filter Dialog Box

Table C-53 describes the Create Hardware Filter dialog box.

Table C-53 Create Hardware Filter Dialog

Attribute	Options	Range
Data Ports	Both Ports, Data Port 1, Data Port 2	—
Frame Length	Equal To, Not Equal To, Greater Than, Less Than	Min. 64, Max 65535
VLAN IDs	Equal To, Not Equal To, Greater Than, Less Than	Min. 1, Max 4095
MPLS Label	Equal To, Not Equal To	Min. 0, Max 1048575
Source Address / Mask	Equal To, Not Equal To	IPv4 address
Destination Address / Mask	Equal To, Not Equal To	IPv4 address
L4 Protocol	Equal To, Not Equal To ICMP, IGMP, IP in IP, GRE, L2Tp, TCP, UDP, Integer	With Custom, you can enter a custom value that is not in the list of common protocols. Enter min. 1, max 255.
L4 Source Port	Equal To, Not Equal To	Min. 1, Max 65535
L4 Destination Port	Equal To, Not Equal To	Min. 1, Max 65535
Pattern Match	Filters packets based on 4-byte hexadecimal patterns anywhere in the first 256 bytes. Equal To, Not Equal To	

NAM Packet Analyzer Decode Window

Table C-54 describes the critical fields on the NAM Packet Analyzer window.

Table C-54 Packet Browser

Field	Description
No.	Packet numbers, listed numerically in capture sequence. If the decode (display) filter is active, the packet numbers might not be consecutive.
Time	Time the packet was captured relative to the first packet displayed (not the first packet in the session). To see the absolute time, see the Detail window.
Source	Packet source, which might be displayed as hostname, IP, IPX, or MAC address. To turn hostname resolution on and off for IP addresses, choose the Setup tab and change this setting under Preferences.
Destination	Packet destination, which might be displayed as hostname, IP, IPX, or MAC address.
Protocol	Top-level protocol of the packet.
Length	Size of the packet, in bytes.
Info	Brief text information about the packet contents.

Software Filter Dialog Box

Table C-55 describes key Software Filter dialog box fields.

Table C-55 Software Filter Dialog Box

Field	Description	Usage Notes
Source Address / Mask	Source address of the packets.	• For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255. • For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: – 1080::8:800:200C:417A – ::FFF:129.144.52.38 **Note** See RFC 5952 for valid text representations. For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.
	The mask applied to the source address.	• If a bit in the Source Mask is set to 1, the corresponding bit in the address is relevant. • If a bit in the Source Mask is set to 0, the corresponding bit in the address is ignored.

Table C-55 Software Filter Dialog Box (continued)

Field	Description	Usage Notes
Destination Address / Mask	Destination address of the packets.	• For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255. • For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: – 1080::8:800:200C:417A **Note** See RFC 5952 for valid text representations. For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.
	The mask applied to the destination address.	• If a bit in the Dest. Mask is set to 1, the corresponding bit in the address is relevant. • If a bit in the Dest. Mask is set to 0, the corresponding bit in the address is ignored.
Network Encapsulation	The protocol to match with the packet.	
Both Directions (check box)	This check box indicates whether the filter is applied to traffic in both directions.	If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A. If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A. The "both directions" check box also affects the ports and not only the addresses (the same logic applies).
VLAN Identifier(s)	The 12-bit field specifying the VLAN to which the packet belongs.	Choose a VLAN Range or enter an individual VLAN IDs. Prime NAM filters the first VLAN only. If you include a range, note this limitation. The VLAN ID can range from 1-4095.
Application[1]	Select the **Application** drop list to filter by application.	Select one protocol to capture from the Application drop-down list.
Source Port(s)	Select the **Port** radio button to filter by port.	Enter one or more ports separated by commas.
Destination Port(s)		Enter one or more ports separated by commas.
IP Protocol		Choose TCP, UDP, or SCTP. No selection (default) means that any will be allowed.

1. The application filter can be used to filter on the highest layer of the protocol parsing; that is usually a layer 4 protocol (based on port). If you want to filter on the transport protocol (for example, UDP or TCP), you will need to use the "IP Protocol" selector. Selecting, for example, TCP in the "IP Protocol" selector will filter on all packets using TCP.

