Cisco Prime Network Analysis Module
User Guide 5.1(3)

Release 5.1.3
August 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
     800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25961-02
# CONTENTS

**Preface**  9

## CHAPTER 1

**Overview**  1-1

- **Prime NAM**  1-1
- **Overview of the NAM Platforms**  1-2
- **Logging In**  1-2
- **Navigating the User Interface**  1-2
  - **Common Navigation and Control Elements**  1-3
    - **Menu Bar**  1-3
    - **Detailed Views**  1-3
    - **Context Menus**  1-4
    - **Quick Capture**  1-4
    - **Interactive Report**  1-5
    - **Chart View / Grid View**  1-5
    - **Mouse-Over for Details**  1-6
    - **Zoom/Pan Charts**  1-6
    - **Sort Grid**  1-7
    - **Bits / Packets**  1-7
    - **Statistics**  1-7
    - **Context-Sensitive Online Help**  1-8
- **Understanding How the Prime NAM Works**  1-8
  - **Understanding How the NAM Uses SPAN**  1-10
  - **Understanding How the NAM Uses VACLs**  1-10
  - **Understanding How the NAM Uses NDE**  1-11
  - **Understanding How the NAM Uses WAAS**  1-12
  - **Understanding How the NAM Uses PA**  1-12

## CHAPTER 2

**Setting Up the Cisco NAM**  2-1

- **Configuration Overview**  2-2
  - **Configuring and Viewing Data**  2-5
  - **Cisco WAAS NAM Virtual Service Blade**  2-5
Default Functions 2-5
  Traffic Analysis 2-6
  Application Response Time Metrics 2-6
  Voice Signaling/RTP Stream Monitoring 2-6
  Traffic Usage Statistics 2-7
Traffic 2-7
  SPAN 2-7
    About SPAN Sessions 2-7
    Creating a SPAN Session 2-10
    Editing a SPAN Session 2-12
    Deleting a SPAN Session 2-13
Data Sources 2-13
  SPAN 2-14
  ERSPAN 2-15
  VACL 2-22
  NetFlow 2-23
  WAAS 2-33
  Performance Agent 2-40
Hardware Deduplication 2-43
Alarms 2-44
  Alarm Actions 2-44
    Alarm Action Configuration 2-45
    Editing Alarm Actions 2-46
    Deleting Alarm Actions 2-46
Thresholds 2-47
  Setting Host Thresholds 2-48
  Setting Conversation Thresholds 2-49
  Setting Application Thresholds 2-50
  Setting Response Time Thresholds 2-51
  Setting DSCP Thresholds 2-52
  Setting RTP Stream Thresholds 2-52
  Setting Voice Signaling Thresholds 2-54
  Setting NDE Interface Thresholds 2-55
  Editing an Alarm Threshold 2-55
  Deleting a NAM Threshold 2-56
User Scenario 2-56
Data Export 2-57
  NetFlow 2-57
    Viewing Configured NetFlow Exports 2-58
CHAPTER 3  
Monitoring and Analysis  3-1

Navigation  3-2
  Context Menus  3-2
  Interactive Report  3-2
  Saving Filter Parameters  3-3
Traffic Summary  3-4
Response Time Summary  3-5
Site Summary  3-6
Alarm Summary  3-6
Analyzing Traffic  3-9
  Application  3-9
    Hosts Detail  3-9
  Host  3-10
    Applications Detail  3-10
NDE Interface Traffic Analysis  3-11
  DSCP Detail  3-12
  DSCP  3-12
    Application Groups Detail  3-13
URL Hits  3-14
  Viewing Collected URLs  3-14
    Filtering a URL Collection List  3-14
Host Conversations  3-15
Network Conversation  3-15
Top Application Traffic  3-15
Application Traffic By Host  3-16
WAN Optimization  3-17
  Top Talkers Detail  3-17
  Application Performance Analysis  3-17
    Transaction Time (Client Experience)  3-18

Voice  2-84
RTP Filter  2-85
URL  2-85
  Enabling a URL Collection  2-86
  Changing a URL Collection  2-87
  Disabling a URL Collection  2-88
WAAS Monitored Servers  2-88
  Adding a WAAS Monitored Server  2-88
  Deleting a WAAS Monitored Server  2-89
CHAPTER 4 Capturing and Decoding Packet Data 4-1

Capture Sessions 4-2
  Capture Sessions Filters 4-2
  Viewing Capture Sessions 4-3
  Configuring Capture Sessions 4-4
  Software Filters 4-7
Creating a Software Filter 4-7
Editing a Software Capture Filter 4-10
Hardware Filters 4-11
   NAM-3 Hardware Filters 4-11
   Other NAM Hardware Filters 4-16
Files 4-19
   Analyzing Capture Files 4-21
   Error Scan 4-21
   Downloading Capture Files 4-22
   Deleting a Capture File 4-23
   Deleting Multiple Capture Files 4-23
Capture Data Storage 4-23
   Capturing to Data Storage 4-24
      Prepare LUNs 4-24
      Use LUNs 4-25
      Decoding Files 4-25
   Connecting and Disconnecting External Storage 4-25
   Recovering Data Storage 4-25
Viewing Packet Decode Information 4-27
   Browsing Packets in the Packet Decoder 4-28
   Filtering Packets Displayed in the Packet Decoder 4-28
   Viewing Detailed Protocol Decode Information 4-29
Using Alarm-Triggered Captures 4-30
Custom Display Filters 4-30
   Creating Custom Display Filters 4-30
   Editing Custom Display Filters 4-33
   Deleting Custom Display Filters 4-33

CHAPTER 5
Performing User and System Administration 5-1
System Administration 5-1
   Resources 5-2
   Network Parameters 5-2
   SNMP Agent 5-3
      Working with NAM Community Strings 5-4
   System Time 5-6
      Synchronizing the NAM System Time with the Switch or Router 5-6
      Synchronizing the NAM System Time Locally 5-7
      Configuring the NAM System Time with an NTP Server 5-7
      Configuring the NAM System Time with Precision Time Protocol (IEEE 1588) 5-7
CHAPTER 6
Understanding NAM Deployment 6-1

Network Performance Management Lifecycle 6-1

Places in the Network Where NAMs Are Deployed 6-2
Choice of Hardware and Software Platforms for a Given Place in the Network 6-4
A Note on the Cisco NAM Appliances 6-6

Use Cases 6-7
Data Center 6-7
Campus 6-8
Branch 6-8

General Usage Scenarios 6-8
NAM Integrations with Monitoring and Reporting Applications 6-8

Deployment Examples 6-8
Using NAMs to Monitor VoIP Quality  6-9
Autodiscovery Capabilities of NAM  6-11
Creating Custom Applications  6-12
Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment  6-12
Integrating NAM with Third Party Reporting Tools  6-14
Integrating NAM with LMS  6-14
Visibility in the Branch  6-15
Monitoring Cisco WAAS and Measuring Its Impact  6-16
Monitoring  6-19
Real-Time Traffic Monitoring and Analysis  6-20
Using NAM to Monitor QoS/DiffServ (DSCP)  6-22
Using NAM for Historical Trends via Interactive Report  6-26
Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications  6-29
Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications  6-29
Monitoring the Nexus 1000V Switch Environment  6-29
Troubleshooting  6-32
Using NAM for Problem Isolation  6-33
Using NAM for SmartGrid Visibility  6-33

APPENDIX A

Troubleshooting  A-1
General NAM Issues  A-1
Error Messages  A-2
Packet Drops  A-2
NAM Not Responding  A-2
NAM Behavior  A-3
WAAS Troubleshooting  A-3
Performance Agent (PA)  A-4

APPENDIX B

Supported MIB Objects  B-1

INDEX
Preface

This guide describes how to use Cisco Prime Network Analysis Module 5.1(3) (Prime NAM 5.1(3)). This preface has the following sections:

- Chapter Overview, page 9
- Audience, page 10
- Conventions, page 10
- Notices, page 10
- Obtaining Documentation and Submitting a Service Request, page 11

For a list of the platforms that Prime NAM 5.1(3) supports, the NAM Compatibility Matrix on Cisco.com.

Chapter Overview

This guide contains the following chapters:

- Chapter 1, “Overview” provides an overview of the NAM, discusses new features in this release, describes the new GUI, and provides information about how to use various components of the NAM.
- Chapter 2, “Setting Up the Cisco NAM,” provides information about the first steps users should take after booting up the NAM and setting up the NAM applications.
- Chapter 3, “Monitoring and Analysis” provides information about options for viewing and monitoring various types data.
- Chapter 4, “Capturing and Decoding Packet Data” provides 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” provides information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance.
- Chapter 6, “Understanding NAM Deployment” provides scenarios for NAM deployment and the details you may need to know about them.
Audience

This guide is designed for network administrators who are responsible for setting up and configuring Cisco Prime Network Analysis Module (NAM) software and hardware 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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td>boldface font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td>italic font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td>screen font</td>
</tr>
<tr>
<td>Information you enter</td>
<td>boldface screen font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td>italic screen font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td>boldface font</td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td>Option &gt; Network Preferences</td>
</tr>
<tr>
<td>Selecting a menu item in tables</td>
<td>Option &gt; Network Preferences</td>
</tr>
</tbody>
</table>

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 5.1(3). Prime NAM 5.1(3) 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 NAM technical documentation.
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.
Overview

This chapter provides information about Cisco Prime Network Analysis Module 5.1(3). It describes features and how to navigate the interface, and provides general information about to use the Prime NAM functions.

This chapter contains the following sections:

- **Prime NAM**, page 1-1
- **Overview of the NAM Platforms**, page 1-2
- **Logging In**, page 1-2
- **Navigating the User Interface**, page 1-2
- **Understanding How the Prime NAM Works**, page 1-8
  - **Understanding How the NAM Uses SPAN**, page 1-10
  - **Understanding How the NAM Uses VACLs**, page 1-10
  - **Understanding How the NAM Uses NDE**, page 1-11
  - **Understanding How the NAM Uses WAAS**, page 1-12

**Prime NAM**

The Prime NAM (NAM) software empowers network managers with an easy to use traffic analysis toolset to optimize network resources, troubleshoot network performance issues, and ensure a consistent end-user experience.

The Cisco Prime™ portfolio of enterprise and service provider management offerings supports integrated lifecycle management of Cisco architectures and technologies based on a service-centric framework. Built on an intuitive workflow-oriented user experience, Cisco Prime products help increase IT productivity and reduce operations costs through innovative management solutions for the network services, infrastructure, and endpoints.

The Prime NAM combines flow-based and packet-based analysis into one solution. Prime NAM can be used for traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics for network-based services such as Voice over IP (VoIP) and video, and problem analysis using deep, insightful packet captures. Prime NAM includes an embedded, web-based GUI that provides quick access to the configuration menus and presents easy-to-read performance monitoring and analysis on web, voice, and video traffic.

For additional details on how to deploy Prime NAM in your network, see **Understanding NAM Deployment**, page 6-1.
Overview of the NAM Platforms

The portfolio of 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 NAM platforms.

See Choice of Hardware and Software Platforms for a Given Place in the Network, page 6-4 for more information about where you may choose to deploy certain platforms.

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

Logging In

Log in to 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.
- Make sure you have downloaded the most recent version of Adobe Flash.
- Clear the browser cache and restart the browser (not necessarily 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 you had accepted the license agreement (WAAS VB, Nexus 1010, and SRE users only) and that the license has not expired.

To view the full documentation set (including the User Guide and Release Notes) for the Cisco NAM software, go to the NAM software Technical Documentation area on Cisco.com:


Navigating the User Interface

Prime NAM 5.x introduces a redesigned interface and user experience, with intuitive workflows and improved operational efficiency. This section describes the improved navigation and control elements in the user interface.
All times in the NAM are typically displayed in 24-hour clock format. For example, 3:00 p.m. is displayed as 15:00.

## Common Navigation and Control Elements

### Menu Bar

To perform the Prime NAM functions, use the menu bar.

The selections enable you to perform the necessary tasks:

**Home:** Brings you to the Traffic Summary Dashboard (Monitor > Overview > Traffic Summary).

**Monitor:** See “summary” views that allow you to view network traffic, application performance, site performance, and alarms at a glance.

**Analyze:** See various “over-time” views for traffic, WAN optimization, response time, managed device, and media functions.

**Capture:** Configure multiple sessions for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets.

**Setup:** Perform all setup needed to run Prime NAM 5.1(3).

**Administration:** Perform user and system administration tasks, and generate diagnostic information for obtaining technical assistance.

### Detailed Views

Under some topics in the mega-menu, the last selection is “Detailed Views.” Click the small arrow to the right of the menu selections to see the submenu and the functions available.
Context Menus

On most charts that appear on the dashboards, 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.

[Image]

The example above is from the Traffic Summary Dashboard, Top N Applications chart. The description to the right of “Selected Application” in the menu shows what item you had clicked on (in this case, “snmp”).

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.

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 the screenshot above) 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 bar chart, 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.
Interactive Report

On most Monitoring and Analyze windows, you can use the Interactive Report on the left side to view and change the parameters of the information displayed in the charts. You can redefine the parameters by clicking the Filter button on the left side of the Interactive Report.

The reporting time interval selection changes depending upon the dashboard you are viewing, and the NAM platform you are using. The NAM supports up to five saved Interactive Reports.

Chart View / Grid View

Most of the data presented by the NAM can be viewed as either a Chart or a Grid. The Chart view presents an overview of the data in an integrated manner, and can show you trending information. The Grid view can be used to see more precise data. For example, to get the exact value of data in graphical view, you would need to hover over a data point in the Chart to get the data, whereas the same data is easily visible in table format using Grid view. To toggle between the two views, use the Chart and Grid icons at the bottom of the panel:

Next to that icon is the “Show as Image” icon, with which you save the chart you are viewing as a PNG file.
Mouse-Over for Details

When in Chart view, you can mouseover the chart to get more detailed information about what occurred at a specific time.

Many of the line charts in 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 figure above, Total Bytes per second is shown on the left axis, and Total Packets per second is shown on the right axis.

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 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.
Sort Grid

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.

![Top N Hosts - In](image)

Bits / Packets

On most 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.

Note that you can choose to display either Bits or Bytes under Administration > System > Preferences.

![Host Traffic - 42.0.0.8](image)

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>http</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>7,823</td>
</tr>
<tr>
<td>Minimum</td>
<td>89</td>
</tr>
<tr>
<td>Maximum</td>
<td>37,817</td>
</tr>
<tr>
<td>Mean (50th)</td>
<td>340</td>
</tr>
<tr>
<td>1st StdDev (68th)</td>
<td>519</td>
</tr>
<tr>
<td>2nd StdDev (95th)</td>
<td>30,394</td>
</tr>
</tbody>
</table>
Understanding How the Prime NAM Works

Above the Statistics legend is a dropdown selector, which allows you to choose which of the metrics shown in the “over-time” chart you would like reflected in the Statistics legend. For example, if the line chart has Bits or Packets in the check boxes above the line chart, the selector over the Statistics legend will show the same choices, Bits or Packets.

Context-Sensitive Online Help

The “Help” link on the top-right corner of the NAM interface will bring you to the Help page for that particular window of the GUI.

In addition to the Help link on the top-right corner of each page, some pages also have a blue “i”, which provides help for that specific subject.

Understanding How the Prime NAM Works

The Cisco Prime NAM product family addresses the following major functional areas:

- **Network layer Traffic Analysis.** The 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. The NAM offers a rich set of reports with which to view traffic by Hosts, Application or Conversations. See the discussions about Dashboards, starting with Traffic Summary, page 3-4.

- **Application Response Time.** The 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.

- **WAN Optimization insight.** The 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.

- **Voice Quality Analysis.** The NAM provides application performance for real time applications like Voice and Video. The NAM can compute MOS, as well as provide RTP analysis for the media stream. See Media, page 3-37.
• Advanced Troubleshooting. The NAM provides robust capture and decode capabilities for packet traces that can be triggered or terminated based on user-defined thresholds.

• Open instrumentation. The NAM is a mediation and instrumentation product offering, and hence provides a robust API that can be used by partner products as well as customers that have home grown applications. See the *Cisco Prime Network Analysis Module 5.1 API Programmer’s Guide* (contact your Cisco account representative for this document).

The NAM delivers the above functionality by analyzing a wide variety of data sources that include:

• Port mirroring technology like SPAN and RSPAN/ERSPAN. The 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

• VACL

• NetFlow Data Export (NDE). The NAM can analyze NetFlow Data Export (NDE) from Managed Devices (Routers/Switches)

• WAAS

• SNMP

• Performance Agent (PA)

• Network Tap Device. Applies to Cisco NAM appliances only.

Prime NAM uses SNMP as a southbound interface for configuration and data retrieval from switches and routers. NAM 5.x moves away from RMON and toward web services and Netflow Data Export as the northbound interface for data objects. NAM 5.x continues to support baseline manageability features of SNMP such as MIB-2 and IF-TABLE, and the health status and interface statistics that can be used by external products like Fault and Configuration Management offerings (for example, CiscoWorks LMS).

For more information about SPAN, RSPAN, and ERSPAN, see Cisco.com

Table 1-1 summarizes the traffic sources that are used for NAM monitoring.

<table>
<thead>
<tr>
<th>Traffic Source</th>
<th>LAN</th>
<th>WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ports</td>
<td>VLANs</td>
</tr>
<tr>
<td>VACL capture</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NetFlow Data Export NDE (local)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NetFlow Data Export NDE (remote)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SPAN</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ERSPAN</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

The next sections describe how the NAM uses the supported data sources:

• Understanding How the NAM Uses SPAN, page 1-10

• Understanding How the NAM Uses VACLs, page 1-10

• Understanding How the NAM Uses NDE, page 1-11

• Understanding How the NAM Uses WAAS, page 1-12

• Understanding How the NAM Uses PA, page 1-12
Understanding How the 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 or 7600 Routers 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.

The NAM-1 platform provides a single destination port for SPAN sessions. The NAM-2 and NAM-3 platform provides two possible destination ports for SPAN and VLAN access control list (VACL) sessions. Multiple SPAN sessions to the NAM are supported, but they must be destined for different ports. The 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, SPAN ports are named as shown in Table 1-2.

For more information about SPAN and how to configure it on the various NAM platforms, see 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 data ports.

Understanding How the NAM Uses VACLs

A VLAN access control list can forward traffic from either a WAN interface or VLANs to a data port 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 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 VACL, page 2-22.

### Understanding How the NAM Uses NDE

The 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 (NDE) is a remote device that allows you to monitor port traffic on the NAM; the NAM can collect NDE from local or remote switch or router for traffic analysis.