Administration User Interface Windows

This section includes the following sections:

System Overview

9

Table C-56 System Overview

Field	Description
Inputs Tab	
Cumulative Input Statistics	Health and usage information on all the traffic received by the NAM. It shows the number of packets received (Rx Packets), number of packets lost or dropped (Rx Packets Lost), and number of bytes received (Rx Bytes). The Cumulative column shows cumulative counts since the start of the NAM, and the Rate column one shows the same counters for the last ten seconds.
Input Traffic	Usage information in bytes and packets based on the input you select. You can toggle between a chart or table format. Data is updated every 30 seconds and contains data from the past hour. The table time interval cannot be changed. The input table rate is calculated every 10 seconds. A table legend provides data for standard statistics provided by the software for data collected over a period of time. To reset the traffic counters, click on **Reset Traffic** at the bottom of Input Traffic chart.
Resources Tab	
Date	Current date and time synchronized with the switch, router, or NTP server.
IPv4 Address **IPv6 Address**	Based on your configuration, IPv4 address and/or IPv6 address displays.
System Uptime	Length of time the host has been running uninterrupted.
Disk Usage	Config, data, and root partitions with their total and free space. Also shows the amount of disk space used by the performance data base files (DB) and the packet capture to disk (capture files). Use this information to ensure you have enough disk space and perform the needed maintenance as necessary.

Table C-56 System Overview (continued)

Field	Description
Inputs Tab	
Cumulative Input Statistics	Health and usage information on all the traffic received by the NAM. It shows the number of packets received (Rx Packets), number of packets lost or dropped (Rx Packets Lost), and number of bytes received (Rx Bytes). The Cumulative column shows cumulative counts since the start of the NAM, and the Rate column one shows the same counters for the last ten seconds.
Input Traffic	Usage information in bytes and packets based on the input you select. You can toggle between a chart or table format. Data is updated every 30 seconds and contains data from the past hour. The table time interval cannot be changed. The input table rate is calculated every 10 seconds. A table legend provides data for standard statistics provided by the software for data collected over a period of time. To reset the traffic counters, click on **Reset Traffic** at the bottom of Input Traffic chart.
Resources Tab	
Utilization	Percentage of memory resources being consumed by the NAM as well as the total memory available.
CPU Usage	Percentage of CPU resources being consumed by the NAM. Each individual CPU in a multi-CPU platform is listed separately.

SNMP Agent

Table C-57 System SNMP Agent Dialog Box

Field	Description
Location	(Optional) The physical location of the switch or router in which the NAM is installed.
Community String	Add permission and community string information.

E-Mail Setting

Table C-58 Mail Configuration Options

Field	Description
Enable Mail	Enables e-mail of reports and notification of alarms
External Mail Server	IP address or hostnameof external mail server

Table C-58 Mail Configuration Options (continued)

Field	Description
Send Test Mail to	Optional. List e-mail addresses for up to three e-mail recipients.Use this as a verification of your mail setup.
Mail Alarm to	This recipient will receive alarm notifications and scheduled exports. Enter multiple addresses using space or comma delimiters.
Advanced Settings	Enables you to designate an e-mail access server port, as well as select a encryption protocol.
Mail Server Port	Optional. Designate an e-mail port for the NAM.If your mail server is configured with a non-default server port number, use this field to ensure it works with Prime NAM.
Mail Server Encryption	Optional. Select Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for e-mail messaging. Use these encryption protocols to authenticate servers and clients and encrypt messages between you and Prime NAM.

Preferences

Table C-59 describes the critical fields of the Preferences window.

Table C-59 System View and Logging Preferences

Field	Description
Refresh Interval (60-3600 sec)	Amount of time between refresh of information on dashboards. Default is 300.
Top N Entries (1-10)	Number of entries on the Top N charts. Default is 5. To view up to 100 entries, use the Table view versus the chart view.
Perform IP Host Name Resolution	Display hostnames instead of IP Addresses. This option performs translation using DNS lookup. Ensure you set your DNS nameserver parameters. See Setting Network Parameters, page 5-3.
Traffic Display Unit	Data displayed in graph and tables; Bits (default) or Bytes.
Response Time Display Unit	Default is automatic. Options include: microseconds, milliseconds, and seconds.
International Notation	Display options for numbering. May affect report accuracy; see the Cisco Bug Search tool for details.