To use an NDE data source for the NAM, you must configure the remote device to export the NDE packets. The default UDP port is 3000, but you can configure it from the NAM CLI as follows:

```
root@nam2x-61.cisco.com# netflow input port ?
<port>                          - input NDE 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 NAM and NetFlow, see NetFlow, page 2-23.

For specific information about creating and managing NDE queries, see the *Cisco Network Analysis Module API Programmer’s Guide 5.1* (contact your Cisco account representative if you need to refer to this document).
Understanding How the 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. 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. Beginning with Prime NAM 5.1(3), the Cisco NAM is accessible from within the Central Manager interface. The Cisco NAM integration with WAAS Central Manager provides for easier viewing of NAM reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments. See WAAS Central Manager, page 2-36.

For more information about WAAS data sources and managing WAAS devices, see Understanding WAAS, page 2-33.

Understanding How the NAM Uses PA

The Performance Agent (PA) can monitor interface traffic and collect, analyze, aggregate, and export key performance analytics to a Cisco Network Analysis Module for further processing and GUI visualization. PA integration with NAM enables you to have a lower cost way to gain visibility into Application Response Time at the branch. NAM integration with PA also reduces complexity of needing to manage a separate NAM product within the branch.

Using Cisco PA, you can gain visibility into application response time and traffic statistics at remote branches. It is supported on ISR 880, ISR 890, and ISR G2 platforms with Cisco IOS Software Release 15.1(4)T. Deployed with WAAS Express, this feature allows an end-to-end view into the WAN-optimized network, delivering a cost-effective and scalable solution.

PA has the ability to consolidate and filter information before it is exported, ensuring that only contextually-required data is exported and consumed versus all data. As an example, NetFlow Export supports a number of functions, including response time and traffic analysis. Instead of exporting multiple different flows, the PA has the intelligence to consolidate, filter, and export flow data that addresses the particular user’s need. Besides consolidating and filtering information, PA’s mediation capabilities also includes the ability to use key Cisco IOS-embedded functionality (for example, Embedded Event Manager, or Class-Based QoS) to enrich both PA functionality and router value.

For information about configuring PA data sources, see Managing ISR PA Devices, page 2-41.
CHAPTER 2

Setting Up the Cisco NAM

This chapter provides information about functions that will begin automatically, and other setup tasks you will need to perform.

This chapter contains the following sections:

- Configuration Overview, page 2-2
- Default Functions, page 2-5
- Traffic, page 2-7
- Alarms, page 2-44
- Data Export, page 2-57
- Managed Device, page 2-62
- Network, page 2-65
- Classification, page 2-74
- Monitoring, page 2-81

Follow the Installation and Configuration Guide for your specific NAM platform to see information about how to install the product, configure it, log in, and get started.
## Configuration Overview

Table 2-1 leads you through the basic configuration steps you can follow for the Cisco NAM. These are not necessarily in the order in which you need to perform them, and many are optional features.

### Table 2-1  Configuration Overview

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>GUI Location</th>
<th>User Guide Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the NAM (upgrade is supported for NAM 5.x platforms)</td>
<td>--</td>
<td>--</td>
<td>See your platform-specific Installation and Configuration Guides</td>
</tr>
<tr>
<td>Configure the Managed Device Information</td>
<td>Traffic will populate on the dashboards if you have configured the managed device.</td>
<td>Setup &gt; Managed Device &gt; Device Information</td>
<td>See Managed Device, page 2-62.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Does not apply to the NAM switch blades.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up the System Time</td>
<td>You will need to set up the System Time correctly; if you do not have the time synchronized, then you will see either incorrect data or no data.</td>
<td>Administration &gt; System &gt; System Time</td>
<td>See System Time, page 5-6.</td>
</tr>
<tr>
<td>Enter additional network connectivity parameters</td>
<td>Add parameters such as your site’s name servers.</td>
<td>Administration &gt; System &gt; Network Parameters</td>
<td>See Network Parameters, page 5-2.</td>
</tr>
<tr>
<td>Verify that traffic has started</td>
<td>Traffic usage statistics for applications, hosts, conversations, VLANs, and DSCP are available on the Traffic Summary Dashboard. This will start automatically after the NAM is turned on and the system time is synchronized correctly.</td>
<td>Home (Traffic Summary Dashboard) or Monitor &gt; Overview &gt; Traffic Summary</td>
<td>See Traffic Analysis, page 2-6.</td>
</tr>
<tr>
<td>Verify that Application Response Time Metrics are being gathered</td>
<td>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. This will start automatically after the NAM is turned on and the system time is synched correctly.</td>
<td>Analyze &gt; Response Time. You can view response times for applications, networks, servers, and clients.</td>
<td>See Application Response Time Metrics, page 2-6.</td>
</tr>
</tbody>
</table>
### Table 2-1 Configuration Overview (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>GUI Location</th>
<th>User Guide Location</th>
</tr>
</thead>
</table>
| **Verify that Voice/RTP Stream Traffic is being gathered** | After the NAM is started, Voice/RTP stream traffic will automatically start being monitored. The NAM enables you to monitor all RTP stream traffic among all SPANed traffic, without having to know the signalling traffic used in negotiating the RTP channels.  
This will start automatically after you turn on the NAM. | Analyze > Media > RTP Streams  
or  
| **Configure NDE Data Export** | Set up the NAM as a producer of NDE (NetFlow Data Export) packets.  
The NAM sends out NDE packets only in NDE v9 format. | Setup > Data Export > NetFlow | See NetFlow, page 2-57. |
| **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 Sites, page 2-65. |
| **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 NAM to notify you, and how you want to be notified.  
Alarms that will be used for Thresholds should be created first, then the Thresholds created second. | Setup > Alarms > Actions  
and  
Setup > Alarms > Thresholds | See Alarm Actions, page 2-44.  
See Thresholds, page 2-47. |
### Chapter 2  Setting Up the Cisco NAM

**Configure Capture**

Configure Capture allows you to configure up to ten sessions for capturing, filtering, and decoding packet data, manage the data in a file control system, 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.

**Configure Scheduled Export**

You can set up scheduled jobs that will generate a daily report at a specified time, in the specified interval, and then e-mail it to a specified e-mail address.

**Set up Northbound API**

NBI (Northbound Interface), also referred to as API (Application Programming Interface), enables partners and customers to provision the NAM and extract performance data. You can write your own scripts based on the NAM Northbound API, but there is setup in the NAM GUI needed.

**Set up TACACS+ server**

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.

**Change System Preferences**

You can change many preferences, such as refresh interval, Top N Entries, Data Displayed, and enabling Audit Trail, as needed.

### Table 2-1  Configuration Overview (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>GUI Location</th>
<th>User Guide Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Capture</td>
<td>Capture allows you to configure up to ten sessions for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets. Per file location, you can have only one capture session. We support up to ten capture sessions. <strong>Note</strong>: NAM virtual blades do not support capture.</td>
<td>Capture &gt; Packet Capture/Decode</td>
<td>See Chapter 4, “Capturing and Decoding Packet Data.”</td>
</tr>
<tr>
<td>Configure Scheduled Export</td>
<td>You can set up scheduled jobs that will generate a daily report at a specified time, in the specified interval, and then e-mail it to a specified e-mail address.</td>
<td>In the Interactive Report (left side of the dashboard), click the Export button</td>
<td>See Scheduled Exports, page 2-60.</td>
</tr>
<tr>
<td>Set up Northbound API</td>
<td>NBI (Northbound Interface), also referred to as API (Application Programming Interface), enables partners and customers to provision the NAM and extract performance data. You can write your own scripts based on the NAM Northbound API, but there is setup in the NAM GUI needed.</td>
<td></td>
<td>For application developers who want to use the NAM APIs to provision network services and leverage data, see the <em>Cisco Network Analysis Module API Programmer’s Guide, 5.1.</em></td>
</tr>
<tr>
<td>Set up TACACS+ server</td>
<td>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.</td>
<td>Administration &gt; Users &gt; TACACS+</td>
<td>See Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 5-17.</td>
</tr>
<tr>
<td>Change System Preferences</td>
<td>You can change many preferences, such as refresh interval, Top N Entries, Data Displayed, and enabling Audit Trail, as needed.</td>
<td>Administration &gt; System &gt; Preferences</td>
<td>See Chapter 5, “Performing User and System Administration.”</td>
</tr>
</tbody>
</table>
Configuring and Viewing Data

Some of the NAM features require configuration of sites. A site is a collection of hosts, or network endpoints, partitioned into views that help you monitor traffic and troubleshoot problems (see Sites, page 2-65 for more detailed information). These features include those in which the NAM provides measurements of application performance on networks where WAAS devices are deployed, and dashboards that show traffic levels between sites and alarms levels per site. All other NAM features can still be used without defining any sites (the default configuration).

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.

Cisco WAAS NAM Virtual Service Blade

To set up Prime NAM 5.1(3) on a Cisco WAAS NAM Virtual Service Blade, you need to follow these steps:

**Step 1** Confirm that you have completed the steps in Chapter 4, “Configuring NAM-WAAS Integration” of the Cisco WAAS NAM Virtual Service Blade Installation and Configuration Guide, specifically for “Configuring WAAS to Send Flow Information to NAM VSB” and “Configuring WAAS Data Source in NAM.”

**Step 2** Configure a site for the Client network. See Sites, page 2-65.

**Step 3** Configure another site for the Server network. See Sites, page 2-65.

**Step 4** Choose Setup > Monitoring > WAAS Servers and click the Add button to add WAAS servers.

**Step 5** Add a specific host IP address of the server that you want to monitor. If there are multiple IP addresses, you can paste them in.

**Step 6** To verify that you have set up the WAAS-NAM properly, choose Analyze > WAN Optimization > Application Performance Analysis and make sure you can see data (passthrough traffic). If you have not properly configured the Client Site and the Server Site, you will not see data in the charts.

Default Functions

After the NAM is turned on, some functions will begin automatically, without any setup steps necessary. These functions are:

- Traffic Analysis, page 2-6
- Application Response Time Metrics, page 2-6
- Voice Signaling/RTP Stream Monitoring, page 2-6
- Traffic Usage Statistics, page 2-7
Traffic Analysis

Traffic usage statistics for applications, hosts, conversations, VLANs, and DSCP will begin populating on the Traffic Summary dashboard (Monitor > Overview > Traffic Summary). To view detailed views of Traffic Summary data, select the Detailed Views submenu.

Application Response Time Metrics

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 menu Analyze > Response Time. You can view response times for applications, networks, servers, and clients. To view detailed views of Response Time data, select the Detailed Views submenu.

After the NAM is started, these metrics will begin to populate.

Voice Signaling/RTP Stream Monitoring

After the NAM is started, voice signaling and RTP stream traffic will automatically start being monitored. The NAM enables you to monitor all RTP stream traffic among all SPANed traffic, without having to know the signalling traffic used in negotiating the RTP channels.

Note

This is not supported on the NAM on Nexus 1010 and WAAS VB.

When RTP Stream Monitoring is enabled, the NAM:
- Identifies all RTP streams among the SPANed traffic
- Monitors the identified RTP traffic
- 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 NAM 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 the 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 packet lost
  - Severe Concealment Seconds: Seconds in which there is more than 5% of packet lost

You can set up thresholds at Setup > Alarms > Thresholds.
You can define filter entries to narrow down to the subset of RTP streams so the NAM monitors only those RTP streams matching the filter criteria.

To verify that the voice signaling/RTP traffic has begun, choose Analyze > Media > RTP Streams or Analyze > Media > Voice Call Statistics.

**Traffic Usage Statistics**

The NAM provides traffic statistics broken out by application, host, conversation, VLAN, and DSCP code point. Summary dashboards show Top N charts broken out by these attributes, as well as detailed views in tabular form. Analysis dashboards show usage over time by one particular application, host, and so forth, as well as other interesting measurements for the particular element being analyzed over a user-specified period of time.

**Traffic**

The NAM menu selections for setting up Traffic are:

- **SPAN**, page 2-7
- **Data Sources**, page 2-13
- **Hardware Deduplication**, page 2-43

**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.

The following sections describe SPAN sessions on devices running the NAM:

- **About SPAN Sessions**, page 2-7
- **Creating a SPAN Session**, page 2-10
- **Editing a SPAN Session**, page 2-12
- **Deleting a SPAN Session**, page 2-13

---

**Note**

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

**About SPAN Sessions**

**Note**

This feature does not apply to all NAM hardware. For details, see the *NAM Compatibility Matrix* on Cisco.com.

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.
Chapter 2      Setting Up the Cisco NAM

Traffic

The NME-NAM device has two Gigabit Ethernet ports—an internal interface and an external interface. One of the two interfaces must be selected as the NAM management port for IP traffic (such as HTTP and SNMP). The 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.

NAM-1 devices can have only one active SPAN session. You can select a switch port or EtherChannel as the SPAN source; however, you may select only one SPAN type. NAM-2 and NAM-3 devices and switch software support two SPAN destination ports.

The SPAN session cannot be configured directly from the NAM user interface. Users can configure SPAN from the Nexus 7000 to the Prime NAM 2300 series appliances.

Before you can monitor data, you must direct specific traffic flowing through a switch to the NAM for monitoring purposes. Use the methods described in Table 2-2, Methods of Directing Traffic.

Table 2-2   Methods of Directing Traffic

<table>
<thead>
<tr>
<th>Method</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch SPAN</td>
<td>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.</td>
</tr>
<tr>
<td>Switch Remote SPAN (RSPAN)</td>
<td>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.</td>
</tr>
<tr>
<td>NetFlow Data Export (NDE)</td>
<td>You can monitor NDE records directly from remote switches or routers. You must configure the NDE source to the NAM from a local switch or remote router, using the switch CLI. For received NDE traffic, a default site will be created including all interfaces from that device. See Sites, page 2-65. SPAN and NDE sources can be in effect simultaneously.</td>
</tr>
</tbody>
</table>

Note Starting with NAM release 5.x, in addition to being a consumer of NDE records, the NAM is also a producer of NDE data packets.

Table 2-3, SPAN Sources, describes the types of SPAN sources and the possible ways to configure them.

Table 2-3   SPAN Sources

<table>
<thead>
<tr>
<th>SPAN Source</th>
<th>Configured with one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any set of physical ports</td>
<td>• NAM (the NAM GUI)</td>
</tr>
<tr>
<td></td>
<td>• Switch CLI</td>
</tr>
<tr>
<td></td>
<td>• Supervisor portCopyTable (SNMP)</td>
</tr>
</tbody>
</table>
Table 2-3  SPAN Sources (continued)

<table>
<thead>
<tr>
<th>SPAN Source</th>
<th>Configured with one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any EtherChannel</td>
<td>• NAM (the NAM GUI)</td>
</tr>
<tr>
<td></td>
<td>• Switch CLI</td>
</tr>
<tr>
<td></td>
<td>• Supervisor portCopyTable (SNMP)</td>
</tr>
</tbody>
</table>

| Any set of VLANs configured on the local switch | NAM (the NAM GUI)                                         |
|                                                | • Switch CLI                                                |
|                                                | • Supervisor portCopyTable (SNMP)                           |

Table 2-4, Active SPAN Sessions Dialog, describes the fields on the SPAN Sessions window.

Table 2-4  Active SPAN Sessions Dialog

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Monitor session ID of the SPAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For switches running Cisco IOS software only.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of SPAN source</td>
</tr>
<tr>
<td>Source</td>
<td>Source of the SPAN session.</td>
</tr>
<tr>
<td></td>
<td>When creating a SPAN session, you can select all ports regardless of their state.</td>
</tr>
<tr>
<td></td>
<td>See Table 2-5, Possible SPAN States for a description of the possible SPAN states.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For switches running Cisco IOS software only.</td>
</tr>
<tr>
<td>Dest. Port</td>
<td>Destination port of the SPAN session.</td>
</tr>
<tr>
<td>Direction</td>
<td>Direction of the SPAN traffic.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the SPAN session:</td>
</tr>
<tr>
<td></td>
<td>• Active—Traffic at the SPAN source is being copied to the SPAN destination</td>
</tr>
<tr>
<td></td>
<td>• Inactive—Traffic at the SPAN source will not be copied to the SPAN destination</td>
</tr>
<tr>
<td></td>
<td>• Unknown—A mixture of both active and inactive status</td>
</tr>
<tr>
<td>Create</td>
<td>Create a SPAN session.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the current active SPAN session in the running-configuration to the startup-configuration for switches running Cisco IOS software only.</td>
</tr>
<tr>
<td>Add Dest. Port 1</td>
<td>Add NAM Port 1 to the selected SPAN session as a SPAN destination. This button is labeled Add Dest. Port on the NAM-1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Does not apply to the NAM appliances.</td>
</tr>
<tr>
<td>Add Dest. Port 2</td>
<td>Add NAM Port 2 to the selected SPAN session as a SPAN destination. This option is not available on the NAM-1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Does not apply to the NAM appliances.</td>
</tr>
</tbody>
</table>
Chapter 2      Setting Up the Cisco NAM

Note

IOS supports only two SPAN sessions, but each SPAN session can have more than one destination. The Add Dest. Port 1 and Add Dest. Port 2 buttons enable you to make the NAM dataport an additional destination to an existing local SPAN session.

Table 2-5 lists the possible SPAN states. The SPAN state displays in parenthesis in the Source - Direction column.

Table 2-5       Possible SPAN States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>SPAN source is valid and traffic from the source is being copied to the SPAN destination</td>
</tr>
<tr>
<td>NotInService</td>
<td>SPAN source might be valid, but traffic that appears at the source will not be copied to the SPAN destination</td>
</tr>
<tr>
<td>NotReady</td>
<td>The SPAN source might be valid, but traffic that appears at the source will not be copied to the SPAN destination</td>
</tr>
<tr>
<td>CreateAndGo</td>
<td>The SPAN source might be valid, but the SPAN source is being added to the SPAN session</td>
</tr>
<tr>
<td>CreateAndWait</td>
<td>The SPAN source might be valid, and the SPAN source is being added to the SPAN session</td>
</tr>
<tr>
<td>Destroy</td>
<td>The SPAN source is being removed from the SPAN session.</td>
</tr>
</tbody>
</table>

Creating a SPAN Session

To create a SPAN session on a switch:

Step 1  Choose Setup > Traffic > SPAN Sessions. The SPAN window displays as shown in Figure 2-1.
Step 2  Click the Create button.

The Create SPAN Session Dialog displays (the fields are described in Table 2-6, Create SPAN Session Dialog). Switch Port is the default for the SPAN Type.

Step 3  Select the appropriate information.

Table 2-6  Create SPAN Session Dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Session</td>
<td>Monitor session of the SPAN.</td>
</tr>
<tr>
<td>SPAN Type</td>
<td>• SwitchPort&lt;br&gt;• VLAN&lt;br&gt;• EtherChannel&lt;br&gt;• RSPAN VLAN&lt;br&gt;Note You can have only one RSPAN VLAN source per SPAN session.</td>
</tr>
<tr>
<td>SPAN Destination Interface</td>
<td>The NAM interface to which you want to send data.</td>
</tr>
<tr>
<td>Switch Module List</td>
<td>Lists all modules on the switch other than NAMs and Switch Fabric Modules.</td>
</tr>
<tr>
<td>SPAN Traffic Direction</td>
<td>• Rx&lt;br&gt;• Tx&lt;br&gt;• Both&lt;br&gt;Note Not applicable to RSPAN VLAN SPAN types.</td>
</tr>
<tr>
<td>Available Sources</td>
<td>SPAN sources that are available for the selected SPAN type.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds the selected SPAN source.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected SPAN source.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Removes all the SPAN sources.</td>
</tr>
<tr>
<td>Selected Sources</td>
<td>SPAN sources selected.</td>
</tr>
</tbody>
</table>
Setting Up the Cisco NAM

Traffic

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.

**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 2-7, Edit SPAN Session Dialog Box**.

**Step 3** Make the appropriate changes.
### Table 2-7  Edit SPAN Session Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Session</td>
<td>Monitor session of the SPAN.</td>
</tr>
<tr>
<td>SPAN Type</td>
<td>Type of SPAN session.</td>
</tr>
<tr>
<td>SPAN Destination interface</td>
<td>The NAM interface to which you want to send data.</td>
</tr>
<tr>
<td>Switch Module List</td>
<td>Lists all modules on the switch other than NAMs and Switch Fabric Modules.</td>
</tr>
<tr>
<td>SPAN Traffic Direction</td>
<td>Direction of the SPAN traffic.</td>
</tr>
<tr>
<td>Available Sources</td>
<td>SPAN sources available for the selected SPAN type.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds the selected SPAN source</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected SPAN source</td>
</tr>
<tr>
<td>Remove All</td>
<td>Removes all the SPAN sources</td>
</tr>
<tr>
<td>Selected Sources</td>
<td>SPAN sources selected.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Causes the NAM to update the switch configuration information with current configuration.</td>
</tr>
<tr>
<td>Submit</td>
<td>Saves changes.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clears all changes since previous Submit.</td>
</tr>
</tbody>
</table>

### Deleting a SPAN Session

**Note**  
This section does not apply to NME-NAM devices.

**Note**  
Deleting a SPAN session that has multiple SPAN destinations will affect all destinations.

To delete a SPAN session, select it from the Active SPAN Session dialog box, then click **Delete**.

### Data Sources

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

The NAM can be configured to “auto discover” data sources. You will be able to see details such as the IP addresses of devices sending packets to the NAM and the time that the last NDE packet was received. In NAM 4.x, this feature was called “Listening Mode”.

If you have configured sites (see Sites, page 2-65), 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.

We recommend that you configure a site using subnets instead of selecting a data source. See Specifying a Site Using Subnets, page 2-66.

The following sections contain configuration steps and specific information about the types of data sources available:

- SPAN, page 2-14
- ERSPAN, page 2-15
- VACL, page 2-22
- NetFlow, page 2-23
- WAAS, page 2-33
- Performance Agent, page 2-40

The NAM Data Sources page (Setup > Traffic > Data Sources) lists the data sources configured for that NAM.

The fields are explained in Table 2-8, NAM Data Sources.

### Table 2-8  NAM Data Sources

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>DATA PORT if it is a local physical port, or the IP address of the learned device.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The source of traffic for the NAM.</td>
</tr>
<tr>
<td></td>
<td>DATA PORT if it is a local physical port.</td>
</tr>
<tr>
<td></td>
<td>WAAS, ERSPAN, or NETFLOW if a data stream exported from the router or switch or WAE device.</td>
</tr>
<tr>
<td><strong>Activity</strong></td>
<td>Shows the most recent activity.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>ACTIVE or INACTIVE.</td>
</tr>
<tr>
<td><strong>Data Source</strong></td>
<td>The Name given to the data source.</td>
</tr>
<tr>
<td><strong>Data Source Details</strong></td>
<td>“Physical Port”, or information about the data source being Enabled or Disabled.</td>
</tr>
</tbody>
</table>

**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 or 7600 Routers chassis.

For more information about SPAN sessions, see SPAN, page 2-7.
### ERSPAN

This section describes how to configure Encapsulated Remote Switched Port Analyzer (ERSPAN) of the Catalyst 6500 switch or Cisco 7600 series router as a NAM data source. You configure ERSPAN as a NAM data source from the Catalyst 6500 switch or Cisco 7600 series router command line interface, not the NAM GUI.

As an ERSPAN consumer, the 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 NAM data ports. The NAM supports ERSPAN versions 1 and 3. Incoming ERSPAN data is parsed by the NAM, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

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

See the following sections about using ERSPAN as a data source:

- Enabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 2-15
- Enabling Autocreation of ERSPAN Data Sources Using the CLI, page 2-16
- Disabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 2-16
- Disabling Autocreation of ERSPAN Data Sources Using the CLI, page 2-16
- Creating ERSPAN Data Sources Using the Web GUI, page 2-17
- Creating ERSPAN Data Sources Using the CLI, page 2-17
- Deleting ERSPAN Data Sources Using the Web GUI, page 2-19
- Deleting ERSPAN Data Sources Using the CLI, page 2-19
- Configuring ERSPAN on Devices, page 2-20

#### 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 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 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. The 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 the 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 the 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 the **Auto Create** button 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 the **Submit** button.

### Enabling Autocreation of ERSPAN Data Sources Using the CLI

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

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

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

The 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 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 CLI

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

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

---

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

**Step 2** Click the **Auto Create** button 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 the **Submit** button.

### 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:

```bash
root@172-20-104-107.cisco.com# no autocreate-data-source erspan
ERSPAN data source autocreate successfully DISABLED
```
Creating ERSPAN Data Sources Using the Web GUI

To manually configure an ERSPAN data source on the NAM using 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 the Create button 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 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 the Submit button.

Creating ERSPAN Data Sources Using the CLI

To manually configure a ERSPAN data source on the 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 NAM and remember the device ID, and then you must create a data source entry using this device ID. In the 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):
Chapter 2  Setting Up the Cisco NAM

Traffic

root@172-20-104-107.cisco.com(sub-device-erspan)# address 192.168.0.1

**Step 4** 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-erspan)# show
DEVEICE TYPE : ERSPAN (Encapsulated Remote SPAN)
DEVICE ADDRESS : 192.168.0.1
```

root@172-20-104-107.cisco.com(sub-device-erspan)#

**Step 5** 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-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
```

root@172-20-104-107.cisco.com(sub-data-source-netflow)#

"
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 the 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 the **Delete** button along the bottom of the window.

### Deleting ERSPAN Data Sources Using the CLI

To delete an 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 autodisable option off, as described earlier.

Configuring ERSPAN on Devices

There are two ways to configure ERSPAN so that the NAM receives the data:

- Sending ERSPAN Data to Layer 3 Interface, page 2-20
- Sending ERSPAN Data Directly to the NAM Management Interface, page 2-21

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 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 data ports, which is the most efficient method and will not have any adverse effect on the NAM’s IP connectivity. Therefore, we recommend this method.

Sample Configuration of ERSPAN Source

monitor session 1 type erspan-source
  no shut
  source interface Fa 3/47
  destination

Chapter 2  Setting Up the Cisco NAM

Traffic

erspan-id N
  ip address aa.bb.cc.dd
  origin ip address ee.ff.gg.hh

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 1 type erspan-destination
  no shut
destination analysis-module 2 data-port 2
source
  erspan-id N
  ip address aa.bb.cc.dd

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 NAM to monitor and capture traffic of the Data Port 2 data source.

Sending ERSPAN Data Directly to the NAM Management Interface

To send the data directly to the 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 or Cisco 7600 series router, 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 2-17).

Note
This method causes the ERSPAN traffic to arrive on the 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
VACL

A VLAN access control (VACL) list can forward traffic from either a WAN interface or VLANs to a data port 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.

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)# vlan access-map wan 100
Cat6509(config)# match ip address 100
Cat6509(config)# action forward capture
Cat6509(config)# 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 NAM data port 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 the 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 172.20.122.226 on VLAN 1 is captured and forwarded to the NAM located in slot 3.

```
Cat6509#config terminal
```
```bash
Cat6509#(config)#access-list 100 permit ip any any
Cat6509#(config)#access-list 110 permit ip any host 172.20.122.226
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
```

## NetFlow

The NAM can function as a NetFlow consumer, a NetFlow producer, or both. For information about NAM as an NDE producer, see Configuring NetFlow Data Export, page 2-58.

As a consumer, the NAM can receive NetFlow packets on its management port 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 NAM data ports. The NAM understands NetFlow v1, v5, v6, v7, v8, and v9. Incoming NetFlow data is parsed by the NAM, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

For the NAM to receive NetFlow packets from an external switch or router, that device must be configured by export flow records to the NAM’s IP address and the correct UDP port number. The default port number on which the NAM listens for NetFlow packets is port 3000. This can be modified using the NAM CLI, but the important point is that the same port must be configured on the NAM and the exporting device(s). 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 2-23
- Understanding NetFlow Flow Records, page 2-24
- Managing NetFlow Data Sources, page 2-24
- Configuring NetFlow on Devices, page 2-25

### Understanding NetFlow Interfaces

To use a device as an NDE data source for the NAM, you must configure the device itself to export NDE packets to UDP port 3000 on the NAM. You might need to configure the device itself on a per-interface basis. An NDE device is identified by its IP address. In the NAM, the default UDP port of 3000 can be changed with a NAM CLI command (see Configuring NetFlow on Devices, page 2-25).

You can define additional NDE 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 NDE devices may export information pertaining to any or all of their individual interfaces. The 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**

An NDE 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 NDE feature incompatibility with your Cisco IOS version, or because of an NDE 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 2-2, shows a sample network configuration with a NetFlow router.

![Sample NetFlow Network](image)

Table 2-9, Reporting Flow Records lists the reported flows if NetFlow is enabled on interface a.

**Table 2-9 Reporting Flow Records**

<table>
<thead>
<tr>
<th>Input Interface</th>
<th>Output Interface</th>
<th>Are Flows Reported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>Y</td>
</tr>
<tr>
<td>a</td>
<td>c</td>
<td>Y</td>
</tr>
<tr>
<td>b</td>
<td>c</td>
<td>N</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>N</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>N</td>
</tr>
<tr>
<td>c</td>
<td>b</td>
<td>N</td>
</tr>
</tbody>
</table>

**Managing NetFlow Data Sources**

A data source entry must exist on the NAM in order for it to accept NetFlow records from an external device. Data source entries may be created manually using the 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 NDE traffic to the NAM when the first packet is received.

Autocreated NetFlow data sources will be assigned a name in the format NDE-<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 “NDE-192.168.0.1-ID-12” for device 192.168.0.1 sending NDE 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.

### Configuring NetFlow on Devices

The configuration commands for NetFlow devices to export NDE packets to the 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 information, see your device documentation.

#### For Devices Running Cisco IOS

**Step 1** Select the interface on which you wish to turn on routed flow cache.

```
Prompt# configure terminal
Prompt(config)# interface <type slot/port>
Prompt(config-if)# ip route-cache flow
```

**Step 2** Export routed flow cache entries to UDP port 3000 of the NAM.

```
Prompt(config)# ip flow-export destination <NAM IP address> 3000
```

**Note** Newer Cisco IOS images support Flexible NetFlow. This feature allows you to configure a router or switch to export certain fields of network traffic flow to the NAM. From the NAM’s perspective, it is not practical to have incomplete flow information, such as flow records with no packet count but byte count. Another exactly is flow records without a source address but with a destination address. These incomplete flow records make the presentation in the NAM GUI confusing. Cisco highly recommends that you export full flow (for example, NDEv5 format) information to the NAM.

#### For Devices Supporting Multi-Layer Switching Cache Running Cisco IOS

**Step 1** Select the version of NDE.

```
Prompt(config)# mls nde sender version <version-number>
```

**Note** The NAM supports NDE versions 1, 5, 6, 7, 8, and 9 aggregation caches.

**Step 2** Select NDE flow mask.

```
Prompt(config)# mls flow ip full
```
Step 3  Enable NetFlow export.

Prompt(config)# mls nde sender

Step 4  Export NetFlow to UDP port 3000 of the NAM.

Prompt(config)# ip flow-export destination <NAM IP address> 3000

For Devices Supporting NDE v8 Aggregations Running Cisco IOS

Step 1  Select a v8 aggregation.

Prompt(config)# ip flow-aggregation cache <aggregation-type>

Where aggregation-type can be:
- destination-prefix
- source-prefix
- protocol-port
- prefix

Step 2  Enable the aggregation cache.

Prompt(config-flow-cache)# enable

Step 3  Export the flow entries in the aggregation cache to NAM UDP port 3000.

Prompt(config-flow-cache)#export destination <NAM address> 3000

For Devices That Support NDE Export From Bridged-Flow Statistics

Step 1  Enable bridged-flows statistics on the VLANs.

Prompt>(enable) set mls bridged-flow-statistics enable <vlan-list>

Step 2  Export the NDE packets to UDP port 3000 of the NAM

Prompt>(enable) set mls nde <NAM address> 3000

For NAMs Located in a Device Slot

If the NAM is located in one of the device slots, the device can be set up to export NDE packets to the NAM.

Step 1  Select the version of NDE.

Prompt>(enable) set mls nde version <nde-version-number>

Step 2  Select NDE flow mask to be full.

Prompt>(enable) sel mls nde full

Step 3  Enable NDE export.
Chapter 2  Setting Up the Cisco NAM

Enabling Autocreation of NetFlow Data Sources Using the Web GUI

To configure the NAM to automatically create data sources when it receives NDE 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 the **Auto Create** button on the bottom left of the window.

**Step 3**  Check the **Netflow** check box to toggle autocreation of NDE data sources on.

**Step 4**  Click the **Submit** button.

Enabling Autocreation of NetFlow Data Sources Using the CLI

Configuration of the autocreate feature is also possible using the NAM CLI. Remember that the autocreate feature is turned ON by default, so in most cases these steps are not necessary.

To configure the NAM to automatically create data sources when it receives NDE 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
NDE data source autocreate successfully ENABLED
```

The 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 NDE packets sent to the NAM. If the same device happens to send NDE 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 the **Auto Create** button on the bottom left of the window.

**Step 3**  Uncheck the **Netflow** check box to toggle autocreation of NDE data sources off.

**Step 4**  Click the **Submit** button.

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
```

Prompt>(enable) set mls nde enable

**Step 4**  Export the NDE packets to the NAM.

Prompt>(enable) set snmp extendedrmon netflow enable <NAM-slot>
Creating NetFlow Data Sources Using the Web GUI

To manually configure a NetFlow data source on the NAM using 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 the **Create** button along the bottom of the window.

**Step 3** From the Type drop-down list, choose “NetFlow.”

**Step 4** Enter the IP address of the device that will export NDE to the NAM (required).

**Step 5** Give the Data Source a name. This name will appear anywhere there is a Data Source drop-down list.

**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 NDE records exported by the device will be grouped into the same data source, regardless of the Engine ID populated in the NDE 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 NDE records. For example, on some Cisco routers, NDE 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, the 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 2-10, SNMP Credentials.

**Table 2-10 SNMP Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode: No Auth, No Priv</strong></td>
<td>SNMP will be used in a mode with no authentication and no privacy.</td>
</tr>
<tr>
<td><strong>Mode: Auth, No Priv</strong></td>
<td>SNMP will be used in a mode with authentication, but no privacy.</td>
</tr>
<tr>
<td><strong>Mode: Auth and Priv</strong></td>
<td>SNMP will be used in a mode with both authentication and privacy.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Enter a username, which will match the username configured on the device.</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up the Cisco NAM

Traffic

Table 2-10  SNMP Credentials (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Password</td>
<td>Enter the authentication password associated with the username that was configured on the device. Verify the password.</td>
</tr>
<tr>
<td>Auth Algorithm</td>
<td>Choose the authentication standard which is configured on the device (MD5 or SHA-1).</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Enter the privacy password, which is configured on the device. Verify the password.</td>
</tr>
<tr>
<td>Privacy Algorithm</td>
<td>Enter the privacy algorithm, which is configured on the device (AES or DES).</td>
</tr>
</tbody>
</table>

Step 10  Click the Submit button.

Creating NetFlow Data Sources Using the CLI

To manually configure a NetFlow data source on the 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 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 NDE 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

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 NDE records from the device will be received and accepted by the 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 autocrreation feature is turned on, and the device continues to send NDE packets to the NAM, the data source will be recreated again automatically as soon as the next NDE 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 the Delete button along the bottom of the window.

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 NDE packets to the NAM, the data source (and device entry) will be re-created again automatically as soon as the next NDE 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. Table 2-11, Device System Information Dialog Box describes the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware description of the device.</td>
</tr>
<tr>
<td>Device Software Version</td>
<td>The current software version running on the device.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Total time the device has been running since the last reboot.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the device.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact information for the device.</td>
</tr>
<tr>
<td>SNMP read from device</td>
<td>SNMP read test result. For the local device only.</td>
</tr>
</tbody>
</table>

If the device is sending NetFlow Version 9 (V9) and the NAM has received the NDE templates, then a V9 Templates button appears below the Device System Information window.

Note

NetFlow v9 templates do not appear in all NDE packets. When there are no templates, the V9 Templates button does not appear.

WAAS

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. 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 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.
Chapter 2  Setting Up the Cisco NAM

- 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 document:

*Cisco Wide Area Application Services Configuration Guide, OL-16376-01*

**Response Time Monitoring from WAAS Data Sources**

The NAM processes the TCP flow data exported from the WAAS and performs application response time (ART) calculations and reports. You use the NAM GUI to create a WAAS data source to monitor WAAS traffic statistics. In addition to ART, NAM monitors and reports other traffic statistics of the WAAS data sources including application, host, and conversation information.

The NAM provides different ART metrics by collecting data at different points as packets flow along their paths. The NAM provides five different collection points, each represented by a WAAS data source. Figure 2-3, “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 2-3  WAAS Data Sources (Data Collection Points)**

You can use the NAM GUI to configure data sources at the locations in the network described in Table 2-12, WAAS Data Collection Points.
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 2-38.

### Monitoring Client Data Sources

By monitoring the TCP connections between the client and the WAE device (Client segment in Figure 2-3), 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 2-3), 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 2-3), 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

---

### Table 2-12 WAAS Data Collection Points

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to NAM for monitoring. To monitor this point, configure a Client data source.</td>
</tr>
<tr>
<td>Client WAN</td>
<td>This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring. To monitor this point, configure a Client WAN data source.</td>
</tr>
<tr>
<td>Server WAN</td>
<td>This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to NAM for monitoring. To monitor this point, configure a Server WAN data source.</td>
</tr>
<tr>
<td>Server</td>
<td>This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to NAM for monitoring. To monitor this point, configure a Server data source.</td>
</tr>
<tr>
<td>Passthrough</td>
<td>This setting configures the WAE device to export the TCP flows that are passed through unoptimized.</td>
</tr>
</tbody>
</table>
Note

NAM measures Network Time by monitoring the TCP three-way handshake between the devices.

Deployment Scenarios

Table 2-13, WAAS Data Source Configurations lists six different deployment scenarios you might consider to monitor the optimized traffic on your WAAS network. Scenario #1 is typical when using NAM-1, -2 or -3 blades. Scenario #2 is typical when using NME-NAM devices.

### Table 2-13 WAAS Data Source Configurations

<table>
<thead>
<tr>
<th>Deployment Scenario</th>
<th>Edge WAE Data Source</th>
<th>Core WAE Data Source</th>
</tr>
</thead>
</table>
| 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 | Client |
|                     |                      |                      |       | |
| 5                   | • Clients and servers in the edge (branch) and the core (data center)  
                     • NAM in the core | Client | Client |
|                     |                      |                      |       | Server |
|                     |                      |                      |       | Client WAN |
|                     |                      |                      |       | Server WAN |
| 6                   | • Clients and servers in the edge (branch) and the core (data center)  
                     • NAM in the edge | Client | Client |
|                     |                      |                      |       | Server |

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.

Starting with Cisco Prime Network Analysis Module 5.1(3), the Cisco NAM is accessible from within the Central Manager interface. The Cisco NAM integration with WAAS Central Manager provides for easier viewing of NAM reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments.
Chapter 2      Setting Up the Cisco NAM

Below is a standard configuration workflow that you can follow. Prerequisites are that the WAAS Central Manager is installed and functional, and the NAM (device or virtual blade) is installed and functional.

---

**Step 1** From the WAAS Central Manager, configure the 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 Sites, page 2-65 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 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 NAM IP. Segments are automatically selected (enabled only if the NAM is configured). The NAM will start to compute baseline ART, protocol distribution, and Top Talkers.

**Step 8** Turn on WAAS optimization. See WAN Optimization, page 3-17 for more information.

**Step 9** Turn on the Flow Agent and identify the servers to monitor to get ART improvements.

---

Managing WAAS Devices

Before you can monitor WAAS traffic, you must first configure the WAAS device to export WAAS flow record data to the NAM using the WAAS command-line interface (CLI) flow monitor command like the following:

```
flow monitor tcpstat-v1 host <nam IP address>
flow monitor tcpstat-v1 enable
```

After you enable flow export to the 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 2-38, 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. Starting with Prime NAM 5.1(3), the Cisco NAM GUI is accessible from within the WAAS Central Manager interface. For more information about WAAS Central Manager, refer to the 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 WAAS Monitored Servers, page 2-88, for more detailed information.

For more information about WAAS and configuring the WAAS components, see the document:
Adding Data Sources for New WAAS Device

Adding Data Sources for New WAAS Device

The 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 the 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 Managing WAAS Devices, page 2-37, 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 the NAM:

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

**Step 2** Click **Create**.

The 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 2-12).

**Step 6** (Optional) If Response Time Export is enabled (see Custom Export, page 2-62), and you want to export passthrough traffic, check the **Passthrough Response Time** check box.

**Step 7** Click **Submit** to add the new WAAS custom data source.

Editing WAAS Data Sources

The 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 the 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 the **Edit** button.

You can configure the WAAS data sources to monitor the following WAAS segments as shown in Figure 2-3, 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 NAM for monitoring.
- **Client WAN**—This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring.
- **Server WAN**—This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to NAM for monitoring.
- **Server**—This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to NAM for monitoring.

SPAN data sources might take the place of the WAE Server data sources listed in Table 2-13. 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 the NAM is configured to export data to an External Response Time Reporting Console, such as the NetQos Super Agent.

**Step 3**
To export WAAS pass-through data to the External Response Time Reporting Console, check the **Passthrough Response Time** check box.

---

**Note**
WAAS pass-through data is not analyzed by the NAM.

See Custom Export, page 2-62 for more information.

---

**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 the **Delete** button.

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 the NAM to configure newly discovered WAE devices using a predefined configuration template using the NAM Auto Config option.

---

**Note**
If most of your WAE devices are edge WAE, you might want to set the auto config 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 the Auto Create button.  
The 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 2-38, for more information.

Performance Agent

The Performance Agent (PA) can monitor interface traffic and collect, analyze, aggregate, and export key performance analytics to a Cisco Network Analysis Module for further processing and GUI visualization. PA integration with NAM enables you to have a lower cost way to gain visibility into Application Response Time at the branch. NAM integration with PA also reduces complexity of needing to manage a separate NAM product within the branch.

PA has the ability to consolidate and filter information before it is exported, ensuring that only contextually-required data is exported and consumed versus all data. As an example, NetFlow Export supports a number of functions, including response time and traffic analysis. Instead of exporting multiple different flows, the PA has the intelligence to consolidate, filter, and export flow data that addresses the particular user’s need. Besides consolidating and filtering information, PA’s mediation capabilities also includes the ability to use key Cisco IOS-embedded functionality (for example, Embedded Event Manager, or Class-Based QoS) to enrich both PA functionality and router value.

The NAM provides five different collection points, each represented by a data source. Figure 2-4, “Performance Agent Data Sources (Data Collection Points)”, shows an example of the data collection points. The solid line represents WAAS FA flows from the Core WAE. The broken line represents data exported from an ISR device only.

![Performance Agent Data Sources (Data Collection Points) Diagram]

You can use the NAM GUI to configure data sources at the locations in the network described in Table 2-14, PA Data Collection Points. The NAM autocreates a data source for each PA optimization segment: Client, Client WAN, Passthrough, and Non-optimized.
Chapter 2  Setting Up the Cisco NAM

Traffic

You can also configure a data source to use Export Passthrough data.

For information about configuring PA data sources, continue to Managing ISR PA Devices, page 2-41.

Managing ISR PA Devices

Before you can monitor PA traffic, you must first configure the device to export PA flow record data to the NAM. Refer to the “Configuring Other System Settings” chapter of the Cisco Wide Area Application Services Configuration Guide (Software Version 4.3.1):


After you enable flow export to the NAM, ISR devices will export data to the NAM, and they will be detected and automatically added to the NAM’s device list.

This section contains the following topics about using the NAM GUI to manage data sources:

- Enabling Autocreation of PA Data Sources Using the NAM GUI, page 2-41
- Creating PA Data Sources Using the NAM GUI, page 2-42
- Disabling Autocreation of PA Data Sources Using the NAM GUI, page 2-43

### Enabling Autocreation of PA Data Sources Using the NAM GUI

To configure the NAM to automatically create data sources when it receives PA 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Setup &gt; Traffic &gt; NAM Data Sources</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Auto Create</strong> button on the bottom left of the window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the <strong>PA</strong> check box to toggle autocreation of PA data sources on.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the <strong>Submit</strong> button.</td>
</tr>
</tbody>
</table>

Table 2-14  PA Data Collection Points

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to NAM for monitoring. To monitor this point, configure a Client data source.</td>
</tr>
<tr>
<td>Client WAN</td>
<td>This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring. To monitor this point, configure a Client WAN data source.</td>
</tr>
<tr>
<td>Passthrough</td>
<td>This is traffic that can be optimized, but is not because the traffic exceeds the WAAS Express’ capability.</td>
</tr>
<tr>
<td>Non-Optimized</td>
<td>This is traffic that is not optimized, because this kind of traffic is not defined in the optimization policy.</td>
</tr>
</tbody>
</table>
Creating PA Data Sources Using the NAM GUI

To manually configure a PA data source on the NAM using the GUI, for example if the autocreation feature is turned OFF, use the following steps. 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 the **Create** button along the bottom of the window.

**Step 3** From the Type drop-down list, choose “PA.”

**Step 4** Enter the IP address of the device that will export PA to the NAM (required).

**Step 5** Click the “Version v1/v2c” radio button 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 PA packets to the NAM. Enter the same string in the “Verify” field. If you chose SNMPv1 or v2c, skip to **Step 8**.

**Step 6** Click the “Version v3” radio button if SNMP v3 will be used to communicate with the device.

**Step 7** Click the “Mode” radio button that corresponds with the desired credentials, and fill in the necessary fields. If valid SNMP credentials are provided, the 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 2-15, **SNMP Credentials** for more information.

**Table 2-15 SNMP Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode: No Auth, No Priv</strong></td>
<td>SNMP will be used in a mode with no authentication and no privacy.</td>
</tr>
<tr>
<td><strong>Mode: Auth, No Priv</strong></td>
<td>SNMP will be used in a mode with authentication, but no privacy.</td>
</tr>
<tr>
<td><strong>Mode: Auth and Priv</strong></td>
<td>SNMP will be used in a mode with both authentication and privacy.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Enter a username, which will match the username configured on the device.</td>
</tr>
<tr>
<td><strong>Auth Password</strong></td>
<td>Enter the authentication password associated with the username that was configured on the device. Verify the password.</td>
</tr>
<tr>
<td><strong>Auth Algorithm</strong></td>
<td>Choose the authentication standard which is configured on the device (MD5 or SHA-1).</td>
</tr>
<tr>
<td><strong>Privacy Password</strong></td>
<td>Enter the privacy password, which is configured on the device. Verify the password.</td>
</tr>
<tr>
<td><strong>Privacy Algorithm</strong></td>
<td>Enter the privacy algorithm, which is configured on the device (AES or DES).</td>
</tr>
</tbody>
</table>

**Step 8** Click the **Test Connectivity** button. You will be shown a success or failure message.

**Step 9** Click the **Submit** button.
Disabling Autocreation of PA Data Sources Using the NAM GUI

Step 1 Choose **Setup** > **Traffic** > **NAM Data Sources**.
Step 2 Click the **Auto Create** button on the bottom left of the window.
Step 3 Uncheck the **PA** check box to toggle autocreation of PA data sources off.
Step 4 Click the **Submit** button.

Hardware Deduplication

**Note** This section applies only to Cisco NAM 2320, 2220, and 2204 appliances.

Prime NAM 5.1(3) supports hardware-based detection of duplicate packets and allows you to configure a single deduplication filter across all adapter ports.

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**.

The Deduplication window displays.

Step 2 Check the **Enabled** check box to enable packet deduplication.

Step 3 Enter a value in the Time Window (1-127 in milliseconds) for the search or buffer period.

The value you set in the Time Window indicates the length of time (n milliseconds) in which two packets can be considered duplicates. If the Time Window is 100 ms but two identical packets arrive 120 ms apart, the second packet would not be dropped. If the identical packets arrive 80 ms apart, the second packet would be dropped.

Step 4 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 5 Click **Submit** to enable the settings you have entered, or click **Reset** to cancel any change.
Alarms

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 the NAM to notify you, and how you want to be notified.

This is the order that you will typically follow for setting up alarms and alarm thresholds:

**Step 1**
Depending on the type of alarm action you would like to configure, define the way you would like to be notified (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 NAM menu selections for setting up Alarms are:

- Alarm Actions, page 2-44
- Thresholds, page 2-47

This section also contains a User Scenario, page 2-56.

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.

**Note**
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.

When you choose Setup > Alarms > Actions, you will see events that have been created. See Table 2-16, Alarm Configuration for descriptions of the fields.
Alarm Action Configuration

When a threshold’s rising water mark is crossed, the alarm condition is met. This will trigger the alarm action to take effect. The NAM supports the following alarm actions:

- **E-mail syslog**: An alarm action that e-mails the syslog content of the alarm condition. To avoid e-mail flooding the network, the NAM does not send more than five e-mails in any given hour.

- **Trap**: An alarm action that sends NAM trap message to one or more trap servers. Any trap server that has the same community string will receive the trap message. The NAM use Cisco Syslog MIB in the trap message. To avoid trap flooding, the NAM’s limit is ten trap messages per interval.

- **Remote syslog**: An alarm action that sends syslog messages to remote syslog servers. The NAM’s limit is ten syslog messages per interval to avoid flooding the network.

- **Trigger capture**: An alarm action to start or stop a pre-defined capture session.

The NAM supports any combination of the above four actions in one alarm condition.

To configure e-mail alarm actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Setup &gt; Alarms &gt; Actions.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click the Create button.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter a Name for the action (up to 63 characters).</td>
</tr>
</tbody>
</table>

### Table 2-16: Alarm Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name given to the alarm at setup.</td>
</tr>
<tr>
<td>Email</td>
<td>If turned on, will show “Enable”. If not turned on, will show “Disable.” E-mail server settings are configured on Administration &gt; System &gt; E-Mail Setting.</td>
</tr>
<tr>
<td>Trap</td>
<td>If configured, will show “Community: xxxxx” as configured on Administration &gt; System &gt; SNMP Trap Setting. If not configured, will be blank.</td>
</tr>
<tr>
<td>Trigger Capture</td>
<td>If configured, will show “Session: xxxxx” as configured on Capture &gt; Packet Capture/Decode &gt; Sessions. If no captures are configured, will be blank.</td>
</tr>
<tr>
<td>Syslog Remote</td>
<td>If turned on, will say “Enable”. If turned off, will say “Disable.” Settings configured on Administration &gt; System &gt; Syslog Setting.</td>
</tr>
<tr>
<td>Status</td>
<td>“Missing Trap” means that the trap configured for that alarm action has been deleted. “OK” means the Alarm action was successfully created.</td>
</tr>
</tbody>
</table>
Step 4  Choose the type of alarm action:
  
  - **Email**: The NAM will use the e-mail address configured in *Administration > System > E-Mail Setting*. NAM alarm mail is sent as a result of NAM alarms, not router or switch alarms.

  The NAM sends up to five e-mails per hour per function (traffic and NDE, 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 NAM does not have any alarms.

  If the NAM is planning to send you many alarm messages, the e-mail may state, for example, “5 of 2,345 alarm messages.”

  - **Trap**: Choose the SNMP community where you would like traps to be sent. The NAM will use the community configured in *Administration > System > SNMP Trap Setting*. After the “Community” field appears, choose the community string from the drop-down list.

  - **Trigger Capture**: 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” or “Stop” radio button.

  - **Syslog**: This will log syslog messages. The default setting is to log syslog messages locally to the NAM. If you want to log syslog messages to remote servers, set up the destination information at *Administration > System > Syslog Setting*.

Step 5  Click **Submit**.

The Alarm Action table displays the newly configured action in its list.

---

### Editing Alarm Actions

To edit an alarm action:

Step 1  Choose **Setup > Alarms > Actions**.

The Alarm Action table displays any configured Alarms.

Step 2  Choose the alarm event you want to modify, and click the **Edit** button.

---

### Deleting Alarm Actions

To delete an alarm:

Step 1  Choose **Setup > Alarms > Actions**.

The Alarm Action table displays any configured Alarms.

Step 2  Choose the alarm event you want to remove, and click the **Delete** button.
Thresholds

The NAM will inspect incoming performance records and apply a configured set of thresholds to the most recent interval of data to detect threshold violations. You can use the NAM GUI to set up alarm thresholds for variables with values that trigger alarms.

**Note**

You could receive two alarms for the same occurrence if both the source and the destination are in the same site.

The NAM Threshold Alarms window (Setup > Alarms > Thresholds) displays already-configured thresholds. If you hover over the arrow next to the threshold Name, as shown in Figure 2-5, a detailed view of the selected threshold will display.

**Figure 2-5**  NAM Threshold Window and Threshold Details

![NAM Threshold Window and Threshold Details](image)

See Table 2-17, Threshold Configuration for descriptions of the fields on the Threshold window.

**Table 2-17**  Threshold Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the threshold.</td>
</tr>
<tr>
<td>Type</td>
<td>You can configure eight types of thresholds. See Figure 2-6 for a complete list.</td>
</tr>
<tr>
<td>Application</td>
<td>Application associated with this threshold.</td>
</tr>
<tr>
<td>Site</td>
<td>Site associated with this threshold.</td>
</tr>
<tr>
<td>Host</td>
<td>Host associated with this threshold.</td>
</tr>
<tr>
<td>Severity</td>
<td>High or Low (user-configured classification). These alarms are displayed on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary). You can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Action</td>
<td>Rising action and Falling action (if configured). Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both.</td>
</tr>
<tr>
<td>Status</td>
<td>“OK” if configuration is complete. Otherwise, the issue will be listed (for example, “Missing Src Site”).</td>
</tr>
</tbody>
</table>
You can set up alarm thresholds by defining threshold conditions for monitored variables on the NAM. Figure 2-6 shows the threshold types you can configure:

**Figure 2-6 Create Threshold**

<table>
<thead>
<tr>
<th>Setup &gt; Alarms &gt; Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
</tr>
</tbody>
</table>

To see the specific steps required for setting up a threshold type, choose the type from the list below:

- Setting Host Thresholds, page 2-48
- Setting Conversation Thresholds, page 2-49
- Setting Application Thresholds, page 2-50
- Setting Response Time Thresholds, page 2-51
- Setting DSCP Thresholds, page 2-52
- Setting RTP Stream Thresholds, page 2-52
- Setting Voice Signaling Thresholds, page 2-54
- Setting NDE Interface Thresholds, page 2-55

### Setting Host Thresholds

**Step 1** Choose Setup > Alarms > Thresholds.

**Step 2** Click the **Create** button and choose the **Host** tab.

**Step 3** The Host Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-18, Host Alarm Thresholds describes the fields available on this window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Give the Host Alarm Threshold a name.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>Choose a site from the list. See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Choose an application from the list. You can enter the first few characters to narrow the selection in the drop-down list.</td>
</tr>
<tr>
<td><strong>DSCP</strong></td>
<td>Choose a DSCP value from the list. You can enter the first few characters to narrow the selection in the drop-down list.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt;Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>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 Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up the Cisco NAM

Alarms

Setting Conversation Thresholds

Step 1  Choose Setup > Alarms > Thresholds.

Step 2  Click the Create button and choose the Conversation tab.

Step 3  The Conversation Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-19, Conversation Alarm Thresholds describes the fields available in this window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the Conversation Alarm Threshold a name.</td>
</tr>
<tr>
<td>Application</td>
<td>Choose an application from the list. You can start typing the first few characters to narrow the list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Source Site/Host</td>
<td>Make a selection from the drop-down lists, or leave as “Any.” See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Destination Site/Host</td>
<td>Make a selection from the drop-down lists, or leave as “Any.” See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the lists, choose a Rising action and a Falling action (optional). See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>Conversation Metrics (per second)</td>
<td>Choose from one of the six metrics, and then enter a Rising threshold and a Falling threshold.</td>
</tr>
</tbody>
</table>

Table 2-18  Host Alarm Thresholds (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Metrics (per second)</td>
<td>Choose the type of metric from the list, and then enter a value for a Rising threshold and a Falling threshold.</td>
</tr>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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.
Alarms

Table 2-19  Conversation Alarm Thresholds (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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 the Create button and choose the Application tab.

Step 3  The Application Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-20, Application Alarm Thresholds describes the fields available in this window.

Table 2-20  Application Alarm Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the Application Alarm Threshold a name.</td>
</tr>
<tr>
<td>Site</td>
<td>Choose a site from the list. See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Application</td>
<td>Choose an application from the list. You can start typing the first few characters to narrow the list.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Choose a DSCP value 0-63, or Any.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the lists, choose a Rising action and a Falling action (optional). See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>Application Metrics (per second)</td>
<td>Choose Bits or Packets, and then enter a Rising threshold and a Falling threshold.</td>
</tr>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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 Response Time Thresholds**

**Step 1**  Choose **Setup > Alarms > Thresholds**.

**Step 2**  Click the **Create** button and choose the **Response Time** tab.

**Step 3**  The Response Time Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-21, **Response Time Thresholds** describes the fields available in this window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the Response Time Alarm Threshold a name.</td>
</tr>
<tr>
<td>Application</td>
<td>Choose an application from the list. You can start typing the first few characters to narrow the list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (<strong>Monitor &gt; Overview &gt;Alarm Summary</strong>), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Client Site/Host</td>
<td>Make a selection from the lists. See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Server Site/Host</td>
<td>Make a selection from the lists, or leave as “Any.” See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the lists, choose a Rising action and a Falling action (optional). See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>Response Time Metrics</td>
<td>Choose a metric from the list, and then enter a Rising threshold and a Falling threshold. For the Packets and Bits-related metrics, the entry is per second. For the time-related metrics, the unit is ms.</td>
</tr>
</tbody>
</table>

**Add Metrics (button)**  Click the **Add Metrics** button to add another row.

**Delete (button)**  Click the **Delete** button to remove that Metrics row.

**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 the Create button and choose the DSCP tab.
Step 3 The DSCP Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-22, DSCP Alarm Thresholds describes the fields available in this window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the DSCP Alarm Threshold a name.</td>
</tr>
<tr>
<td>Site</td>
<td>Choose a site from the list. See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Chose a DSCP value from the list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the drop-down lists, choose a Rising action and a Falling action (optional).</td>
</tr>
<tr>
<td>DSCP Metrics (per second)</td>
<td>Choose one of the metric types from the list, and then enter a Rising threshold and a Falling threshold.</td>
</tr>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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

Step 1 Choose Setup > Alarms > Thresholds.
Step 2 Click the Create button and choose the RTP Streams tab.
Step 3  The RTP Stream Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-23, RTP Streams Thresholds describes the fields available in this window.

Table 2-23  RTP Streams Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the RTP Streams Alarm Threshold a name.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Codec</td>
<td>Choose a Codec from the list.</td>
</tr>
<tr>
<td>Source Site/Host</td>
<td>Make a selection from the drop-down lists, or leave as “Any.” See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the drop-down lists, choose a Rising action and a Falling action (optional). See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>RTP Stream Metrics</td>
<td>Choose a metric from the list:</td>
</tr>
<tr>
<td></td>
<td>• Jitter: Variation of packet arrival time compare to expected arrival time.</td>
</tr>
<tr>
<td></td>
<td>• Adjusted packet loss percent: Percent of packet loss which includes packets actually lost and packets that arrived beyond the NAM expected buffering capability of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Actual packet loss percent: Percent of packets that the NAM has never seen.</td>
</tr>
<tr>
<td></td>
<td>• MOS: Mean opinion score that is composed of both jitter and adjusted packet loss.</td>
</tr>
<tr>
<td></td>
<td>• Concealment seconds: Number of seconds in which the NAM detected packets lost.</td>
</tr>
<tr>
<td></td>
<td>• Severe concealment seconds: Number of seconds in which the NAM detected packets lost of more than 5%.</td>
</tr>
</tbody>
</table>

Enter a Rising threshold and a Falling threshold.

Add Metrics (button) Click the Add Metrics button to add another row.

Delete (button) Click the Delete button to remove that Metrics row.

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 the NAM to monitor voice call quality. When Cisco Call 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. The 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 the Create button and choose Voice Signaling tab.

Step 3  The Voice Signaling Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-24, Voice Signaling Thresholds describes the fields available under the Voice Signaling Metrics drop-down menu.

Table 2-24  Voice Signaling Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the Voice Signaling Alarm Threshold a name.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>Choose a Rising action and a Falling action from the lists (optional). See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>Voice Signaling Metrics</td>
<td>Choose Jitter to enable an alarm when the NAM detects jitter to be more than the value set here. Check Packet Loss % to enable an alarm when the NAM detects Packet Loss percentage to be outside of the values you entered.</td>
</tr>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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 NDE Interface Thresholds

Step 1  Choose Setup > Alarms > Thresholds.

Step 2  Click the Create button and choose the NDE Interface tab.

The NDE Interface Alarm Threshold Configuration window displays. The fields are described in Table 2-25, NDE Interface Alarm Thresholds.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the NDE Interface Alarm Threshold a name.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Choose a data source from the list.</td>
</tr>
<tr>
<td>Interface</td>
<td>Choose an interface from the list.</td>
</tr>
<tr>
<td>Direction</td>
<td>Choose Ingress or Egress.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard</td>
</tr>
<tr>
<td></td>
<td>(Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High,</td>
</tr>
<tr>
<td></td>
<td>Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>Choose a Rising action and a Falling action from the lists (optional).</td>
</tr>
<tr>
<td></td>
<td>See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>NDE Interface Metrics</td>
<td>Choose Bits or Packets, and enter a Rising and Falling threshold.</td>
</tr>
<tr>
<td>(per second)</td>
<td>Add Metrics (button) Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

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 an Alarm Threshold

To edit an alarm threshold:

Step 1  Choose Setup > Alarms > Thresholds.

The Thresholds table displays.

Step 2  Select the alarm to edit, then click Edit.

The dialog box displays for the type of alarm; for example, “Host Threshold.”
**Deleting a NAM Threshold**

To delete a NAM alarm threshold, simply select it from the Alarms table, then click **Delete**. Click **OK** to confirm deletion, or click **Cancel** to leave the configuration unchanged.

**User Scenario**

If you want the NAM to notify you of any violations of Response Time metrics for a particular server, and then initiate a packet capture, complete the following steps:

**Step 1** Set up the e-mail and capture settings.
   a. Choose **Administration > System > E-Mail Setting** to define the e-mail settings.
   b. Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session for this particular server.

**Step 2** Define an Alarm Action.
   a. Choose **Setup > Alarms > Actions**.
   b. Click the **Create** button.
   c. Enter a Name.
   d. Check the **Email** check box.
   e. Check the **Trigger Capture** check box, choose the session you created in **Step 1** from the drop-down menu, and select the Start or Stop radio button.
   f. Click the **Submit** button.

**Step 3** Define the Threshold for this alarm.
   a. Choose **Setup > Alarms > Thresholds**.
   b. Click the **Create** button.
   c. Choose the Response Time tab.
   d. Give the Response Time Alarm Threshold a Name, and choose the Application and Severity.
   e. Choose the server from the Host drop-down list.
   f. Choose the action you created in **Step 2**, define the metrics for the thresholds, and click the **Submit** button.
Data Export

The NAM selections for setting up Data Export are:

- **NetFlow**, page 2-57
- **Scheduled Exports**, page 2-60
- **Custom Export**, page 2-62

NetFlow

NetFlow collects traffic statistics by monitoring packets that flow through the device and storing the statistics in the NetFlow table. NDE converts the NetFlow table statistics into records, and exports the records to an external device, which is called a NetFlow collector. The NAM sends out NDE packets only in NDE v9 format.

There are currently six record types (or templates) that NAM exports (four in Core Stats, one in ART):

- Application
- Host
- Client Server Response Time
- Application Conversations
- Network Conversations
- RTP Metrics

The NDE data is exported in a fixed selection of aggregated data records that are shipped with the product. This part of the NDE descriptor defines what is to be exported:

- Record Type
- Period (in minutes)
- NetFlow options selector

After you select the Record Type, you will make selections for Filters. The purpose of the Filter is to restrict the set of exported records to the subset matching the filter's conditions;

- Depending on which fields are contained in the specified record type, the filter can specify conditions on site, application (whenever applicable), and host (or server, or client, depending on record type)
- The semantics of multiple conditions is conjunctive; for example, if filter specifies “siteA” and “app1,” then the values in exported records will have to match both “siteA” and “app1.”
- Filter specification is optional, and by default all fields can be assumed as having value of Any
- The host (if applicable, or server, or client, depending on record type) allows multiple values to be selected. If multiple values are specified, for example “host1, host2”, then the NAM assumes “host1 or host2.”

The following sections describe setting up NetFlow Data Export:

- **Viewing Configured NetFlow Exports**, page 2-58
- **Configuring NetFlow Data Export**, page 2-58
- **Editing NetFlow Data Export**, page 2-60
Viewing Configured NetFlow Exports

To view already-configured NetFlow Exports:

**Step 1** Choose **Setup > Data Export > NetFlow**.

**Step 2** The NetFlow Exports window appears (shown in Figure 2-7).

![NetFlow Exports Window](image)

Already defined NetFlow Exports will be listed. If you hover over the “quick view” arrow icon next to the Record Type, as shown in Figure 2-5, a detailed view of the filter details of the selected NetFlow export will display.

The fields are described in Table 2-26.

Configuring NetFlow Data Export