Table C-59 System View and Logging Preferences (continued)

Field	Description
Audit Trail	Display a listing of recent events that have been recorded. This includes CLI and GUI configuration events. To view, choose **Administration > Diagnostics > Audit Trail**.
IP TOS Flow Key	Include type of service (TOS) data in the NAM network flow. Select only if you are measuring Differentiated Services Code Point (DSCP) for monitored traffic. If you require ART and other flow-based analysis and expect that the TOS information in your network may change in an on-going flow, do not select TOS information to be part of flow configuration. **Note** If TOS byte changes in an on-going flow this results in a new flow being created. If this option is not selected, the entire flow transaction is treated as one flow regardless of a TOS change in this flow. See Using NAM to Monitor QoS/DiffServ (DSCP).

New User Dialog Box

Table C-60 describes the critical fields in the New User dialog box.

Table C-60 New User Dialog Box

Field	Description	Usage Notes
Password **Verify Password**	The account password	Enter a password that adheres to your site security policies.
Privileges	Privileges associated with this account	Select each privilege to grant to the user.

User Privileges

Table C-61 describes the critical fields in the User Privileges window.

Table C-61 User Privileges

Privilege	Access Level
AccountMgmt	Enables a user to create, delete, and edit user accounts.
SystemConfig	Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.
Capture	Enables a user to perform packet captures and manage capture sessions and use the NAM packet analyzer to decode packet data.
AlarmConfig	Enables a user to create, delete, and edit alarms on the switch/router and NAM.

Table C-61 User Privileges (continued)

Privilege	Access Level
MonitorConfig	Enables a user to create, delete, and edit the following: • Collections and reports • Protocol directory entries • Protocol groups • URL-based applications
MonitorView	Enables a user to view monitoring data and reports (granted to all users).

TACACs+ Authentication and Authorization

Table C-62 TACACS+ Authentication and Authorization Dialog Box

Field	Usage Notes
Enable TACACS+ Authentication and Authorization	Determines whether TACACS+ authentication and authorization is enabled. • To enable, check the check box. • To disable, uncheck the check box.
Primary TACACS+ Server	Enter the IP address of the primary server.
Backup TACACS+ Server	Enter the IP address of the backup server (optional). **Note** If the primary server does not respond after 30 seconds, the backup server will be contacted.
Secret Key	Enter the TACACS+ secret key.
Verify Secret Key	Reenter the TACACS+ secret key.

Current User Sessions

Table C-63 describes the critical fields in the Current User Sessions window.

Table C-63 Current User Sessions

Field	Description
From	The name of the machine the user logged in from.
Last Activity	The time stamp of the last user activity.

Report Descriptions

Table C-64 lists the MIB objects supported by the NAM.

Table C-64 NAM RMON Support

Description	Source
MIB-II: All groups except Exterior Gateway Protocol (EGP) and transmission.	RFC 1213
RMON-MIB: Alarm and Event groups only	RFC 2819
RMON2: trapDestTable only	RFC 2021
CDP-MIB: Cisco Discovery Protocol	
EntityMIB	RFC 2737

Troubleshooting Network and NAM Issues

This appendix addresses some common issues you might encounter while using Cisco Prime Network Analysis Module as well as how to use NAM to troubleshoot NAM network connection issues.

This appendix contains the following topics:

Resolving Typical NAM Issues

Q. I see a notification message `No data for selected time interval` on my dashboard reports. What should I do?

A. You may have created a filter that needs to be changed in order to see data. Use the Interactive Report Filter to do any or all of the following actions until your data displays:

- Change the site filters
- Change the application filter
- Incrementally expand the time range from the default to a greater time range

Review the following question for additional details if this does not resolve your issue.

Q. I am sending traffic to the NAM but nothing comes up on the default monitoring page. What could be wrong?

A. There are two typical issues that are seen when first setting up traffic to the NAM:

- Wait for at least five minutes after traffic is sent to the NAM. Prime NAM collects and displays information at intervals and traffic may not display in charts immediately.
- Ensure the client time is synchronized with the NAM time. Typically this means setting your NTP server to synchronize your NAM time. For details, see Synchronizing Your System Time, page 5-5.