To configure NetFlow Data Export:

**Step 1** Choose **Setup > Data Export > NetFlow**.

**Step 2** Click the **Create** button.

**Step 3** At the NetFlow Export Configuration window, fill in the fields. See Table 2-26, **NetFlow Exports Fields** for field descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP Address</td>
<td>The IP address of the device to be exported to. Only IPv4 addresses are supported.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The port number of the device to be exported to. Valid characters: 1-9. Length: Min 1, Max 65535.</td>
</tr>
</tbody>
</table>
### Table 2-26  NetFlow Exports Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Record Type</td>
<td>The record types supported by NAM for NetFlow are:</td>
</tr>
<tr>
<td></td>
<td>- Application</td>
</tr>
<tr>
<td></td>
<td>- Host</td>
</tr>
<tr>
<td></td>
<td>- ART Client Server Application</td>
</tr>
<tr>
<td></td>
<td>- Application Conversations</td>
</tr>
<tr>
<td></td>
<td>- Network Conversations</td>
</tr>
<tr>
<td></td>
<td>- RTP Metrics</td>
</tr>
<tr>
<td>Export Interval (min)</td>
<td>Uses only short-term aggregation interval.</td>
</tr>
<tr>
<td>Options (button)</td>
<td>The NetFlow option selection contains a set of check boxes. These allow independent selections of on or off settings for individual NetFlow options, which can be exported in addition to the NDE packets with data and templates, as follows:</td>
</tr>
<tr>
<td></td>
<td>- Mapping of integer application ID values into application names (as strings)</td>
</tr>
<tr>
<td></td>
<td>- Mapping of integer site ID values into site names and descriptions (as strings)</td>
</tr>
<tr>
<td></td>
<td>If there are several NetFlow Export Descriptors defined for the same destination, then the last user’s selection of option exports flags is enforced on all descriptor instances that exist for the same export destination.</td>
</tr>
<tr>
<td>Filter</td>
<td>After you choose the Export Record Type (above), the Filter menus populate depending on your selection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Site</strong>: List of created sites for the NAM (configured in Setup &gt; Network &gt; Sites). Select <strong>Any</strong> to use any of the selections for that parameter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Application</strong>: All applications created on the NAM (configured in Setup &gt; Classification &gt; Applications). Select <strong>Any</strong> to use any of the selections for that parameter.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Source</strong>: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Sources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Destination</strong>: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Destinations.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Host</strong>: List of available hosts. Click the right arrow to add it to the list of Chosen Hosts. If more than one host is selected, the filter will apply to records with the value being one of the selected set.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Client</strong>: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Clients.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong>: List of available servers. Click the right arrow to add it to the list of Chosen Servers.</td>
</tr>
</tbody>
</table>

**Note**  When you choose a record type with two sites (for example serverSite and clientSite in Client Server Response Time), the value specified by the filter will apply to either of these fields. If a certain site is chosen, then the filter will match records having the specified value in any of the site fields.

---

**Chapter 2      Setting Up the Cisco NAM**

**Data Export**
Step 4  Click the **Submit** button to save the configuration, or click the **Reset** button to clear the fields, or click the **Cancel** button to exit without configuration.

---

**Editing NetFlow Data Export**

To edit NetFlow Data Export:

---

**Step 1**  Choose **Setup > Data Export > NetFlow**.

**Step 2**  Highlight the export you want to edit and click the **Edit** button.

**Step 3**  Make the desired changes.

**Step 4**  Click:

- The **Submit** button to submit the edits
- The **Reset** button to clear the changes you made
- The **Cancel** button to close the dialog box and return to the previous window.

---

**Scheduled Exports**

You can set up scheduled jobs that will generate a daily report at a specified time, in the specified interval, and then e-mail it to a specified e-mail address. You can also obtain a report on the spot by clicking on the **Preview** button, rather than wait for the scheduled time. This report can also be sent after you preview it.

At the **Setup > Data Exports > Scheduled Export** window, you will only be able to edit or delete an already-configured scheduled export. The creation of a Scheduled Export can only be done from a “Monitor” or “Analyze” window.

Scheduled Export is not supported on all NAM 2000 series appliances. For details, see the *Release Notes for Cisco Prime NAM*.

To set up a Scheduled Export:

---

**Step 1**  In most windows under the “Monitor” or “Analyze” menus, the Interactive Report is available on the left side. Click the **Export** button in the Interactive Report box.

**Step 2**  Choose the Export Type (Daily or Weekly).

**Step 3**  Choose the Export Time (when you would like the report delivered to you): Day and Hour.

**Step 4**  Choose the Report Time (if Daily) or the Data Time Range (if Weekly). This is the interval of time you would like measured.

- The Report Time for a daily report is restricted to the current 24 hours.
- The Report Time for a weekly report is always from 17:00 to 17:00, for however many days chosen.

For example:

- If you choose Export Type “Weekly,” Data Time Range “Last 2 Days,” and Export Time: Day “Wednesday” and Hour “13:00,” the report will show data from Sunday at 17:00 to Tuesday at 17:00.
If you choose Export Time: Day “Wednesday” and Hour “18:00,” the report will show data from Monday at 17:00 to Wednesday at 17:00.

**Step 5** Enter the e-mail address to which you would like the report delivered.

**Step 6** Choose the delivery option (HTML or CSV).

**Step 7** Enter the report description, which will appear at the end of the filename of the report delivered to you.

**Step 8** Click:

- The **Reset** button to clear the values in the dialog box
- The **Preview** button to preview the report
- The **Submit** button to submit the request for the scheduled job
- The **Cancel** button to close the dialog box and return to the previous window

---

**Editing a Scheduled Export**

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Highlight the job you would like to edit.

**Step 3** Click the **Edit** button.

**Step 4** Modify the information as desired. In this window, you can only change the Email, Delivery Option (HTML or CSV), and Report Description.

**Step 5** Click:

- The **Submit** button to submit the request for the scheduled job
- The **Reset** button to clear the values in the dialog box
- The **Cancel** button to close the dialog box and return to the previous window.

---

**Deleting a Scheduled Export**

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Highlight the job you would like to delete.

**Step 3** Click the **Delete** button.

**Step 4** Click **OK** to confirm, or click **Cancel** to return to the previous window without deleting the job.
Custom Export

You can enable Custom Export to send response time data to an external reporting console such as NetQoS SuperAgent.

After you enable Custom Export, you may also want to enable the “Export Passthrough Response Time” option when creating a WAAS Data Source (Setup > Traffic > NAM Data Sources > Auto Create).

Custom Export is not supported on all NAM 2000 series appliances. For details, see the Release Notes for Cisco Prime NAM.

To enable the NAM to export response time data to an external console:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the NAM GUI, choose <strong>Setup &gt; Data Export &gt; Custom Export</strong>. The Response Time Export window displays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Check the <strong>Enable Export</strong> check box.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the IP address of the external reporting console in the IP Address field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the UDP port number of the external console (blank is default).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Optionally, click <strong>Export Non-WAAS Traffic</strong>. This enables the export of SPAN and other data as well as WAAS traffic.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Submit</strong> to enable traffic export, or click <strong>Reset</strong> to clear the changes from the window.</td>
</tr>
</tbody>
</table>

Managed Device

A managed device is the device on which SPAN is configured, and where system health ifTable statistics are polled via SNMP.

The NAM menu selections for setting up Managed Devices are:

- **Device Information**, page 2-62
- **NBAR Protocol Discovery**, page 2-64

Device Information

To view the switch information, choose **Setup > Managed Device > Device Information**. The fields are described in **Table 2-27, Device Information**.

<table>
<thead>
<tr>
<th><strong>Table 2-27 Device Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>SNMP Test information</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Hardware</td>
</tr>
<tr>
<td>Supervisor Software Version</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up the Cisco NAM

Managed Device

Table 2-27  Device Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Uptime</td>
<td>Total time the device has been running.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of the device.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact name of the network administrator for the device.</td>
</tr>
<tr>
<td>SNMP read from switch</td>
<td>SNMP read test result.</td>
</tr>
<tr>
<td>SNMP write to switch</td>
<td>SNMP write test result.</td>
</tr>
<tr>
<td>Mini-RMON on switch</td>
<td>For Cisco IOS devices, displays the status if there are any ports with Mini-RMON configured (Available) or not (Unavailable).</td>
</tr>
<tr>
<td>NBAR on switch</td>
<td>Displays if NBAR is available on the device.</td>
</tr>
<tr>
<td>VLAN Traffic Statistics on Switch</td>
<td>Displays if VLAN data is Available or Unavailable.</td>
</tr>
</tbody>
</table>

Note  Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.

Note  For the NAM-1, -2, and -3 platforms, SNMPv3 is not required. SNMP requests and responses are communicated over an internal interface within the chassis, and SNMPv3 is not used.

This section describes how to set router/managed device parameters.

Note  This section applies to all NAM platforms except the NAM-1, NAM-2, and NAM-3 blades.

Step 1  Choose Setup > Managed Device > Device Information.

The Router System Information displays as shown in Table 2-28, Router/Managed Device System Information.

Table 2-28  Router/Managed Device System Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware description of the router.</td>
</tr>
<tr>
<td>Managed Device Software Version</td>
<td>Current software version of the router.</td>
</tr>
<tr>
<td>Managed Device System Uptime</td>
<td>Total time the switch has been running.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of the router.</td>
</tr>
<tr>
<td>Contact</td>
<td>Name of the network administrator for the router.</td>
</tr>
<tr>
<td>Managed Device</td>
<td>IP address of the router.</td>
</tr>
</tbody>
</table>
Step 2  Click the Test Connectivity button to perform an SNMP test. Click Close when finished.

Step 3  Click Submit to submit the information and close the window.

## NBAR Protocol Discovery

**Note**

NBAR is supported on ISR routers and switches with the Catalyst 6500 Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) running IOS 12.2(18)ZY (or later).

To set up NBAR Protocol Discovery, choose **Setup > Managed Device > NBAR Protocol Discovery**. From the NBAR Protocol Discovery window, you can view the NBAR Status information and enable or disable NBAR on all interfaces.

You must enable the NBAR Interfaces feature for the NAM to provide information about ethernet ports.

**Note**

If your switch does not support NBAR, a message displays indicating that NBAR is not supported on your switch.
If NBAR Protocol Discovery is enabled, the NBAR Interfaces window lists known interfaces by name and type. *Table 2-29, NBAR Interface Details* describes the fields in the window.

<table>
<thead>
<tr>
<th>Field / Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (check box)</td>
<td>Check indicates that NBAR is enabled.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Name of the 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 Gi1/2/1 to represent a Gigabit port on switch 1, module 2, port 1.</td>
</tr>
<tr>
<td>Interface Description</td>
<td>Description of the interface.</td>
</tr>
</tbody>
</table>

To narrow the list of interfaces, choose “Interface Name” or “Interface Description” from the drop-down list, enter any part of the interface name or description in the text box, and click the **Filter** button. To clear the Filter text box, click **Clear**. To return to showing all interfaces, check the **All** check box and click the **Submit** button.

Check the check box to enable an interface, and then click the **Submit** button.

The **Save** button will save the router’s running configuration to startup configuration.

**Network**

The NAM menu selections for setting up the Network are:

- **Sites**, page 2-65
- **NDE Interface Capacity**, page 2-71
- **DSCP Groups**, page 2-71

**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 analysis data to a specific city, a specific building, or even a specific floor of a building, you can use the Sites function.

*Note* If there are multiple data sources configured for the same site, the same traffic may be accounted for more than once, resulting in inflated traffic statistics. For example, if the NAM is configured to receive SPAN traffic for a particular site, and also is receiving Netflow records for that same site, they will both be combined in the traffic statistics. In this case, if you then want to only see the statistics for a particular data source, you would need to use the Interactive Report window on the left side of the window to specify both the Site and Data Source.
The site definition is very flexible and can accommodate various scenarios. The site definition is used not only for viewing of data, but for data export and data retention as well. Normally, a site is defined by its subnet(s), but a site can also be defined using the following rules:

- Subnet (IP address prefix)
- Subnet from a data source
- Subnet from a given VLAN of a SPAN data source
- WAE device serving the site

The preferred way to define sites is using subnets, and should be used whenever possible.

Note

The same rule cannot be defined in multiple sites.

Note

If you are configuring a WAAS device, you will need to add WAAS servers to the NAM. See Auto Create of New WAAS Devices, page 2-39.

See the following sections to set up sites:

- Definition Rules, page 2-66
- Viewing Defined Sites, page 2-67
- Defining a Site, page 2-68
- Editing a Site, page 2-70

Definition Rules

Specifying a Site Using Subnets

Normally, subnets alone are sufficient to define a site. For example:

Site Data-Center = subnet 172.20.0.0/16

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 or VLANs can be used to differentiate the subnets. For example:

Site NewYork = subnet 10.11.0.0/16 from "NDE-NewYork" data source.
Site LosAngeles = subnet 10.11.0.0/16 from "NDE-LosAngeles" data source.
Site Sale-Dept = subnet 10.11.0.0/16 from VLAN 10 of "DATA PORT 1" data source.
Site Finance-Dept = subnet 10.11.0.0/16 from VLAN 12 of "DATA PORT 1" data source.

Specifying a Site Using WAE devices (WAAS Data Sources)

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.

Note

We recommend that you use subnets to specify WAAS-optimized sites. Use this method only if the site’s subnets cannot be determined.
Specifying a Site Using Multiple Rules

You can define a site using a combination of multiple rules described above. 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 NDE 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.

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 SPAN1 = SiteA
1.2.3.0/24 from SPAN1 = SiteB

Using a prefix is the preferred method. Data source and VLAN are 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/VLAN). In the following two scenarios, the first would receive the higher priority.

1.2.3.0/24 from SPAN1 = Site A
1.2.0.0/16 from SPAN1 = 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 SPAN1 = Site A
1.2.3.0/24 (any datasrc) = Site D

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 2-30, Sites Window.

Table 2-30  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of what the site includes.</td>
</tr>
<tr>
<td>Rule</td>
<td>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).</td>
</tr>
<tr>
<td>Status</td>
<td>Shows if the site is Enabled or Disabled.</td>
</tr>
</tbody>
</table>

Defining a Site

The “Definition Rules” section on page 2-66 gives specific information about various scenarios. To set up a Site or Sites:

Step 1    Choose **Setup > Network > Sites.**

Step 2    Click the **Create** button.

Step 3    The Site Configuration window appears. Enter a Name, Description, Subnet, Data Source, and/or VLAN as appropriate.
See Figure 2-8 for an example.

**Figure 2-8 Site Configuration Window**

![Site Configuration Window](image)

The fields are defined below in Table 2-31, Site Configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique text string for naming a site.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional text string for describing site.</td>
</tr>
<tr>
<td>Disable Site (check box)</td>
<td>If you check this checkbox, the NAM 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.</td>
</tr>
<tr>
<td>Subnet</td>
<td>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 NAM to look for subnets in the traffic. See the next section, Subnet Detection.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Specify the data source where the site traffic is coming from. Leave this field blank if the site traffic can come from multiple data sources.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Specify the VLAN where the site traffic is coming from. Leave this field blank if the site traffic can come from multiple VLANs.</td>
</tr>
</tbody>
</table>

*Note: The VLAN selection is not enabled for NDE and WAAS data sources.*
Step 4  
Click the **Submit** button.

---

**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.

---

**Subnet Detection**

When you click the **Detect** button at **Setup > Network > Sites > Sites Configuration**, the NAM will look for subnets detected within in the past hour. See **Table 2-32, Subnet Detection** for information about the fields.

**Table 2-32  Subnet Detection**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the bit mask is 32 or less, the NAM will detect an IPv4 subnet. If the bit mask is between 33 and 64, then it will detect an IPv6 subnet.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Choose the data source in which you would like to detect subnets.</td>
</tr>
<tr>
<td>Interface</td>
<td>Choose the interface in which you would like to detect subnets.</td>
</tr>
<tr>
<td>Filter Subnets Within Network</td>
<td>Enter an IPv4 or IPv6 address</td>
</tr>
<tr>
<td>Unassigned Site (check box)</td>
<td>The “Unassigned” site includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.</td>
</tr>
</tbody>
</table>

When you click the **Detect** button, the NAM will find those that meet the criteria that you entered.

**Editing a Site**

You can edit sites that have been created. Note that 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 the **Edit** button.

**Step 4**  
Edit the desired field.

**Step 5**  
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.
NDE Interface Capacity

After you have set up NetFlow data sources (see NetFlow, page 2-23), 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 NAM to calculate interface utilization on the NDE Interface Traffic Analysis window (Analyze > Traffic > NDE Interface). Otherwise, the NAM can only display the throughput of the interface, but cannot show its utilization.

You can click Edit to edit the interface. You can edit the name (for example, WAN link to Boston) and speed of the interface.

The interface name and speed will be automatically discovered by the NAM if you configure the router’s SNMP credentials in Setup > NAM Data Sources > Create > Type: NETFLOW.

To add an interface, continue to Creating an NDE Interface, page 2-71.

Creating an NDE Interface

To add an interface, at the NDE Interface Capacity window (Setup > Network > NDE Interface Capacity), click the Add button. Then fill in the fields as described in Table 2-33, Add NDE Interface.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Enter the IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>ifIndex</td>
<td>Unique identifying number associated with a physical or logical interface. Valid characters: 0-9.</td>
</tr>
<tr>
<td>ifName</td>
<td>Name of the interface. Valid characters are A-Z, a-z, 0-9</td>
</tr>
<tr>
<td>ifSpeed(Mbps)</td>
<td>An estimate of the interface’s current bandwidth in bits per second.</td>
</tr>
</tbody>
</table>

Note

It is normally not necessary to manually create NDE interfaces. They will be discovered automatically when the device sends NDE packets to the NAM.

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 or more 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:
These topics help you set up and manage the DSCP groups:

- Creating a DSCP Group, page 2-72
- Editing a DSCP Group, page 2-73
- Deleting a DSCP Group, page 2-73

## Creating a DSCP Group

To create a DSCP Group:

**Step 1** Choose **Setup > Network > DSCP Groups**.

The DSCP Groups table displays.

**Step 2** Click the **Create** button.

The DSCP Group Configuration window displays.

**Step 3** Fill in the fields as described in Table 2-34, DSCP Group Setup Dialog Box.

### Table 2-34 DSCP Group Setup Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the profile.</td>
<td>Enter the name of the profile you are creating. The maximum is 64 characters.</td>
</tr>
<tr>
<td>Label Format</td>
<td>DSCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>AF / EF / CS</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Bit Field</td>
<td>Six bits in the IP header of a packet. See Table 2-35.</td>
</tr>
</tbody>
</table>

Table 2-35, DSCP Group Label Formats shows the available formats and associated values.

### Table 2-35 DSCP Group Label Formats

<table>
<thead>
<tr>
<th>DSCP Format (DSCP 0 through DSCP 63)</th>
<th>AF/EF/CS Format</th>
<th>Bit Field Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP 0</td>
<td></td>
<td>000000</td>
</tr>
<tr>
<td>DSCP 8</td>
<td>CS1</td>
<td>000100</td>
</tr>
<tr>
<td>DSCP 10</td>
<td>AF11</td>
<td>0001010</td>
</tr>
<tr>
<td>DSCP 12</td>
<td>AF12</td>
<td>0001100</td>
</tr>
<tr>
<td>DSCP 14</td>
<td>AF13</td>
<td>0001110</td>
</tr>
<tr>
<td>DSCP 16</td>
<td>CS2</td>
<td>0010000</td>
</tr>
</tbody>
</table>
Table 2-35  DSCP Group Label Formats (continued)

<table>
<thead>
<tr>
<th>DSCP Format (DSCP 0 through DSCP 63)</th>
<th>AF/EF/CS Format</th>
<th>Bit Field Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP 18</td>
<td>AF21</td>
<td>010010</td>
</tr>
<tr>
<td>DSCP 20</td>
<td>AF22</td>
<td>010100</td>
</tr>
<tr>
<td>DSCP 22</td>
<td>AF23</td>
<td>010110</td>
</tr>
<tr>
<td>DSCP 24</td>
<td>CS3</td>
<td>011000</td>
</tr>
<tr>
<td>DSCP 26</td>
<td>AF31</td>
<td>011010</td>
</tr>
<tr>
<td>DSCP 28</td>
<td>AF32</td>
<td>011100</td>
</tr>
<tr>
<td>DSCP 30</td>
<td>AF33</td>
<td>011110</td>
</tr>
<tr>
<td>DSCP 32</td>
<td>CS4</td>
<td>100000</td>
</tr>
<tr>
<td>DSCP 34</td>
<td>AF41</td>
<td>100010</td>
</tr>
<tr>
<td>DSCP 36</td>
<td>AF42</td>
<td>100100</td>
</tr>
<tr>
<td>DSCP 38</td>
<td>AF43</td>
<td>100110</td>
</tr>
<tr>
<td>DSCP 40</td>
<td>CS5</td>
<td>101000</td>
</tr>
<tr>
<td>DSCP 46</td>
<td>EF</td>
<td>101110</td>
</tr>
<tr>
<td>DSCP 48</td>
<td>CS6</td>
<td>110000</td>
</tr>
<tr>
<td>DSCP 56</td>
<td>CS7</td>
<td>111000</td>
</tr>
</tbody>
</table>

**Step 4**  Click **Submit** to save your changes, or click **Reset** to cancel.

**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 one or more DSCP groups, simply select the profiles from the DSCP Groups table, then click **Delete**.
Classification

In Network Analysis Module release 5.x, the RMON-based protocol directory was replaced with a new application ID classification system. When defining applications, you will be able to view and select from a list of candidate IP addresses and port numbers for the traffic being analyzed.

The NAM enables the selection of the “better” application identifier, wherein “better” is defined as the deeper inspection to be used for application classification. You can also manually select the preferred inspection method.

For example, the NBAR Application ID inspection may report a “better” classification than the NAM’s Protocol Directory, and so you may want to use the NBAR Application ID instead.

The NAM also allows for the configuration of custom applications via the North Bound Interface (NBI). This is needed to ensure uniform application classification across a number of NAMs.

The menu selections for setting up Classification are:

- Applications, page 2-74
- Application Groups, page 2-77
- URL-Based Applications, page 2-78
- Encapsulations, page 2-81

Applications

The NAM recognizes an application on the basis of port number, port number range, stateful inspection of traffic (for example, voice signaling traffic or FTP), heuristics (for example, MS-RPC or SUN-RPC), or standardized application identifiers exported by Cisco platforms with NDE. If the 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.

The Applications window lists applications that have been set up for this NAM. To view the Applications window, choose Setup > Classification > Applications. Use this window to view and add proprietary applications, and edit the user-defined applications.

Figure 2-9 shows an example of what the window may look like.
Chapter 2  Setting Up the Cisco NAM

Classification

Table 2-36, Applications describes the fields on the Applications setup page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Standard protocols, or name given by the user (if user-created).</td>
</tr>
<tr>
<td>Protocol/Port</td>
<td>Application protocol and port.</td>
</tr>
<tr>
<td></td>
<td>The port is an arbitrary number you assign to handle the additional ports for</td>
</tr>
<tr>
<td></td>
<td>the protocol family. This protocol number must be unique so it does not</td>
</tr>
<tr>
<td></td>
<td>conflict with standard protocol/port assignments.</td>
</tr>
<tr>
<td></td>
<td>The port number range will vary depending on the protocol type selected.</td>
</tr>
<tr>
<td>Selector</td>
<td>An arbitrary number, unique within an engine-id. It will be automatically</td>
</tr>
<tr>
<td></td>
<td>assigned if left blank.</td>
</tr>
<tr>
<td></td>
<td>This allows you to configure applications consistently across multiple NAMs,</td>
</tr>
<tr>
<td></td>
<td>so that the same user-created application is exported with the same value.</td>
</tr>
<tr>
<td></td>
<td>This should be used when configuring the same custom applications on multiple</td>
</tr>
<tr>
<td></td>
<td>NAMs.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>Will show “Custom” if it was user-created.</td>
</tr>
<tr>
<td>Application Tag</td>
<td>Predefined for standard protocols.</td>
</tr>
<tr>
<td></td>
<td>For user-created, the application tag is a combination of the engine ID and</td>
</tr>
<tr>
<td></td>
<td>the Selector. The 32 bit is generated by using the engine ID as the highest</td>
</tr>
<tr>
<td></td>
<td>order byte, and the Selector makes up the other 3 bytes.</td>
</tr>
<tr>
<td>Description</td>
<td>Full name of the protocol.</td>
</tr>
<tr>
<td>Status</td>
<td>Active or Inactive.</td>
</tr>
</tbody>
</table>

This section provides the following procedures:

- Creating a New Application, page 2-75
- Editing an Application, page 2-76
- Deleting a Protocol, page 2-77
- Activate/Inactivate an Application, page 2-77

Creating a New Application

When defining applications, you will be able to view and select from a list of candidate IP addresses and port numbers for the traffic being analyzed. You can create additional ports to enable the NAM to handle additional traffic for standard applications.

To create a new application:

**Step 1** Choose Setup > Classification > Applications.

The Applications window displays.

**Step 2** Choose the type you would like to create and click Create.

The Application Configuration window displays.

**Step 3** Enter a name in the Name field.
Step 4  Enter a Selector value. This is an arbitrary number, unique within an engine-id. It will be 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.

Step 5  Choose a protocol family from the list:
- CISCO-SNAP
- DCE-RPC
- ETHER2
- IP
- LLC
- SCTP-PORT
- SCTP-PPI
- SUN-RPC
- TCP
- UDP

Choose the type of traffic you want to create the additional protocol to handle.

Step 6  Enter a port number; the range will vary depending on the protocol family selected. This 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.

Step 7  Click the right arrow to add the selections to the “Chosen Protocol/Port” list. To remove an item from that list, highlight it and click the left arrow.

Step 8  Repeat Step 4 through Step 7 as many times as desired.

Step 9  Click:
- The Submit button to create the new application.
- The Reset button to clear the values on the window.
- The Cancel button to close the window and return to the previous window.

Step 10 Use the pull-down menu to choose a Protocol Family.

Step 11 Enter an integer to use as the beginning port number for the protocol you want to create.
The range is 1-255 for IP and 1-65535 for TCP, UDP, and SCTP.

Step 12 Click the right arrow to add the port to the “Chosen Protocol/Port” field.

Step 13 Click Submit to create the new protocol ports, or click Cancel to clear the dialog of any characters you entered or restore the previous settings.

---

**Editing an Application**

In NAM you can only modify the user-defined applications, and not the standard 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 (you will only be able to change the name and protocol/port/port range).
Step 4 Do one of the following:
- To accept the changes, click Submit.
- To leave the configuration unchanged, click Cancel.
- To delete the protocol, click Delete.

Deleting a Protocol

To delete a protocol, simply select it from the Application Configuration window, then click Delete.

Activate/Inactivate an Application

To activate or inactivate a predefined application, choose the application and then click the Activate/Inactivate button. When you are prompted to confirm the selection, choose OK or Cancel.

An instance in which you may want to inactivate an application is when the same application appears in the list two times but under two different names, and you would like to hide one of them.

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 2-77
- Editing an Application Group, page 2-78
- Deleting an Application Group, page 2-78

Creating an Application Group

To create an application group:

Step 1 Choose Setup > Classification > Application Groups.
The Application Groups window displays.
Step 2 Click the Create button.
Step 3 Enter the name in the Application Group Name field.
Step 4 Use the next Application field and the Filter button to narrow the list of selectable applications.
Step 5 Select an application and click the Add button. Applications appear in the Selected Applications box.
You can select multiple applications at once by using the Shift button, and then click Add.

**Step 6**  
Click **Submit** to save your changes, or click **Reset** to cancel.

---

### Editing an Application Group

To edit an application group:

**Step 1**  
Choose **Setup > Classification > Application Groups**.

**Step 2**  
Select the Application Group by clicking the radio button, then click **Edit**.

**Step 3**  
Make the necessary changes, then click **Submit** to save your changes, or click **Reset** to cancel.

---

### Deleting an Application Group

To delete an application group, simply select the application and then click the **Delete** button. You can only delete one application group at a time.

---