Q. What information should I collect and what else should I do when the NAM is not responding?

A. Determine the answers to the following questions and gather the following information:

- Does **session** from the switch/router CLI work?
- Does **ping** over EOBC (127 subnet) work?
- Does **ping** to the management IP address work?
- Collect output of **show tech-support** command from both the NAM and the switch or router.
- Collect core files.
- Check if NAM hardware is seated correctly in chassis

Perform the following tasks to troubleshoot your issue:

- Reset NAM
- Reset into maintenance image or helper
- Clear the configuration
- Reinstall the application image (using the --**reformat** option)

Q. What can I do to increase my Prime vNAM performance level?

A. Prime NAM virtual appliance (vNAM) supports different traffic monitoring speeds based on your deployments. For more details about licensing options and hypervisor dependencies, see the Prime vNAM Data Sheet on Cisco.com.

Q. How can I view NAM log files and send them to TAC for review?

A. From the GUI, go to **Administration -> Diagnostics -> Tech Support**. After the support screen dump is complete, click **Download log files**. Save the files to your local disk. You can analyze the files locally or, if requested forward on to your technical support team for review.

Troubleshooting Login Issues

Log into the NAM by using the username and password that the NAM administrator provided you, and click the Login button. If you are having problems logging in:

- Make sure you are using a browser that is currently supported for use with NAM:
English Firefox 3.6+ or Microsoft Internet Explorer 8+ (Microsoft Internet Explorer 7 is not supported)
- Make sure you are using a platform that is currently supported for use with NAM:
Microsoft Windows XP or Microsoft Windows 7. The Macintosh platform is not supported on this release.
- Make sure you have JavaScript enabled.
- Clear the browser cache and restart the browser (not necessary if installing NAM for the first time).
- Make sure cookies are enabled in your browser.
- If you see the following message: “Initializing database. Please wait until initialization process finishes,” you must wait until the process finishes.
- Make sure your username and password does not use any special characters.
- If your platform requires licensing, make sure you accepted the license agreement and that the license has not expired.
- If the Prime vNAM permanent license is installed and you log in for the first time and accept the EULA, you may be logged out so the permanent license can take effect. We recommend you wait several minutes before you attempt another logon.

To view the full documentation set (including the User Guide and Release Notes) for the Cisco Prime NAM software, go to the NAM software Technical Documentation area on Cisco.com:

- http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html

Understanding Typical Error Messages

Q. I'm waiting for the graphical data to populate on a dashboard. What does this red error "Request Error -- Please Try Again" mean?

A. This means an internal error has occurred, or the login session may have timed out.

Q. I'm waiting for the graphical data to populate on a dashboard. What does this red error "Query resulted in no data" mean?

A. The NAM does not have any data for the specified time frame and specified filter. Go to the Interactive Report (the pane on the left side of the window) and click the **Filter** button to check the filter settings and data sources to make sure the NAM is getting data. You can also check the Overview page to ensure the traffic is reaching the NAM. If no traffic appears, check your data sources and SPAN session configuration.

Q. What does the message "Client or NAM time is incorrect" mean?

A. The browser or client time and the NAM time must be synchronized to avoid this error. See Synchronizing Your System Time, page 5-5.

Frequently Asked Questions about Prime NAM Behavior

Q. How does NAM calculate network latency?

A. To calculate network latency, the software looks at each packet and associates it to a transaction. For example, NAM looks at SYN and SYN-ACK and timestamps these packets to perform these calculations.

Q. How can Prime NAM be restricted to one tenant's traffic when using SPAN or ERSPAN on a Nexus 1000V?

A. Prime NAM can be deployed per tenant so they each NAM has their own portal. NAM processes VxLAN, LISP, FabricPath, and OTV for multiple tenants.

Q. Why is the browser behaving strangely? It is displaying data for no apparent reason or is not displaying expected data.

A. Clear the browser cache, close the browser, and open a new session and try again. Also, make sure you are using a supported browser (see the *Cisco Prime Network Analysis Module Release Notes*).

Q. Why is the NAM performance lower than expected?

A. Disk capture will reduce the NAM performance considerably. It is due to the disk input/output speed. You will see a warning in the top right corner of the window.