### URL-Based Applications

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 application, in the order of the index, until a match is found. When a match is found, the remaining URL-based applications are not considered.

A URL consists of the following parts:

- a host
- a path
- an argument

For example, in the URL `http://host.domain.com/intro?id=123`:

- the **host** part is `host.domain.com`
- the **path** part is `/intro`
- the **argument** part is `?id=123`

In the configuration of an URL-based application, the path part and the argument path are combined and called the **path part**.

---

**Note**  
The match strings of the URL-based applications are POSIX-limited regular expressions.
A maximum of 64 URL-based applications can be defined.

To create a URL-based application from a collected URL:

**Step 1** Choose **Setup > Classification > URL-based Applications.**

**Step 2** Click **Create.**

The Create URL-based Application window displays.

Enter values in the fields according to **Table 2-37, URL-Based Applications.**

**Table 2-37 URL-Based Applications**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>A unique number (1-64) of each URL-based application. You can define up to 64 URL-based applications in NAM.</td>
</tr>
<tr>
<td>URL Host Part Match</td>
<td>Matching criteria in the host portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression(^1).</td>
</tr>
<tr>
<td>URL Path Part Match</td>
<td>Matching criteria in the path portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression(^1).</td>
</tr>
<tr>
<td>Content-Type Match</td>
<td>Matching criteria in the Content-Type field of the HTTP packets. This match is a POSIX Regular Expression(^1).</td>
</tr>
<tr>
<td>Protocol Description</td>
<td>Description of this URL-based application.</td>
</tr>
</tbody>
</table>

---

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").

**Step 3** Click:

- The **Submit** button to submit the request
- The **Reset** button to clear the values in the window
- The **Cancel** button to close the dialog box and return to the previous window

**Example**

After you click **Submit**, the NAM will have an application named “my_host HTTPserver.” It functions like any user-defined application in the NAM. The packets or octets counter is the number of HTTP packets that have the URL “HOST=my_host.mydomain.com.”
See Figure 2-10 for an example of creating a URL-based application.

**Figure 2-10 Example of Creating a URL-Based Application**

<table>
<thead>
<tr>
<th>Index (1 ... 64)</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Host Port Match</td>
<td>my_host.mydomain.com</td>
</tr>
<tr>
<td>URL Path Port Match</td>
<td></td>
</tr>
<tr>
<td>Content-Type Match</td>
<td></td>
</tr>
<tr>
<td>Protocol Description</td>
<td>my_host_HTTPserver</td>
</tr>
<tr>
<td><em>Fill in values then Apply →</em></td>
<td>Submit</td>
</tr>
</tbody>
</table>

### Editing a URL-Based Application

To edit URL-based applications:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Setup &gt; Classification &gt; URL-based Applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select a radio button and click Edit.</td>
</tr>
</tbody>
</table>

**Note**

When editing a URL-based application, the index can not be changed. To change the index (to change the order of execution) delete the URL-based application and recreate it.

Change the information as desired.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Click:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The Submit button to submit the request</td>
</tr>
<tr>
<td></td>
<td>• The Reset button to clear the values in the window</td>
</tr>
<tr>
<td></td>
<td>• The Cancel button to close the dialog box and return to the previous window</td>
</tr>
</tbody>
</table>

### Deleting a URL-based Application

To delete a URL-based application:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Setup &gt; Classification &gt; URL-based Applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the radio button for the item you would like to delete.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Delete button.</td>
</tr>
</tbody>
</table>
Encapsulations

Using Encapsulation gives you increased flexibility when trying to monitor (such as counting or grouping) different types of application traffic. The encapsulation settings affect how traffic of certain IP based tunneling protocols are treated in the NAM.

You can use the NAM to set up the way you monitor different types of encapsulation in network traffic for the following protocols:

- IPIP4—IP in IP tunneling
- GREIP—IP over GRE tunneling
- IPESP—IP with Encapsulating Security Payload
- GTP—GPRS (General Packet Radio Service) Tunneling Protocol
- IPIP6—IP in IP tunneling

To configure encapsulation:

**Step 1** Choose Setup > Classification > Encapsulations.

The Encapsulations configuration page appears.

**Step 2** Use the pull-down menu to choose the type of Encapsulation Configuration you want for each protocol.

- Application in Tunnel, Inner IP Addresses
  
  In default mode, the NAM uses Application in Tunnel, Inner IP Addresses. In this mode, the NAM will classify the application based on the payload of the tunneled traffic, and use the inner IP addresses (IP addresses of the traffic carried inside the tunnel) for reporting and capture.

- Application in Tunnel, Outer IP Addresses
  
  In the Application in Tunnel, Outer IP Addresses mode, the NAM will also classify the traffic based on the payload of the tunneled traffic, but use the outer IP addresses (the IP addresses of the tunnel endpoints) for reporting and capture.

- Tunnel as Application
  
  In the Tunnel as Application mode, the traffic will be classified as the tunnel protocol and the packet not further parsed. The outer IP addresses will be used in this case.

**Step 3** Click Submit to change the Encapsulation Configuration.

Click Reset to revert to the previous settings since the last Submit.

Monitoring

Before you can monitor data on the NAM, you must set up the data collections. The NAM menu selections for setting up Monitoring are:

- Aggregation Intervals, page 2-82
- Response Time, page 2-83
- Voice, page 2-84
- RTP Filter, page 2-85
Aggregation Intervals

The NAM has short-term and long-term aggregation intervals (this was referred to as long-term reporting in NAM 4.x). In NAM 5.x, the aggregated data will be 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. The 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 NAM long term data to only contain information for hosts classified to the user-defined sites. This check box only applies to the long term data; short term will 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 NAM database. See Table 2-38, Data Retention for information about data retention.

**Table 2-38 Data Retention**

<table>
<thead>
<tr>
<th></th>
<th>Short-Term Aggregated Data (Normal)</th>
<th>Short-Term Aggregated Data (Minimum)</th>
<th>Long-Term Aggregated Data (Normal)¹</th>
<th>Long-Term Aggregated Data (Minimum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1 and WS-SVC-NAM-2</td>
<td>24 hours</td>
<td>5 hours</td>
<td>30 days</td>
<td>10 days</td>
</tr>
<tr>
<td>All other platforms</td>
<td>72 hours</td>
<td>14 hours</td>
<td>100 days (with default polling interval)</td>
<td>30 days (with default polling interval)</td>
</tr>
</tbody>
</table>

1. Can depend on how the user configures the LT polling interval. The more frequent polling, the shorter the duration.

**Response Time**

To configure the timing parameters (or *buckets*) 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 milliseconds 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 the Configure Filter button to configure a filter.

**Step 4** Enter the Response Time settings as described in Table 2-39, Response Time Configuration Window.

**Table 2-39 Response Time Configuration Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RspTime1 (msec)</td>
<td>Upper response time limit for the first bucket</td>
<td>Enter a number in milliseconds. The default is 5.</td>
</tr>
<tr>
<td>RspTime2 (msec)</td>
<td>Upper response time limit for the second bucket</td>
<td>Enter a number in milliseconds. The default is 10.</td>
</tr>
<tr>
<td>RspTime3 (msec)</td>
<td>Upper response time limit for the third bucket</td>
<td>Enter a number in milliseconds. The default is 50.</td>
</tr>
<tr>
<td>RspTime4 (msec)</td>
<td>Upper response time limit for the fourth bucket</td>
<td>Enter a number in milliseconds. The default is 100.</td>
</tr>
<tr>
<td>RspTime5 (msec)</td>
<td>Upper response time limit for the fifth bucket</td>
<td>Enter a number in milliseconds. The default is 200.</td>
</tr>
<tr>
<td>RspTime6 (msec)</td>
<td>Upper response time limit for the sixth bucket</td>
<td>Enter a number in milliseconds. The default is 500.</td>
</tr>
<tr>
<td>Late RspTime (msec)</td>
<td>The maximum interval that the NAM waits for a server response to a client request</td>
<td>Enter a number in milliseconds. The default is 1000.</td>
</tr>
</tbody>
</table>
Step 5: Accept the default settings or change the settings to the values you want to monitor. Click **Submit** to save your changes, or click **Reset** to cancel.

---

**Voice**

After you set up the NAM to monitor voice data, you will be able to view the collected voice data under the **Analyze > Media** menu in the NAM. For more information on viewing the voice data, see Media, page 3-37.

**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 2-40, Voice Monitor Setup Window.

**Table 2-40  Voice Monitor Setup Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Monitoring</td>
<td>Enables voice monitoring</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables voice monitoring</td>
</tr>
<tr>
<td>MOS Values</td>
<td>Highest quality MOS score (5.0 being highest). The default value is 5.0.</td>
</tr>
<tr>
<td>Excellent</td>
<td>Quality less than excellent; MOS score ranges from this setting to less than excellent. The default value is 4.33.</td>
</tr>
<tr>
<td>Good</td>
<td>Quality less than good; MOS score ranges from this setting to less than good. The default value is 4.02.</td>
</tr>
<tr>
<td>Fair</td>
<td>Quality less than excellent; MOS score ranges from this setting to less than fair. The default value is 3.59.</td>
</tr>
</tbody>
</table>

**Table 2-41, Maximum and Default Voice/Video and RTP Stream Parameters per Platform** provides the maximum numbers allowed for various voice, video, and RTP streams depending on the NAM platform. The default values for each parameter are in parenthesis.

<table>
<thead>
<tr>
<th>Field</th>
<th>2x20 Appliance</th>
<th>2x04 Appliance</th>
<th>NAM-2(x)</th>
<th>NAM-1(x)</th>
<th>NME-NAM</th>
<th>NAM SRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Streams</td>
<td>4,000 (2000)</td>
<td>1,500 (750)</td>
<td>800 (400)</td>
<td>400 (200)</td>
<td>100 (50)</td>
<td>800 (400)</td>
</tr>
<tr>
<td>Max Active Calls</td>
<td>2,000 (1,000)</td>
<td>750 (375)</td>
<td>400 (200)</td>
<td>200 (100)</td>
<td>50 (25)</td>
<td>50 (25)</td>
</tr>
</tbody>
</table>

---
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.

Step 4
Click Submit to save your changes, or click Reset to cancel and revert to the previous settings.

**RTP Filter**

When the NAM is initially started, RTP stream traffic will automatically start being monitored. The NAM enables you to monitor all RTP stream traffic among all SPANed 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 the Submit button to apply the change.

To create an RTP filter:

**Step 1**
Choose Setup > Monitoring > RTP Filter.

**Step 2**
Click the Create button.

**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.

**URL**

The URL collection listens to traffic on TCP port 80 of a selected datasource 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 datasource 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).

The collection can be configured to collect all parts or it can configured to collect only some of the parts and ignore others.

<table>
<thead>
<tr>
<th>Field</th>
<th>2x20 Appliance</th>
<th>2x04 Appliance</th>
<th>NAM-2(x)</th>
<th>NAM-1(x)</th>
<th>NME-NAM</th>
<th>NAM SRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Phones</td>
<td>10,000 (5,000)</td>
<td>3,500 (1,750)</td>
<td>2,000 (1,000)</td>
<td>1,000 (500)</td>
<td>250 (125)</td>
<td>250 (125)</td>
</tr>
<tr>
<td>Phone History</td>
<td>25,000 (12,500)</td>
<td>7,000 (3,500)</td>
<td>5,000 (2,500)</td>
<td>2,500 (1,250)</td>
<td>600 (300)</td>
<td>600 (300)</td>
</tr>
</tbody>
</table>
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**.

The URL window displays.

**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 2-42, URL Collection Configuration Dialog Box**.

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
Check the check box for one of the following:

- Collect complete URL (Host, Path and Arguments)
- Collect Host only (ignore Path and Arguments)
- 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**.

The URL page (Figure 2-11) displays.

### Step 2
Change the information as described in **Table 2-42, URL Collection Configuration Dialog Box**.

### 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.

---

**Table 2-42 URL Collection Configuration Dialog Box**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source</td>
<td>Identifies type of traffic incoming from the application.</td>
<td>Select one of the options from the drop-down box.</td>
</tr>
<tr>
<td>Max Entries</td>
<td>Maximum number of URLs to collect.</td>
<td>Select one of the following options from the drop-down box:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1000</td>
</tr>
<tr>
<td>Match only</td>
<td>The application URL to match.</td>
<td>Optional parameter to limit collection of URLs that match the regular expression of this field.</td>
</tr>
</tbody>
</table>
Disabling a URL Collection

To disable a URL collection:

2. Uncheck the Enable check box.
3. Click Submit.

WAAS Monitored Servers

WAAS monitored servers specify the servers from which WAAS devices export traffic flow data to the NAM monitors. To enable WAAS monitoring, you must list the servers to be monitored by the NAM using the WAAS device's flow monitoring.

Note

The NAM is unable to monitor WAAS traffic until you set up WAAS monitored servers. The NAM displays status of WAAS devices as pending until you set up WAAS monitored servers.

This section contains the following topics:
- Adding a WAAS Monitored Server, page 2-88
- Deleting a WAAS Monitored Server, page 2-89

Adding a WAAS Monitored Server

To add a WAAS monitored server:

1. Choose Setup > Monitoring > WAAS Servers. The WAAS Servers page displays. Figure 2-12 shows an example of the WAAS Monitored Servers table.

![Figure 2-12 WAAS Monitored Servers Table](image)

2. Check the Filter Response Time for all Data Sources by Monitored Servers check box if you want the 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 NAM workload and to improve NAM overall performance.
Step 3  Click Add.
The Add WAAS Server(s) dialog box displays.
Step 4  Enter the server IP address in the Server Address field. You can paste multiple IP addresses here as well.
Step 5  Click Submit.

Deleting a WAAS Monitored Server

To delete a WAAS monitored server data source:

Step 1  Choose Setup > Monitoring > WAAS Servers.
The WAAS Servers page displays any WAAS monitored servers.
Step 2  Select the monitored WAAS server to delete, then click Delete.
A confirmation dialog displays to ensure you want to delete the selected WAAS monitored server.
Step 3  Click OK to delete the WAAS monitored server.
Cisco Prime Network Analysis Module 5.1(3) has two types of dashboards: One type is the “summary” views found under the Monitor menu, and the other type is the “over time” views found under the Analyze menu. The Monitor dashboards allow you to view 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.

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

This chapter contains the following sections:

- **Navigation**, page 3-2
- **Monitor**
  - Traffic Summary, page 3-4
  - Response Time Summary, page 3-5
  - Site Summary, page 3-6
  - Alarm Summary, page 3-6
- **Analyze**
  - Analyzing Traffic, page 3-9
  - WAN Optimization, page 3-17
  - Response Time, page 3-18
  - Managed Device, page 3-29
  - Media, page 3-37
Navigation

Context Menus

On most of the dashboards, you can left-click on the colored bar of data to get a context menu, with which you can get more detailed information about one particular application.

The description to the right of “Selected Application” in the menu shows what item you had clicked on (in the case above, “ftp”).

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.

Interactive Report

In most Monitor and Analyze windows, you can use the Interactive Report on the left to redefine the parameters of the information displayed in the dashboards. Click the Filter button to change the parameters of the information displayed in the charts.

You can choose from various parameters, such as the time interval for the data being displayed. An asterisk represents required fields.

The reporting time interval selection changes depending upon the dashboard you are viewing, and the NAM platform you are using:

- The NAM appliance supports the following short term intervals: Last 5 minutes, last 15 minutes, last 1 hour, last 4 hours, and last 8 hours.
- The Branch Routers (NME-NAM) support the following short term intervals: Last 5 minutes, last 15 minutes, and last 1 hour.
- The other platforms support the following short term intervals: Last 5 minutes, last 15 minutes, last 1 hour, and last 4 hours.
- The Long Term interval selections (Last 1 day, 1 week, and 1 month) are disabled from the following dashboards: RTP Streams, Voice Call Statistics, Calls Tables, RTP Conversations, Host Conversations, Conversations, and Response Time Details Views.
• Maximum interval for up to one hour is supported for the following dashboards: RTP Streams, Voice Call Statistics, Calls Tables, RTP Conversations, Host Conversations, Conversations, and Response Time Details Views.

The “From” and “To” fields are only enabled when the Time Range is set to “Custom.”

**Saving Filter Parameters**

After clicking the **Filter** button in the Interactive Report and selecting the desired parameters, you can then save these selections with the purpose of viewing that same data at a future time. Enter a name in the “Filter Name” field, as shown at the bottom of Figure 3-1. A filter will only be saved if a Filter Name is entered. Also, only saved filters are persisted across multiple login sessions. Click the **Submit** button.

![Figure 3-1 Saving Filter Information](image)

This filter is now saved and displayed underneath the Interactive Report, as shown in Figure 3-2. You can save up to five filters.

![Figure 3-2 Filter Parameters Accessible](image)
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 by Bits (or Bytes), Top N DSCP, and Top N VLAN being monitored on your network. It provides automonitoring of traffic from all potential data sources (for example, SPAN, NDE, 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, VLAN, or reporting time interval. 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.

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

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.

The charts shown on this dashboard are:

- **Top N Applications**
  The Top N Applications Chart enables you to view the traffic rate (bits per second or bytes per second) or traffic volume (bits or bytes), depending on the Interactive Report filter selection (data rate or cumulative, respectively). When you place your cursor over the colored bar, you will see the number of bits per second collected or the total bits over the last time interval. 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 Chapter 4, “Capturing and Decoding Packet Data” for more information about Capture).

- **Top N Application Groups**
  This chart shows a detailed analysis of the Top N application groups and the traffic rate or volume for this interval. 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.

- **Top N Hosts (In and Out)**
  This chart displays the traffic rate (bits per second or bits per second) or traffic volume (bytes or bits). To get more specific details about the host activity, left-click on the colored bar and make a selection. You can also choose “Capture” from the context menu to start a capture on this data (see Chapter 4, “Capturing and Decoding Packet Data” for more information about Capture).

- **IP Distribution by Bits (or Bytes)**
  This chart shows the percentages of bits being distributed to IP protocols (for example, IPv4 TCP).

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

- **Top N DSCP**
  This chart shows statistics for the top DSCP Aggregation Groups.

- **Top N VLAN**
  This chart shows the Top N VLAN statistics. In this chart, you may see VLAN 0, which is for traffic that does not have any VLAN tags. You can also use this value in Capture to do filtering.
If you left-click on a colored bar and choose “Capture” from the context menu, you can start a capture on this data (see Chapter 4, “Capturing and Decoding Packet Data” for more information about Capture).

To see a chart in table format, use the “View as Chart / View as Grid” toggle button on the bottom right corner of the chart. You can also click the “View as Image” button to view the image and save it as a PNG file.

When viewing the data as a Grid, the numbers will be 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.

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). In NAM 4.x, this was referred to as Intelligent Application Performance (IAP) analytics.

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, VLAN, 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 “View as Chart / View as Grid” toggle button on the bottom right corner of the chart. You can also click the “View as Image” button to view the image and save it as a PNG file.

The dashboard charts will show you the following information:

- **Top N Applications by Server Response Time**
  This chart displays the server response times for the applications in the site, data 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 is shown in microseconds.

- **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 is shown in microseconds.

- **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 is shown in milliseconds.

- **Top N Clients By Bits (or Bytes)**
  This chart displays the total bits or rate of traffic for the top clients.
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 Sites, page 2-65.

The charts displayed on the Alarm Summary dashboard are:

- **Top N Site Pairs by Traffic**
  This chart shows top site to site traffic.

- **Top N Sites by Average Transaction Time**
  This chart shows the average transaction time by site.

- **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.

- **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.

To see any of the charts in table format, use the “View as Chart / View as Grid” toggle button on the bottom right corner of the chart. You can also click the “View as Image” button to view the image and save it as a PNG file. The numbers will be formatted according to what you have configured in Administration > Settings > Preferences.

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 Alarms, page 2-44.

**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.
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).

NDE 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 NDE Interface alarms raised.

The five charts displayed on the Alarm Summary dashboard are:

- **Top N Sites by Alarm Count**
  This chart will list the Top N sites (maximum of 10) that have the most alarm triggers during the selected time range. If no thresholds are configured, this chart will have 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.
  You can use the Filter drop-down menu to filter the alarms.

- **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.
  You can click the “All Alarms” button at the bottom to bring up a separate window, which will show you all 50 alarms without the need for scrolling.
  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.
### Table 3-1  Last 50 Alarms

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>This contain site or source and destination sites (source - destination) of the network traffic that generated the alarm message.</td>
</tr>
<tr>
<td>Alarm Triggered By</td>
<td>Details information of the network traffic that generated the alarm message. The format of the alarm triggered by string are:</td>
</tr>
<tr>
<td></td>
<td>• Triggered by application threshold: application</td>
</tr>
<tr>
<td></td>
<td>• Triggered by application with DSCP threshold: DSCP:codepoint - application</td>
</tr>
<tr>
<td></td>
<td>• Triggered by host threshold: host</td>
</tr>
<tr>
<td></td>
<td>• Triggered by host with application threshold: host - application</td>
</tr>
<tr>
<td></td>
<td>• Triggered by host with application and DSCP: DSCP: code point - host - application</td>
</tr>
<tr>
<td></td>
<td>• Triggered by host with DSCP: DSCP: code point - host</td>
</tr>
<tr>
<td></td>
<td>• Triggered by conversation: source - destination</td>
</tr>
<tr>
<td></td>
<td>• Triggered by conversation with application: source - application - destination</td>
</tr>
<tr>
<td></td>
<td>• Triggered by response time: IAP: client - application - server.</td>
</tr>
<tr>
<td></td>
<td>• Triggered by DSCP: DSCP: code point</td>
</tr>
<tr>
<td></td>
<td>• Triggered by RTP stream: source - source port - codec(codec string) - SSRC(number) - destination - destination port</td>
</tr>
<tr>
<td></td>
<td>• Triggered by voice signaling: Calling (address - number) Called (address - number) ID/References(id() - ref(calling:called))</td>
</tr>
<tr>
<td></td>
<td>• Triggered by NDE interfaces: NDE: Device (address) - If-Index(number) - Ingress/Egress</td>
</tr>
<tr>
<td>Threshold Variable</td>
<td>Parameter of the threshold that is used to evaluate alarm condition.</td>
</tr>
<tr>
<td>Threshold Value</td>
<td>User defined rising value of the threshold variable.</td>
</tr>
<tr>
<td>Triggered Time</td>
<td>Time when the alarm condition was found occurred.</td>
</tr>
<tr>
<td>Triggered Value</td>
<td>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.</td>
</tr>
<tr>
<td>Clear Time</td>
<td>Time when the alarm condition was resolved. The alarm variable has fallen below the falling threshold value.</td>
</tr>
</tbody>
</table>
Analyzing Traffic

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, as shown below.

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.

The Cisco Prime Network Analysis Module 5.1(3) menu selections for **Analyze > Traffic** are:

- Application, page 3-9
- Host, page 3-10
- NDE Interface Traffic Analysis, page 3-11
- DSCP, page 3-12
- URL Hits, page 3-14

Application

The Application Analysis window will show you at a glance the traffic level for a given application over a selected period of time. It is available under the menu option **Analyze > Traffic > Application**. It will show you:

- A graph of application traffic over time
- Top hosts transmitting and receiving traffic on that application for the selected time period
- Application Configuration -- Shows the criteria by which the NAM classifies packets as that application. This is typically a list of TCP and/or UDP ports that identify the application. Note that some applications are identified by heuristic or other state-based algorithms.

Hosts Detail

On the “Top N Hosts - Traffic In” or “Top N Hosts - Traffic Out” chart, you can left-click a colored bar to get the context menu, and choose “Hosts Detail” to see the All Hosts window and the detailed information about all hosts. **Table 3-2** describes the fields in this window.
Chapter 3 Monitoring and Analysis

Analyzing Traffic

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

- Input and output traffic for the host over time
- Top N application activity of the host over the selected interval
- Total application usage distribution for the host

![Host Traffic Analysis](image)

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 3-3 describes the fields in this window.

### Table 3-2 Host Detail

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host address</td>
</tr>
<tr>
<td>Application</td>
<td>Application type</td>
</tr>
<tr>
<td>In Bits/sec</td>
<td>Number of bits per second incoming</td>
</tr>
<tr>
<td>In Packets/sec</td>
<td>Number of packets per second incoming</td>
</tr>
<tr>
<td>Out Bits/sec</td>
<td>Number of bits per second outgoing</td>
</tr>
<tr>
<td>Out Packets/sec</td>
<td>Number of packets per second outgoing</td>
</tr>
</tbody>
</table>
Chapter 3  Monitoring and Analysis

Analyzing Traffic

### NDE Interface Traffic Analysis

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

You first need to configure the NDE interface capacity to see both the utilization in the charts and the interface name on the NDE interface list. See NDE Interface Capacity, page 2-71 for configuration procedures.

You can also give the SNMP RO (or RW) community string to an NDE data source, and then the NAM will fill up the NDE interface Capacity. Choose **Setup > Traffic > NAM Data Sources** to enter the community string. For more information, see Creating NetFlow Data Sources Using the Web GUI, page 2-28 or Creating NetFlow Data Sources Using the CLI, page 2-29.

To view NDE Interface Analysis, choose **Analyze > Traffic > NDE Interface**. The default view is “Interface View,” shown in Figure 3-4.

#### Table 3-3  Applications Detail

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application type</td>
</tr>
<tr>
<td>Application Group</td>
<td>The application group (set of applications that can be monitored as a whole).</td>
</tr>
<tr>
<td>Bits/sec</td>
<td>Traffic rate; number of bits per second</td>
</tr>
<tr>
<td>Packets/sec</td>
<td>Traffic rate; number of packets per second</td>
</tr>
</tbody>
</table>

**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 NDE device are entered in data source table.

### DSCP Detail

On the “Top N DSCP Aggr - Ingress” and “Top N DSCP Aggr - Egress” chart, you can left-click a colored bar to get the context menu, and 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 DSCP” button on the right.

Table 3-4 describes the fields in the All Applications window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>DSCP value</td>
</tr>
<tr>
<td>Application</td>
<td>Application type</td>
</tr>
<tr>
<td>Bits/sec or Bytes/sec</td>
<td>Traffic rate; number of bits or bytes per second. In Administration &gt; System &gt; Preferences, you can choose to display NAM data in Bits or Bytes.</td>
</tr>
<tr>
<td>Packets/sec</td>
<td>Traffic rate; number of packets per second</td>
</tr>
</tbody>
</table>

### 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 DSCP Groups, page 2-71.

You can monitor the DSCP information by going to Analyze > Traffic > DSCP Traffic Analysis. You will see the DSCP group information as shown in Figure 3-5.
In this window, you will see:

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

### Application Groups Detail

On the “Top N Application Groups” chart, you can left-click a colored bar to get the context menu, and choose “Applications Groups Detail” to see the All Application Groups window and the detailed information about all application groups. Table 3-5 describes the fields in the All Applications window.

**Table 3-5 Application Groups Detail**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>The application group (set of applications that can be monitored as a whole).</td>
</tr>
<tr>
<td>Site</td>
<td>Applicable site (or Unassigned if no site)</td>
</tr>
<tr>
<td>Bits/sec</td>
<td>Traffic rate; number of bits per second</td>
</tr>
<tr>
<td>Packets/sec</td>
<td>Traffic rate; number of packets per second</td>
</tr>
</tbody>
</table>
URL Hits

You can analyze the URLs collected by the NAM (for setup, see URL, page 2-85). This section contains the following procedures:

- Viewing Collected URLs
- Filtering a URL Collection List

Viewing Collected URLs

To view collected URLs:

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

The URLs Window displays with the collected URLs. The columns are described in Table 3-6.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>URL index</td>
</tr>
<tr>
<td>URL</td>
<td>URL text</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of hits</td>
</tr>
</tbody>
</table>

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

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), 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.
Host Conversations

If you choose Analyze > Traffic > Detailed Views > Host Conversations, and click on “Host” in the host conversation tables, you can see detailed lists of all the conversations for a particular host:

- Table of hosts which are sending packets to the selected host, along with application, vlan, and traffic rate information.
- Table of hosts which are receiving packets from the selected host, along with application, vlan, and traffic rate information.
- 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, Network Conversation, RTP Streams, Voice Calls Statistics, Calls Table, and RTP Conversations.

Network Conversation

If you choose Analyze > Traffic > Detailed Views > Conversations, you can see a detailed analysis of all Network Conversations (including packets and bits information).

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

Figure 3-6 Network Conversations

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

Top Application Traffic

When you choose Analyze > Traffic > Detailed Views > Top Application Traffic, you can view the top applications by traffic rate over a selected time and for the specified site and/or data source.

“Top Application Traffic”, as shown in Figure 3-7, will show 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.
Analyzing Traffic

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.

**Figure 3-7  Top Application Traffic**

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.

**Application Traffic By Host**

When you choose **Analyze > Traffic > Detailed Views > Application Traffic By Hosts**, you will see the traffic for a given application broken out by individual hosts using the application (see **Figure 3-8**). You may specify the time period to view, as well as the application, site (optional), data source (optional), and VLAN (optional).

**Figure 3-8  Application Traffic By Host**

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

The 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. The Cisco Prime Network Analysis Module 5.1(3) menu selections for WAN Optimization are:

- Top Talkers Detail, page 3-17
- Application Performance Analysis, page 3-17
- Conversation Multi-Segments, page 3-18
- Conversation Single-Segment, page 3-18

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

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. For information about setting up WAN traffic, see Adding Data Sources for New WAAS Device, page 2-38.

When you choose Analyze > WAN Optimization > Top Talkers Detail, you will see the window that assists you in the pre-deployment process. Use the Interactive Report window to select the traffic you want to analyze for optimization. It will show you Top Applications, Top Network Links, Top Clients, and Top Servers.

The Top Talkers Detail reports total bits/bytes. If the data source is from SPAN, PA, or WAAS, it does not include the packet header; if the data source is NDE, 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.

Application Performance Analysis

To analyze the WAAS traffic, choose Analyze > WAN Optimization > Application Performance Analysis.

The charts available on this page are:

- Transaction Time (Client Experience)
- Traffic Volume and Compression Ratio
- Average Concurrent Connections (Optimized vs. Passthru)
- Multi-Segment Network Time (Client LAN - WAN - Server LAN)
Transaction Time (Client Experience)

This chart 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. The data is shown in milliseconds.

Traffic Volume and Compression Ratio

This chart shows the bandwidth reduction ratio between the number of bits before compression and the number of bits after compression.

Average Concurrent Connections (Optimized vs. Passthru)

This chart shows the number of concurrent connections during a specified time and can be used for capacity planning.

Multi-Segment Network Time (Client LAN - WAN - Server LAN)

This chart shows the network time between the multiple segments. The data is shown in milliseconds.

Conversation Multi-Segments

Use the Conversation Multiple Segments window to monitor WAAS traffic across multiple segments. 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.

Conversation Single-Segment

Use the Conversation Single-Segments window to monitor WAAS traffic across a single segment. This window provides an uncorrelated view of data from different data sources, and allows you to 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).

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 5.1(3) response time monitoring provides end-to-end response times to help you locate possible network and application delays.
Prime NAM 5.1(3) does not support 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 3-9 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 3-9   NAM Application Response Time Measurements**

![Diagram of NAM Application Response Time Measurements]

Figure 3-10 shows a representation of total transaction time as opposed to application response time.

**Figure 3-10   Transaction Time versus Response Time Measurements**

![Diagram of Transaction Time versus Response Time Measurements]
Table 3-7 lists and describes the ART metrics measured by Prime NAM 5.1(3).

**Table 3-7  Application Response Time Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Response Time</td>
<td>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 millisecond (msec) units.</td>
</tr>
<tr>
<td>Min Response Time</td>
<td></td>
</tr>
<tr>
<td>Max Response Time</td>
<td></td>
</tr>
<tr>
<td>Number of Responses</td>
<td>Total number of request-response pairs observed during the monitoring interval</td>
</tr>
<tr>
<td>Number of Late Responses</td>
<td>Total number of responses that exceed the Max Response Time</td>
</tr>
<tr>
<td>Number of Responses 1</td>
<td>Number of responses with a response time less than RspTime1 threshold</td>
</tr>
<tr>
<td>Number of Responses 2</td>
<td>Number of responses with response time less than RspTime2 and larger than RspTime1</td>
</tr>
<tr>
<td>Number of Responses 3</td>
<td>Number of responses with response time less than RspTime3 and larger than RspTime2</td>
</tr>
<tr>
<td>Number of Responses 4</td>
<td>Number of responses with response time less than RspTime4 and larger than RspTime3</td>
</tr>
<tr>
<td>Number of Responses 5</td>
<td>Number of responses with response time less than RspTime5 and larger than RspTime4</td>
</tr>
<tr>
<td>Number of Responses 6</td>
<td>Number of responses with response time less than RspTime6 and larger than RspTime5</td>
</tr>
<tr>
<td>Number of Responses 7</td>
<td>Number of responses with response time less than LateRsp and larger than RspTime6</td>
</tr>
<tr>
<td>Client Bits</td>
<td>Number of TCP payload bits sent from the client(s) during the monitoring interval</td>
</tr>
<tr>
<td>Server Bits</td>
<td>Number of TCP payload bits sent from the server(s) during the monitoring interval</td>
</tr>
<tr>
<td>Client Packets</td>
<td>Number of TCP packets sent from the client(s) during the monitoring interval</td>
</tr>
<tr>
<td>Server Packets</td>
<td>Number of TCP packets sent from the server(s) during the monitoring interval</td>
</tr>
<tr>
<td>Average number of concurrent connections</td>
<td>Average number of concurrent TCP connections during the reporting interval</td>
</tr>
<tr>
<td>Number of new connections</td>
<td>Number of new TCP connections made (TCP 3-way handshake) during the monitoring interval</td>
</tr>
<tr>
<td>Number of closed connections</td>
<td>Number of TCP connections closed during the monitoring interval</td>
</tr>
<tr>
<td>Number of unresponsive connections</td>
<td>Number of TCP connection requests (SYN) that are not responded during the monitoring interval</td>
</tr>
<tr>
<td>Number of refused connections</td>
<td>Number of TCP connection requests (SYN) that are refused during the monitoring interval</td>
</tr>
<tr>
<td>Average Connection duration</td>
<td>Average duration of TCP connections during the monitoring interval</td>
</tr>
<tr>
<td>Average Server Response Time</td>
<td>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.</td>
</tr>
<tr>
<td>Min Server Response Time</td>
<td></td>
</tr>
<tr>
<td>Max Server Response Time</td>
<td></td>
</tr>
<tr>
<td>Average Network Time</td>
<td>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.</td>
</tr>
<tr>
<td>Min Network Time</td>
<td></td>
</tr>
<tr>
<td>Max Network Time</td>
<td></td>
</tr>
</tbody>
</table>
**Table 3-7  Application Response Time Metrics (continued)**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Client Network Time</td>
<td>Client Network Time is the network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Min Client Network Time</td>
<td>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).</td>
</tr>
<tr>
<td>Max Client Network Time</td>
<td>Server Network Time is the network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Average Server Network Time</td>
<td>In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.</td>
</tr>
<tr>
<td>Min Server Network Time</td>
<td>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.</td>
</tr>
<tr>
<td>Max Server Network Time</td>
<td>Use Total Response Time with care because it is not measured directly and mixes the server response time metric with the network time metric.</td>
</tr>
<tr>
<td>Average Total Response Time</td>
<td>Transaction Time is the total amount of time between the client request and the final response packet from the server.</td>
</tr>
<tr>
<td>Min Total Response Time</td>
<td>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.</td>
</tr>
<tr>
<td>Max Total Response Time</td>
<td>Number of Transactions is the number of transactions completed during the monitoring interval.</td>
</tr>
<tr>
<td>Average Data Transmission Time</td>
<td>Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.</td>
</tr>
<tr>
<td>Average Data Time</td>
<td>Data Time: Average data time portion of transaction time.</td>
</tr>
<tr>
<td>Packets Retransmitted</td>
<td>Number of retransmitted packets detected during the monitoring interval.</td>
</tr>
<tr>
<td>Bits Retransmitted</td>
<td>Number of retransmitted bits detected during the monitoring interval.</td>
</tr>
<tr>
<td>Average Retransmission Time</td>
<td>Average time to retransmit lost packets per transaction.</td>
</tr>
<tr>
<td>Client ACK Round Trip Time</td>
<td>Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point.</td>
</tr>
<tr>
<td>Number of Client ACK Round Trips</td>
<td>Number of client ACK RTs observed during the monitoring interval.</td>
</tr>
</tbody>
</table>

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 3-22
- Network Response Time, page 3-22
- Server Response Time, page 3-22
- Client Response Time, page 3-23
- Client-Server Response Time, page 3-23
When you select **Analyze > Response Time > Detailed Views**, you will be able to select one of the following, each of which contains detailed lists of the response events:

- Server Application Responses, page 3-23
- Server Application Transactions, page 3-24
- Server Network Responses, page 3-25
- Client-Server Application Responses, page 3-26
- Client-Server Application Transactions, page 3-27
- Client-Server Network Responses, page 3-28

**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 “Metric1” and “Metric2” drop-down.

Next are the Top Clients and Top Servers charts. These will 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 “Metric1” and “Metric2” drop-down.

The Top Clients and Top Servers charts will 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 “Metric1” and “Metric2” 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 “Metric1” and “Metric2” 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 “Metric1” and “Metric2” 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 3-8 provides definitions of each field of the Server Application Responses window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site.</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Name of the data source</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
<tr>
<td>Server</td>
<td>Name or IP address of the server</td>
</tr>
<tr>
<td>Application</td>
<td>Application currently running</td>
</tr>
<tr>
<td>Number of Clients</td>
<td>Total number of clients</td>
</tr>
</tbody>
</table>
Server Application Transactions

The Server Application Transaction window displays when you click 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 3-9 provides definitions of each field of the Server Application Transactions window.

Table 3-9       Server Application Transactions Metrics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site.</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site.</td>
</tr>
</tbody>
</table>

Table 3-8       Server Application Responses Metrics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Responses</td>
<td>Total number of responses</td>
</tr>
<tr>
<td>Average Client Network Time (ms)</td>
<td>Client Network Time is the network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Maximum Client Network Time (ms)</td>
<td>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).</td>
</tr>
<tr>
<td>Average Server Response Time (ms)</td>
<td>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 &quot;think time,&quot; 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.</td>
</tr>
<tr>
<td>Maximum Server Response Time (ms)</td>
<td></td>
</tr>
<tr>
<td>Average Total Response Time (ms)</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Total Response Time (ms)</td>
<td></td>
</tr>
</tbody>
</table>
### 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 3-10** provides definitions of each field of the Server Network Response Times window.

### Table 3-10  Server Network Responses Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site</td>
</tr>
<tr>
<td>Data Source</td>
<td>Name of the data source</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
</tbody>
</table>

---

**Table 3-9**  Server Application Transactions Metrics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source</td>
<td>Name of the data source</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
<tr>
<td>Server</td>
<td>Name or IP address of the server</td>
</tr>
<tr>
<td>Application</td>
<td>Application currently running</td>
</tr>
<tr>
<td>Number of Clients</td>
<td>Total number of clients</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>Total number of transactions</td>
</tr>
<tr>
<td>Average Transaction Time (ms)</td>
<td>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.</td>
</tr>
<tr>
<td>Average Server Response Time (ms)</td>
<td>Amount of time it takes a server to send the initial response to a client request as seen by the NAM.</td>
</tr>
<tr>
<td>Average Data Transfer Time (ms)</td>
<td>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.</td>
</tr>
<tr>
<td>Average Retransmission Time (ms)</td>
<td>Average time to retransmit lost packets, per transaction.</td>
</tr>
<tr>
<td>Client ACK Round Trip Time (ms)</td>
<td>Average round trip time for the client to acknowledge (ACK) a server TCP packet.</td>
</tr>
</tbody>
</table>
Chapter 3  Monitoring and Analysis

Response Time

Client-Server Application Responses

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

The Client-Server Application Responses window displays. Table 3-11 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.

Table 3-10  Server Network Responses Window (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Name or IP address of the server</td>
</tr>
<tr>
<td>Application</td>
<td>Application being used by server</td>
</tr>
<tr>
<td>Number of Clients</td>
<td>Total number of clients during the monitoring interval</td>
</tr>
<tr>
<td>Number of Connections</td>
<td>Total number of connections during the monitoring interval</td>
</tr>
<tr>
<td>Average Server Network Time (ms)</td>
<td>Average of the Server Network Time (network time between a server and NAM probing point).</td>
</tr>
<tr>
<td>Maximum Server Network Time (ms)</td>
<td>Maximum of the Server Network Time (network time between a server and NAM probing point).</td>
</tr>
<tr>
<td>Average Network Time</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Network Time</td>
<td>Maximum of the network time between client and server.</td>
</tr>
<tr>
<td>Server Bytes</td>
<td>Number of TCP payload bytes sent from the server(s) during the monitoring interval.</td>
</tr>
<tr>
<td>Client Bytes</td>
<td>Number of TCP payload bytes sent from the client(s) during the monitoring interval.</td>
</tr>
</tbody>
</table>

Table 3-11  Client-Server Application Responses Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site</td>
</tr>
<tr>
<td>Data Source</td>
<td>Name of the data source.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
<tr>
<td>Server</td>
<td>Name or IP address of the server</td>
</tr>
<tr>
<td>Client</td>
<td>Host address of the client.</td>
</tr>
<tr>
<td>Application</td>
<td>Application being used by server</td>
</tr>
<tr>
<td>Number of Responses</td>
<td>Total number of responses observed during the monitoring interval</td>
</tr>
</tbody>
</table>
3-27

Chapter 3 Monitoring and Analysis

Response Time

Table 3-11 Client-Server Application Responses Window (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Client Network Time (ms)</td>
<td>Minimum network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Average Client Network Time (ms)</td>
<td>Average network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Maximum Client Network Time (ms)</td>
<td>Maximum network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Minimum Server Network Time (ms)</td>
<td>Minimum network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Average Server Network Time (ms)</td>
<td>Average network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Maximum Server Network Time (ms)</td>
<td>Maximum network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Minimum Transaction Time (ms)</td>
<td>The total amount of time between the client request and the final response</td>
</tr>
<tr>
<td></td>
<td>packet from the server.</td>
</tr>
<tr>
<td>Average Transaction Time (ms)</td>
<td>Average time (ms) elapsed from the start of a client request to the</td>
</tr>
<tr>
<td></td>
<td>completion of server response. Transaction times might vary significantly</td>
</tr>
<tr>
<td></td>
<td>depending upon application types. Relative thresholds are useful in this</td>
</tr>
<tr>
<td></td>
<td>situation.                     Transaction time is a key indicator when detecting application performance</td>
</tr>
<tr>
<td></td>
<td>anomalies.                     anomalies.</td>
</tr>
<tr>
<td>Maximum Transaction Time (ms)</td>
<td>The total amount of time between the client request and the final response</td>
</tr>
<tr>
<td></td>
<td>packet from the server.</td>
</tr>
</tbody>
</table>

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 3-12 provides definitions of each field of the Client-Server Application Transactions window.
Chapter 3 Monitoring and Analysis

Response Time

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 3-13 describes the fields of the Server-Client Network Response Time window.

### Table 3-12  
**Client-Server Application Transactions Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site.</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Name of the data source.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
<tr>
<td>Server</td>
<td>Name or IP address of the server</td>
</tr>
<tr>
<td>Client</td>
<td>Host address of the client.</td>
</tr>
<tr>
<td>Application</td>
<td>Application being used by server</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>Total number of transactions observed during the monitoring interval</td>
</tr>
<tr>
<td>Average Transaction Time (ms)</td>
<td>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.</td>
</tr>
<tr>
<td>Average Server Response Time (ms)</td>
<td>Amount of time it takes a server to send the initial response to a client request as seen by the NAM.</td>
</tr>
<tr>
<td>Average Data Transmission Time (ms)</td>
<td>Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.</td>
</tr>
<tr>
<td>Average Retransmission Time (ms)</td>
<td>Average time to retransmit lost packets per transaction</td>
</tr>
<tr>
<td>Client ACK Round Trip Time (ms)</td>
<td>Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point</td>
</tr>
</tbody>
</table>

### 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 3-13 describes the fields of the Server-Client Network Response Time window.

### Table 3-13  
**Client-Server Network Responses Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Site</td>
<td>Name of the client site.</td>
</tr>
<tr>
<td>Server Site</td>
<td>Name of the server site.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Name of the data source.</td>
</tr>
</tbody>
</table>
Table 3-13  Client-Server Network Responses Window (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN</td>
</tr>
<tr>
<td>Server</td>
<td>Name or IP address of the server.</td>
</tr>
<tr>
<td>Client</td>
<td>Host address of the client.</td>
</tr>
<tr>
<td>Application</td>
<td>Application being used by server.</td>
</tr>
<tr>
<td>Number of Connections</td>
<td>Number of connections.</td>
</tr>
<tr>
<td>Minimum Client Network Time (ms)</td>
<td>Minimum network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Average Client Network Time (ms)</td>
<td>Average network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Maximum Client Network Time (ms)</td>
<td>Maximum network time between a client and the NAM switch or router.</td>
</tr>
<tr>
<td>Minimum Server Network Time (ms)</td>
<td>Minimum network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Average Server Network Time (ms)</td>
<td>Average network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Maximum Server Network Time (ms)</td>
<td>Maximum network time between a server and NAM probing point.</td>
</tr>
<tr>
<td>Minimum Network Time (ms)</td>
<td>Minimum of the network time between client and server.</td>
</tr>
<tr>
<td></td>
<td>Network Time is the sum of Client Network Time and Server Network Time. The 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.</td>
</tr>
<tr>
<td>Average Network Time (ms)</td>
<td>Average of the network time between client and server.</td>
</tr>
<tr>
<td>Maximum Network Time (ms)</td>
<td>Maximum of the network time between client and server.</td>
</tr>
</tbody>
</table>

Managed Device

From the Analyze > Managed Device window, you can view interface information, view system health data, and view Network Based Application Recognition (NBAR) data. The Cisco Prime Network Analysis Module 5.1(3) menu selections for analyzing Managed Devices are:

- Interface, page 3-30
- Health, page 3-31
- NBAR, page 3-37
### Interface

#### 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. 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.

![Interfaces Stats Table](image)

The fields in the table are described in **Table 3-14**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface number.</td>
</tr>
<tr>
<td>In % Utilization</td>
<td>Utilization percentage of the port.</td>
</tr>
<tr>
<td>Out % Utilization</td>
<td>Utilization percentage of the port.</td>
</tr>
<tr>
<td>In Packets/s</td>
<td>Number of incoming packets collected per second.</td>
</tr>
<tr>
<td>Out Packets/s</td>
<td>Number of outgoing packets sent out per second.</td>
</tr>
<tr>
<td>In Bits/s</td>
<td>Number of bits collected per second.</td>
</tr>
<tr>
<td>Out Bits/s</td>
<td>Number of bits sent out per second.</td>
</tr>
<tr>
<td>In Non-Unicast/s</td>
<td>Number of non-unicasts collected per second.</td>
</tr>
<tr>
<td>Out Non-Unicast/s</td>
<td>Number of non-unicasts sent out per second.</td>
</tr>
<tr>
<td>In Discards/s</td>
<td>Number of discards collected per second.</td>
</tr>
<tr>
<td>Out Discards/s</td>
<td>Number of discards sent out per second.</td>
</tr>
<tr>
<td>In Errors/s</td>
<td>Number of errors collected per second.</td>
</tr>
<tr>
<td>Out Errors/s</td>
<td>Number of errors sent out per second.</td>
</tr>
</tbody>
</table>

#### Interface Statistics Over Time

When you select an interface in the Interface Stats Table, the statistics for that interface will be graphed in the area below, as shown in **Figure 3-12**.
Figure 3-12 Interface Statistics Over Time

There are four check boxes above the graph: Bits, Packets, Discards, and Errors. 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.

Health

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

Switch Health

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

- Chassis Health, page 3-32
- Chassis Information, page 3-32
- Crossbar Switching Fabric, page 3-33
- Ternary Content Addressable Memory Information, page 3-34
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 3-15 Chassis Memory Information**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Type</td>
<td>Type of memory including DRAM, FLASH, NVRAM, MBUF, CLUSTER, MALLOC.</td>
</tr>
<tr>
<td>Used</td>
<td>Number of used MB for a particular memory type.</td>
</tr>
<tr>
<td>Free</td>
<td>Number of free MB for a particular memory type.</td>
</tr>
<tr>
<td>Largest Free</td>
<td>Number of largest contiguous free MB for a particular memory type.</td>
</tr>
</tbody>
</table>

Chassis Information

The Chassis Information window displays.

**Table 3-16 Chassis Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.</td>
</tr>
<tr>
<td>Hardware</td>
<td>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.</td>
</tr>
<tr>
<td>Backplane</td>
<td>The chassis backplane type.</td>
</tr>
<tr>
<td>Supervisor Software Version</td>
<td>The full name and version identification of the system’s software operating-system and networking software.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The time (in hundredths of a second) since the network management portion of the system was last re-initialized.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of this node.</td>
</tr>
</tbody>
</table>
Table 3-16 Chassis Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>The textual identification of the contact person for this managed node and information on how to contact this person.</td>
</tr>
<tr>
<td>Modem</td>
<td>Indicates whether the RS-232 port modem control lines are enabled.</td>
</tr>
<tr>
<td>Baud rate</td>
<td>The baud rate in bits per second of the RS-232 port.</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Description of the power supply being instrumented.</td>
</tr>
<tr>
<td>Power Supply Type</td>
<td>The power supply source:</td>
</tr>
<tr>
<td></td>
<td>• unknown</td>
</tr>
<tr>
<td></td>
<td>• ac</td>
</tr>
<tr>
<td></td>
<td>• dc</td>
</tr>
<tr>
<td></td>
<td>• externalPowerSupply</td>
</tr>
<tr>
<td></td>
<td>• internalRedundant</td>
</tr>
<tr>
<td>Power Supply Status</td>
<td>The current state of the power supply being instrumented.</td>
</tr>
<tr>
<td></td>
<td>1: normal</td>
</tr>
<tr>
<td></td>
<td>2: warning</td>
</tr>
<tr>
<td></td>
<td>3: critical</td>
</tr>
<tr>
<td></td>
<td>4: shutdown</td>
</tr>
<tr>
<td></td>
<td>5: notPresent</td>
</tr>
<tr>
<td></td>
<td>6: notFunctioning</td>
</tr>
<tr>
<td>Power Redundancy Mode</td>
<td>Power Redundancy Mode:</td>
</tr>
<tr>
<td></td>
<td>The power-supply redundancy mode.</td>
</tr>
<tr>
<td></td>
<td>1: not supported</td>
</tr>
<tr>
<td></td>
<td>2: redundant</td>
</tr>
<tr>
<td></td>
<td>3: combined</td>
</tr>
<tr>
<td>Power Total</td>
<td>Total current available for FRU usage.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When Redundancy Mode is combined, the total current available will be the sum of the capacities of all operating power supplies.</td>
</tr>
<tr>
<td>Power Drawn</td>
<td>Total Current Drawn by powered-on FRUs.</td>
</tr>
</tbody>
</table>

Crossbar Switching Fabric

This option shows the Crossbar Switching Fabric information. See Table 3-17.
### Table 3-17 Crossbar Switching Fabric Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crossbar Switching Fabric</td>
<td>Physical and configuration information about the module:</td>
</tr>
<tr>
<td></td>
<td><strong>Active slot</strong>—Indicates the slot number of the active switching fabric module. A value of zero indicates that the active switching fabric module is either powered down or not present in the chassis.</td>
</tr>
<tr>
<td></td>
<td><strong>Backup slot</strong>—Indicates the slot number of the backup switching fabric module. A value of zero indicates that the backup switching fabric module is either powered down or not present in the chassis.</td>
</tr>
<tr>
<td></td>
<td><strong>Bus Only Mode Allowed</strong>—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.</td>
</tr>
<tr>
<td></td>
<td><strong>Truncated Mode Allowed</strong>—Indicates whether truncated mode is administratively enabled on the device or not.</td>
</tr>
<tr>
<td>Module Switching Mode</td>
<td>Indicates switching mode of the module:</td>
</tr>
<tr>
<td></td>
<td><strong>busmode</strong>—Module does not use fabric. Backplane is used for both lookup and data forwarding.</td>
</tr>
<tr>
<td></td>
<td><strong>crossbarmode</strong>—Module uses the backplane for forwarding decision and fabric for data forwarding.</td>
</tr>
<tr>
<td></td>
<td><strong>defemode</strong>—Module uses fabric for data forwarding and local forwarding is enabled.</td>
</tr>
<tr>
<td>Module-Channel</td>
<td>Module slot number</td>
</tr>
<tr>
<td>Module-Status</td>
<td>Status of the fabric channel at the module</td>
</tr>
<tr>
<td>Fabric Status</td>
<td>Status of the fabric channel at the slot</td>
</tr>
<tr>
<td>Speed (MB)</td>
<td>Speed (MB/second) of the module</td>
</tr>
<tr>
<td>Module-Channel</td>
<td>Channel for the module</td>
</tr>
<tr>
<td>In Errors</td>
<td>The total number of error packets received since this entry was last initialized.</td>
</tr>
<tr>
<td>Our Errors</td>
<td>The total number of error packets transmitted since this entry was last initialized.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The total number of dropped packets transmitted since this entry was last initialized.</td>
</tr>
<tr>
<td>In Utilization (%)</td>
<td>Input utilization of the channel for the module.</td>
</tr>
<tr>
<td>Out Utilization (%)</td>
<td>Output utilization of the channel for the module.</td>
</tr>
</tbody>
</table>

### Ternary Content Addressable Memory Information

Shows the Ternary Content Addressable Memory (TCAM) usage information. Table 3-18 lists and describes the TCAM information.
If your device is a router, the Router Health window displays with a drop-down box that provides the following options:

- Router Health, page 3-35
- Router Information, page 3-36

### Router Health

The Router Health window displays a real-time graph and information about the health of a router. Table 3-19 describes the contents of the Router Health window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage (graph)</td>
<td>Overall CPU busy percentage in the last 5 minute period</td>
</tr>
<tr>
<td>CPU Type</td>
<td>Describes type of CPU being monitored</td>
</tr>
<tr>
<td>Last 1 minute</td>
<td>Overall CPU busy percentage in the last 1 minute period.</td>
</tr>
<tr>
<td>Last 5 minutes</td>
<td>Overall CPU busy percentage in the last 5 minute period.</td>
</tr>
<tr>
<td>Temperature Description</td>
<td>Description of the test point being measured</td>
</tr>
</tbody>
</table>
The Router Information window displays router information. Table 3-20 lists and describes the fields of the Router Information window.

Table 3-20 Router Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.</td>
</tr>
<tr>
<td>Hardware</td>
<td>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.</td>
</tr>
<tr>
<td>Supervisor Software Version</td>
<td>The full name and version identification of the system's software operating-system and networking software.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time (in hundredths of a second) since the network management portion of the system was last re-initialized.</td>
</tr>
</tbody>
</table>
You can use the NAM to view Network Based Application Recognition (NBAR) data. To view the NBAR data collected for a switch or router, select Analyze > Managed Device > NBAR.

If NBAR is not enabled on your switch or router, you will see a message stating that you cannot see NBAR information without an IOS version that supports NBAR. After you acquire the correct IOS version, you can enable the feature under Setup > Managed Devices > NBAR Protocol Discovery.

Media

The Cisco Prime Network Analysis Module 5.1(3) menu selections for Analyzing Media are:

- RTP Streams, page 3-38
- Voice Call Statistics, page 3-40
- Calls Table, page 3-40
- RTP Conversation, page 3-42
RTP Streams

Purpose

The RTP Streams 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-minute interval reports that takes duration into account, and the highest score among per-interval reports of the stream.

Note: Duration-weighted is calculated with the following formula:
\[
\text{SUM (per-minute-mos * duration)} / \text{SUM (duration)}
\]

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