Q. Why won't the system change the storage option for my capture session from disk to memory and then back to disk?

A. If you set up a capture session to disk and later modify the same packet session to save into memory, Prime NAM is unable to change the storage selection back to disk because it is in the *in use* state. You cannot delete the capture session to release the disk for capture. The workaround is to reboot the NAM. This has been fixed in the latest patch (patch 5) on the Cisco software download web page.

Q. What MIBs do the Prime NAM support?

A. Table D-1 lists the MIB objects supported by Prime NAM.

Table D-1 Supported MIBs

Description	Source
MIB-II: All groups except Exterior Gateway Protocol (EGP) and transmission.	RFC 1213
RMON2: trapDestTable only	RFC 2021
CDP-MIB: Cisco Discovery Protocol[1]	
EntityMIB	RFC 2737

1. CDP is received on NAM management ports only. NAM does not transmit CDP packets.

Q. Why do all platforms except for NAM-NX1 need if-mib (ifTable) to provide A**nalyze > Managed Device** interface data?

A. NAM-NX1 gets this data by exchanging messaging with the Supervisor Engine on EOBC channel. There is no MIB involved

Q. Which platforms require MIBs?

A. All NAM platforms except NAM-NX1 and NAM appliance platform require the Entity-mib, mib-2, if-mib, and… (don't remember) to get and configure SPAN sessions. NAM-NX1 uses EOBC and proprietary messaging with SUP on EOBC to get and configure SPAN session. Appliance NAM platforms have two options: For the SNMP option, the requirements are the same as other NAM platforms. With a NetConf interface, there is not any MIB involved.

Troubleshooting WAAS Data Issues

Q. Why does Prime NAM display the status of WAAS devices as pending?

A. Prime NAM is unable to monitor WAAS traffic until you set up WAAS monitored servers. To change the pending status, you must set up WAAS monitored servers. See your product documentation for more details.

Q. Why is no WAAS data seen in the Monitor windows?

A. Perform the following steps:

- Use the NAM GUI to verify that the Monitored Servers list is configured with the correct server IP addresses.
- Use the NAM GUI to verify that WAAS data sources have data collection enabled for applicable segments.

- Use the WAAS CLI **show statistics flow filters** to verify that the servers have active traffic flows that are optimized and monitored.
- Use the WAAS CLI **show statistics flow mon tcpstat** to verify that WAAS Flow Agent exports flow data to the correct NAM IP address.

Q. The WAAS is not sending data to the NAM, and the reports are not showing any values.

A. The WAAS will not send data unless filtering is enabled on the NAM. Enable filtering at **Setup > Data Sources > WAAS > Monitored Servers**, and check the "Filter Response Time for all Data Sources by Monitored Servers" check box.

Using the CLI to Troubleshoot Issues

Locating Packet Drops

Q. How can I find out using the CLI if packets are being dropped?

A. The following CLI command shows packet drops at different layers of the NAM system at 5 minute intervals and up to the last 24 hours:

```
root@NAM1x-18.cisco.com# show pkt-drop-counters Hour-0

Start time of the hour: 2010-11-05 13:00 PDT
Time        hardware pkts dropped      FM pkts dropped      ART pkts dropped
13:05                        3548                    0                     0
13:10                        3354                    0                     0
13:15                        2843                    0                     0
13:20                        2629                    0                     0
13:25                        3592                    0                     0
13:30                        3298                    0                     0
13:35                        1823                    0                     0
13:40                        2549                    0                     0
00:00                           0                    0                     0
00:00                           0                    0                     0
00:00                           0                    0                     0
00:00                           0                    0                     0
```

Handling an Unresponsive NAM

Q. Why is my NAM Blade not responding?

A. Do the following:

- Check the NAM IP configuration (using the CLI command **show ip**)
- Check VLAN configuration of management port on Sup:

```
analysis module <slot> management-port access-vlan <#>
```

- Does the session from the switch/router work?
- Does a ping to NAM mgmt IP address work?
- What is the module status on Sup/router?

  `show modules CLI`

Using the CLI to Troubleshoot Performance Agent (PA)

Q. Why is the NAM not receiving data from PA?

A. Prime NAM no longer uses Performance Agent as a remote data source. Use Prime Infrastructure or Prime Assurance to collect PA data.

INDEX

A

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W