Note: Duration-weighted are used with the following formula:
\[
\text{SUM(per-interval-jitter * duration)} / \text{SUM(duration)}
\]

- Worst / Overall / Min Actual Packet Loss: Loss percent of RTP packets that are not seen by NAM and RTP packets that arrived beyond the buffer capability of the receiving end point. 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 and 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

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, data source, or VLAN.

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 End Points**: 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 Call 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 3-21, Calls Table, are based on a one minute interval.

Table 3-21 provides descriptions of the fields of the Calls Table.
Chapter 3 Monitoring and Analysis

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’s qualities. The columns of the RTP Stream are described in Table 3-22.

---

**Table 3-21 Calls Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Number</td>
<td>Calling number as it appears in the signaling protocol.</td>
</tr>
<tr>
<td>Called Number</td>
<td>Called number as it appears in the signaling protocol.</td>
</tr>
<tr>
<td>Calling Host Address</td>
<td>RTP receiving address of the calling party detected by the NAM from</td>
</tr>
<tr>
<td></td>
<td>inspecting the call signaling protocol.</td>
</tr>
<tr>
<td>Calling Port</td>
<td>RTP receiving port of the calling party detected by NAM from inspecting</td>
</tr>
<tr>
<td></td>
<td>call signaling protocol.</td>
</tr>
<tr>
<td>Calling Alias</td>
<td>Calling party name detected by NAM from inspecting call signaling protocol.</td>
</tr>
<tr>
<td>Called Host Address</td>
<td>IP address of the phone receiving the call.</td>
</tr>
<tr>
<td>Called Port</td>
<td>Port of the phone receiving the call.</td>
</tr>
<tr>
<td>Called Alias</td>
<td>Alias name, MGCP endpoint ID, or SIP URI of the called party phone.</td>
</tr>
<tr>
<td>Calling Reported Jitter (ms)</td>
<td>Jitter value reported by calling party at the end of the call.</td>
</tr>
<tr>
<td>Calling Reported Packet Loss (%)</td>
<td>Percentage of packet loss reported by calling party at the end of the call.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time when the call was detected to start.</td>
</tr>
<tr>
<td>End Time</td>
<td>Time when the call was detected to end.</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the call.</td>
</tr>
</tbody>
</table>

**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.)

<table>
<thead>
<tr>
<th>Called Reported Jitter (ms)</th>
<th>Jitter value reported by called party at the end of the call.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called Reported Pkt Loss (%)</td>
<td>Percentage of packet loss reported by called party at the end of the call.</td>
</tr>
</tbody>
</table>
You can see more detailed information about each RTP stream by selecting the RTP stream and clicking on the \textit{RTP Stream Details} button. A pop up window will show you the detailed information of the stream displayed.

### RTP Conversation

To get detailed information about RTP conversations, choose \textit{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 3-23, RTP Conversations Table.

### Table 3-22 RTP Streams for the Selected Call table

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>IP Address of the originator of the RTP stream</td>
</tr>
<tr>
<td>Source Port</td>
<td>UDP port of the originator of the RTP stream</td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP address of the receiver of the RTP stream</td>
</tr>
<tr>
<td>Destination Port</td>
<td>UDP port of the receiver of the RTP stream</td>
</tr>
<tr>
<td>Codec</td>
<td>Encoding decoding format/algoritham of the RTP stream</td>
</tr>
<tr>
<td>SSRC</td>
<td>Synchronization source number as it appear in the RTP header</td>
</tr>
<tr>
<td>Duration Weighted MOS</td>
<td>NAM calculated score that takes into account of the duration of the stream</td>
</tr>
<tr>
<td>Duration Weighted Jitter</td>
<td>Jitter that takes into account of the duration of the RTP stream among all per-interval reports</td>
</tr>
<tr>
<td>Overall Adjusted Packet Loss</td>
<td>Percentile of adjust packets lost against total packets of all per-interval RTP reports</td>
</tr>
</tbody>
</table>

### Table 3-23 RTP Conversations Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Time when the RTP stream was discovered by the NAM</td>
</tr>
<tr>
<td>Source Address</td>
<td>IP Address of the originator of the RTP stream</td>
</tr>
<tr>
<td>Source Port</td>
<td>UDP port of the originator of the RTP stream</td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP address of the receiver of the RTP stream</td>
</tr>
<tr>
<td>Destination Port</td>
<td>UDP port of the receiver of the RTP stream</td>
</tr>
<tr>
<td>Codec</td>
<td>Encoding decoding format/algoritham of the RTP stream</td>
</tr>
<tr>
<td>SSRC</td>
<td>Synchronization source number as it appear in the RTP header</td>
</tr>
<tr>
<td>Duration Weighted MOS</td>
<td>NAM calculated score that takes into account of the duration of the stream</td>
</tr>
</tbody>
</table>
Capturing and Decoding Packet Data

The Capture feature of Cisco Prime Network Analysis Module 5.1(3) allows you to set up multiple sessions for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets.

Note
Capture does not apply to the NAM virtual service blades.

This chapter contains the following sections:
- Capture Sessions, page 4-2
  - Software Filters, page 4-7
  - Hardware Filters, page 4-11
- Files, page 4-19
- Capture Data Storage, page 4-23
- Viewing Packet Decode Information, page 4-27.

Quick Capture
From the Context menu of many of the dashboard bar charts which show Applications or Hosts or VLANs, you can start a capture. For example, when you click on an Application in a bar chart (as shown in Figure 4-1) 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
Capture Sessions

The purpose of Capture Sessions is to capture, filter, and decode packet data, manage the data in a file control system, and display the contents of the packets. The captured packets can then be decoded and analyzed on the NAM for more efficient problem isolation.

This section contains the following subjects:

- Capture Sessions Filters, page 4-2
- Viewing Capture Sessions, page 4-3
- Configuring Capture Sessions, page 4-4
- Software Filters, page 4-7
- Software Filters, page 4-7
- Hardware Filters, page 4-11

Capture Sessions Filters

You can filter specific packet data and manage that information in a file control system. This increases your visibility into network issues and allows you to filter out unnecessary information.

As shown in Figure 4-2, 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. See Hardware Filters, page 4-11 for more information about hardware filters.

Note

Hardware filters are supported on Prime NAM 2320, 2220, 2204, and NAM-3.

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. See Software Filters, page 4-7 for more information about software filters.
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 4-2 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.

**Figure 4-2  NAM Capture Sessions Example**

![Diagram showing Capture Sessions]

### 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. **Capture Session Fields, Table 4-1**, describes the Capture Sessions fields.

**Table 4-1  Capture Session Fields**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the capture session</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time the capture was last started. You can stop and restart the capture as many times as necessary.</td>
</tr>
</tbody>
</table>
Chapter 4  Capturing and Decoding Packet Data

Configuring Capture Sessions

Per file location, you can have only one capture session. We support up to ten capture sessions. If you have external storage you can save to local disk and some number of LUNs. You can have one session for each of those. Additionally, you can have multiple sessions saved to memory.

As part of configuring a capture session, you can also create software filters, if desired (see Creating a Software Filter, page 4-7).

To configure a new capture session:

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

Table 4-1  Capture Session Fields (continued)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (MB) (Capture to Memory)</td>
<td>Size of the session</td>
</tr>
<tr>
<td>Size(MB) x No. files (Capture to Files)</td>
<td>Note  Capture to files indicates the capture is being stored in one or more files and is a clickable link to those files.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets</td>
</tr>
<tr>
<td>State</td>
<td>The current status of the capture:</td>
</tr>
<tr>
<td></td>
<td>• Running—Packet capture is in progress</td>
</tr>
<tr>
<td></td>
<td>• Stopped—Packet capture is stopped. Captured packets remain in buffer, but no new packets are captured</td>
</tr>
<tr>
<td></td>
<td>• Full—The memory or file is full, and no new packets will be captured.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the capture (Memory, Local Disk, and external storage).</td>
</tr>
</tbody>
</table>

Table 4-2, Buttons in the Capture Session Operations Window describes the operations that you can perform from the Capture Sessions window.

Table 4-2  Buttons in the Capture Session Operations Window

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a new capture session. See Configuring Capture Sessions, page 4-4.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit the settings of the selected capture.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete a selected session.</td>
</tr>
<tr>
<td>Start</td>
<td>Start capturing to a selected session. The number in the Packets column for that session will start to rise.</td>
</tr>
<tr>
<td>Stop</td>
<td>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.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clear captured data from memory.</td>
</tr>
<tr>
<td>Decode</td>
<td>Display details of the capture session.</td>
</tr>
<tr>
<td>Save to File</td>
<td>Save a session to a file on the NAM hard disk. See Files, page 4-19.</td>
</tr>
</tbody>
</table>

Configuring Capture Sessions
Step 2  Click the Create button to set up a new capture. The NAM displays the Configure Capture Session window. The Capture Settings window provides a field for you to enter a name for the capture and four status indicators described in Table 4-3.

Step 3  Enter information in the Capture Settings Fields (Table 4-3) as appropriate.

Table 4-3  Capture Settings Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the capture</td>
<td>Enter a capture name.</td>
</tr>
<tr>
<td>Packet Slice Size</td>
<td>The slice size in bytes; used to limit the size of the captured packets.</td>
<td>Enter a value between 64 and 9000. Enter zero (0) to not perform slicing.</td>
</tr>
<tr>
<td>(bytes)</td>
<td></td>
<td>If you have a small session but want to capture as many packets as possible, use a small slice size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Capture Source</td>
<td>Data-Port or ERSPAN</td>
<td>Choose the capture source (check one or more check boxes):</td>
</tr>
<tr>
<td>Storage Type: Memory</td>
<td>Check to store captures in memory</td>
<td>• Data-port: This accepts SPAN, RSPAN, and VACL capture.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ERSPAN: Locally terminated is recommended.</td>
</tr>
</tbody>
</table>

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. See Table 4-4 for maximum session sizes for each NAM platform.

The NAM will grant less memory than requested if the available memory is less than requested.

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 4-3  
**Capture Settings Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Type: File(s)</td>
<td>File Size (MB)</td>
<td>Enter a value for <strong>File Size</strong> (file size can be from 1 MB to 2 GB). About 400 MB of free disk space is reserved for working files. If available disk space is below 400 MB, you will not be able to start new capture-to-disk sessions. See Table 4-4, Maximum Capture to Memory Session Sizes for NAM Platforms.</td>
</tr>
<tr>
<td>Number of Files</td>
<td>Enter a value for <strong>Number Of Files</strong> to use for continuous capture. The maxium 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.</td>
<td></td>
</tr>
</tbody>
</table>
| Rotate Files        | Check the **Rotate Files** check box to rotate files in continuous capture. Available only for remote storage or NAM appliances. See section Capturing to Data Storage, page 4-24, for information about configuring remote storage.  
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 Capture Data Storage, page 4-23). |

Table 4-4 lists the hardware platforms that Prime NAM 5.1(3) supports and their maximum session size (the maximum capture to memory buffer size). This is the maximum capture memory buffer size for all capture sessions together, not individually. Maximum capture memory buffer size is based on the NAM hardware memory, as referenced in the table.

**Table 4-4  Maximum Capture to Memory Session Sizes for NAM Platforms**

<table>
<thead>
<tr>
<th>NAM Platform</th>
<th>Maximum Session Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1</td>
<td>125 MB</td>
</tr>
<tr>
<td>WS-SVC-NAM-1 with memory upgrade</td>
<td>500 MB</td>
</tr>
<tr>
<td>MEM-C6KNAM-2GB</td>
<td></td>
</tr>
<tr>
<td>WS-SVC-NAM-1-250S</td>
<td>200 MB</td>
</tr>
<tr>
<td>WS-SVC-NAM-2</td>
<td>300 MB</td>
</tr>
<tr>
<td>WS-SVC-NAM-2 with memory upgrade</td>
<td>500 MB</td>
</tr>
<tr>
<td>MEM-C6KNAM-2GB</td>
<td></td>
</tr>
<tr>
<td>WS-SVC-NAM-2-250S</td>
<td>500 MB</td>
</tr>
<tr>
<td>WS-SVC-NAM-3</td>
<td>10 GB</td>
</tr>
<tr>
<td>WS-SVC-NAM-3-250S</td>
<td></td>
</tr>
<tr>
<td>NAM2204-RJ45</td>
<td>2 GB</td>
</tr>
<tr>
<td>NAM2204-SFP</td>
<td>2 GB</td>
</tr>
<tr>
<td>NAM2220</td>
<td>10 GB</td>
</tr>
</tbody>
</table>
Table 4-4 Maximum Capture to Memory Session Sizes for NAM Platforms (continued)

<table>
<thead>
<tr>
<th>NAM Platform</th>
<th>Maximum Session Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAM2304-RJ45</td>
<td>20 GB</td>
</tr>
<tr>
<td>NAM2304-SFP</td>
<td>20 GB</td>
</tr>
<tr>
<td>NAM2320</td>
<td>20 GB</td>
</tr>
<tr>
<td>NME-NAM-120S</td>
<td>300 MB</td>
</tr>
<tr>
<td>SM-SRE-700/710</td>
<td>1 GB</td>
</tr>
<tr>
<td>SM-SRE-900/910</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

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 the Submit button to finish configuration for this session, or configure Software Filters for this session (see the next section, Software Filters, page 4-7).

Software Filters

You can create and save specialized filters that will disregard everything except the information you are interested in when you capture data (see Figure 4-2). 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).

For NAM-3, multiple software filters will use the “OR” logic; in other words, if a packet passes any software filter, it will be captured.

If you create a session and then start it, you cannot edit the session without stopping it. If you edit a session containing already captured data, you will get a warning saying that the session will be cleared and the data removed. If you ignore the warning and add a filter to the session, and submit it, the new filter settings will be used.

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.

See these topics for help setting up and managing software filters:

- Creating a Software Filter, page 4-7
- Editing a Software Capture Filter, page 4-10

Creating a Software Filter

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

- Source host address
- Destination host address
- Network encapsulation
- VLAN or VLAN range
Capture Sessions

- Application
- Source port or port range
- Destination port or port range

To create a software capture filter:

**Step 1** Choose Capture > Packet Capture/Decode > Sessions. The Configure Capture Session dialog box is displayed.

**Step 2** The bottom half of the window displays any configured Software Filters. Click the Create button at the bottom of the Software Filters area to create a new software filter.

The Software Filter Dialog displays.

**Step 3** Enter information in each of the fields as appropriate. See Table 4-5 for descriptions of the fields.

### Table 4-5 Software Filter Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name of the new filter.</td>
<td></td>
</tr>
<tr>
<td>Source Address / Mask</td>
<td>Source address of the packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The mask applied to the source address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If a bit in the Source Mask is set to 1, the corresponding bit in the address is relevant.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If a bit in the Source Mask is set to 0, the corresponding bit in the address is ignored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 1080::8:800:200C:417A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ::FFF:129.144.52.38</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> See RFC 2373 for valid text representations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For MAC address, enter hh 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. The default mask (if blank) for IPv6 addresses is ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> See RFC 2373 for valid text representations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For MAC address, enter hh 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.</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 4: Capturing and Decoding Packet Data

#### Table 4-5  **Software Filter Dialog Box (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
</table>
| **Destination Address / Mask** | Destination address of the packets.                   | • For IP, IPIPv4, 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 2373 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.           | • For IP, IPIPv4, 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. The default mask (if blank) for IPv6 addresses is ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.  
  **Note** See RFC 2373 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. |
| **Network Encapsulation** | The protocol to match with the packet.                 | Choose the protocol from the drop-down list.  
- Choose MAC to use the source/destination MAC address of the packets.  
- Choose IP to use the source/destination IP addresses of the packets.  
- Choose IPIPv4 for IP addresses including those tunneled over IP protocol 4.  
- Choose GRE.IP for IP addresses including those tunneled over GRE.  
- Choose IPv6 for addresses using IP version 6.  
- Choose GTP.IPv4 for IPv4 address for tunneled packet over GTP.  
- Choose GTP.IPv6 for IPv6 address for tunneled packet over GTP. |
| **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 from one to four individual VLAN IDs.  
For better performance, use as narrow a range as possible. The VLAN ID can range from 1-4095. |
Table 4-5  Software Filter Dialog Box (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Select the Application drop list to filter by application.</td>
<td>Select one protocol to capture from the Application drop-down list.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the Port radio button to filter by Port.</td>
<td>In the Source Port(s) field, enter one or more ports separated by commas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the Destination Port(s) field, enter one or more ports separated by commas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>From the IP Protocol pull-down menu, choose TCP, UDP, or SCTP. No selection (default) means that any will be allowed.</td>
</tr>
</tbody>
</table>

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.

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.

Step 4  Click the Submit button 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.

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

Step 2  Choose the filter to edit, then click Edit.

The Software Filter dialog box (see Table 4-5 on page 4-8) is displayed.

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.
Hardware Filters

Depending on your NAM, the hardware filter support varies:

- NAM-3 Hardware Filters, page 4-11
- Other NAM Hardware Filters, page 4-16

NAM-3 Hardware Filters

NAM-3 hardware filters allow you to improve capture performance by eliminating extraneous traffic, since the packets filtered out by hardware filters are not processed by the NAM. Also, because you can tell the NAM to capture only a portion of the packet and discard the rest, you may want to use hardware filters to look for specific packets in a capture decode.

Hardware filters and global packet slicing affect all capture sessions. See Figure 4-2, “NAM Capture Sessions Example” for an architectural overview.

Cisco Prime Network Analysis Module 5.1(3) supports up to four hardware filters. You can disable hardware filters without deleted them.

There are two levels of hardware filter logic: AND/OR. Within each filter, you can set up conditions with the AND/OR logic. Only the same 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 4-3 for examples of filter logic you can use.

**Figure 4-3  Hardware Filter Logic (AND/OR)**

The selections are described in the following sections. For information about how you can achieve specific results, see Examples, page 4-13.

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 a Hardware Filter, page 4-12
- Hardware Filter Settings, page 4-13
- Examples, page 4-13
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 a 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 the Create button. The Hardware Filter Dialog appears.

**Step 3** Enter a name for the hardware filter in the Name field.

**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 4-6).

**Step 6** Check the boxes for the attributes you would like to filter on, and then in the corresponding drop-down menu, select the desired option. The “Check All” checkbox will select all check boxes. See Table 4-6.

---

**Table 4-6 Create Hardware Filter Dialog**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Options</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Ports</td>
<td>Both Ports, Data Port 1, Data Port 2</td>
<td></td>
</tr>
<tr>
<td>Frame Length</td>
<td>Equal To, Not Equal To, Greater Than, Less Than</td>
<td>Min 64, Max 65535</td>
</tr>
<tr>
<td>VLAN IDs</td>
<td>Equal To, Not Equal To, Greater Than, Less Than</td>
<td>Min 1, Max 4095</td>
</tr>
<tr>
<td>MPLS Label</td>
<td>Equal To, Not Equal To</td>
<td>Min 0, Max 1048575</td>
</tr>
<tr>
<td>Source Address / Mask</td>
<td>Equal To, Not Equal To</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>Destination Address / Mask</td>
<td>Equal To, Not Equal To</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>L4 Protocol</td>
<td>Equal To, Not Equal To ICMP, IGMP, IP in IP, GRE, L2Tp, TCP, UDP, Integer</td>
<td>With Custom, you can enter a value that is not in the list of common protocols. Enter min 1, max 255.</td>
</tr>
<tr>
<td>L4 Source Port</td>
<td>Equal To, Not Equal To</td>
<td>Min 1, Max 65535</td>
</tr>
<tr>
<td>L4 Destination Port</td>
<td>Equal To, Not Equal To</td>
<td>Min 1, Max 65535</td>
</tr>
<tr>
<td>Pattern Match</td>
<td>Filters packets based on 4-byte hexadecimal patterns anywhere in the first 256 bytes. Equal To, Not Equal To</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4  Capturing and Decoding Packet Data

Capturing and Decoding Packet Data

Capture Sessions

Step 7  Click:
- **Apply** to complete the configuration of the hardware filter
- **Cancel** to abort and return to the previous window
- **Reset** to revert to the previous settings

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, follow these steps:

Step 1  Choose **Capture > Packet Capture/Decode > Sessions**.
Step 2  In the Hardware Filters section at the bottom, click the **Hardware Filter Settings** button.
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 4-3.
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 the **Apply** button.

Examples

**IP Subnet + L4 Port (Application)**

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

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

To see the opposite direction of the HTTP conversations:

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

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 the Create button.
**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 the Apply button.

**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 the Create button.
**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 the Apply button.
**Step 7**  Click the Create button 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 the Apply button.
**Step 13**  Repeat Step 7 through Step 12 for a third and fourth host, if desired.
**Step 14**  Click the Hardware Filter Settings button 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 the Create button.
**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 the Apply button.
Step 6  Click the Create button 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 the Apply button.
Step 11 Click the Hardware Filter Settings button 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 the Create button.
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, select 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 the Apply button.

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

Step 1  On the Hardware Filters window, click the Create button.
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 the Apply button.

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 the Create button.
Step 2  Enter a name in the Name field.
Step 3  Choose the Logic “AND” radio button.
Chapter 4      Capturing and Decoding Packet Data

Capture Sessions

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 the **Apply** button.

Step 7  Click the Create button 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 the **Apply** button.

Step 13 Click the **Hardware Filter Settings** button and click the **OR** radio button.

Step 14 Click the **Apply** button.

---

**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 the **Hardware Filter Settings** button.

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

Step 3  Click the **Apply** button.

Go to the next section, **Software Filters, page 4-7**, for information about configuring software filters for capture sessions.

---

**Other NAM Hardware Filters**

Hardware Filters enable you to improve capture performance by providing hardware-specific filters that eliminate as much extraneous traffic as possible. The packets filtered out by hardware filters are not processed by the NAM, and therefore capture performance improves.

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.

See **Configuring a Hardware Filter, page 4-16** for detailed steps.

---

**Configuring a Hardware Filter**

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, in the Hardware Filters section, click the **Create** button.

**Step 3** Enter a name in the Name field.

**Step 4** Choose one of the following types of filters from the Type drop-down list:
- VLAN
- VLAN and IP
- IP
- IP and TCP/UDP
- IP and Payload Data
- Payload Data

**Step 5** Data fields will then appear that correspond with the type of hardware filter you selected. Fill in the desired fields. See the following sections for more specific information.

**Step 6** Click **Submit** to complete the configuration of the capture session. Otherwise, click **Reset** to revert to the previous settings, or click **Cancel** to abort.

### VLAN

To configure a VLAN hardware filter:

**Step 1** Enter a Filter Name.

**Step 2** From the Type drop-down menu, choose **VLAN**.

**Step 3** Choose either the Range or Individuals radio button. For Range, enter a range of VLANs. For Individuals, enter up to four individual VLANs.

**Step 4** Click the **Submit** button.

### VLAN and IP

To configure a VLAN and IP hardware filter:

**Step 1** Enter a Filter Name.

**Step 2** From the Type drop-down menu, choose **VLAN and IP**.

**Step 3** Enter the ID of the desired VLAN. The VLAN ID can range from 1-4095.

**Step 4** Enter a Source Address / Mask (optional).

**Step 5** Enter a Destination Address / Mask (optional).

**Step 6** Choose a Layer 4 Protocol (optional).

**Step 7** Click **Submit**.
**IP**

To configure an IP hardware filter:

**Step 1** Enter a Filter Name.

**Step 2** From the Type drop-down menu, choose **IP**.

**Step 3** Enter a Source Address / Mask (optional).

**Step 4** Enter a Destination Address / Mask (optional).

**Step 5** Choose a Layer 4 IP Protocol (optional)

**Step 6** Click **Submit**.

---

**IP and TCP/UDP**

To configure an IP and TCP/UDP hardware filter:

**Step 1** Enter a Filter Name.

**Step 2** From the Type drop-down menu, choose **IP and TCP/UDP**

**Step 3** Enter a Source Address / Mask (optional).

**Step 4** Enter a Destination Address / Mask (optional).

**Step 5** Choose an IP Protocol, either TCP or UDP.

**Step 6** Enter a TCP/UDP Source Port (optional).

**Step 7** Enter a TCP/UDP Destination Port (optional).

**Step 8** Click **Submit**.

---

**IP and Payload Data**

To configure an IP and Payload Data hardware filter:

**Step 1** Enter a Filter Name.

**Step 2** From the Type drop-down menu, choose **IP and Payload Data**.

**Step 3** Enter a Source Address / Mask (optional).

**Step 4** Enter a Destination Address / Mask (optional).

**Step 5** Choose an IP Protocol, either TCP or UDP.

**Step 6** Enter the values for Payload Data:

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

**Step 7** Repeat **Step 6** for up to four payload data segments.
Chapter 4  Capturing and Decoding Packet Data

Files

Payload Data

To configure a Payload Data hardware filter:

Step 1  Enter a Filter Name.
Step 2  From the Type drop-down menu, choose Payload Data.
Step 3  Choose an IP Protocol, either TCP or UDP.
Step 4  Enter the values for Payload Data:
   - Enter an Offset from 1-1023. The offset is relative to the beginning of the payload (Layer 5).
   - Enter a Value of up to four bytes (eight hex characters).
   - Enter a Mask of up to four bytes (eight hex characters).
Step 5  Repeat Step 4 for up to four payload data segments.

Note  Only one payload segment (one row) is required. Be careful not to create 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.

Files

Use the Files option to decode, download, rename, convert/merge, delete, analyze, or error-scan saved capture files. See the section Capture Sessions, page 4-2 and Table 4-2 for information about how to save capture sessions to files. You can download files in either .enc or .pcap file formats. See Preferences, page 5-11, for information about setting the download file format.

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

Choose Capture > Packet Capture/Decode > Files to display the Capture Files window. The Capture Files window shows the following information:

   - Name:
   - Size:
If you are using a Prime NAM appliance, the NAM will create a `xxx.pcap` file. If you click on the download button, a `xxx.pcap` file will be created regardless of whether you accept the download action or cancel it (a `xxx.pcap` file will be created once the download button is clicked). This is why one capture using an appliance could have an extra file compared with a capture from another NAM platform.

**Table 4-7 Buttons in the Capture Files Operations Window**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decode</td>
<td>Display the packets in a file.</td>
</tr>
<tr>
<td>Download</td>
<td>Download a file to your computer in .enc or .pcap file format.</td>
</tr>
<tr>
<td>Note</td>
<td>Do not add a file suffix when you provide the filename. The suffix .pcap is added automatically.</td>
</tr>
<tr>
<td>Note</td>
<td><code>.capture</code> to <code>.pcap</code> conversion will occur when you download a capture file. You will need to manually delete the <code>.pcap</code> file when it is done.</td>
</tr>
<tr>
<td>Rename</td>
<td>Give the file a new name. A dialog box displays and asks you to enter the new name for the selected capture file.</td>
</tr>
<tr>
<td>Merge or Convert/Merge</td>
<td>Merge packets of files (in chronological order). A dialog box displays and asks you to enter the new name for the merged capture files. Enter a name for the merged capture files and choose OK.</td>
</tr>
<tr>
<td>Note</td>
<td>Merged files cannot exceed 2 GB.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete files.</td>
</tr>
<tr>
<td>Analyze</td>
<td>View statistical analysis of the selected capture. See Analyzing Capture Files, page 4-21.</td>
</tr>
<tr>
<td>Errors Scan</td>
<td>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 Error Scan, page 4-21.</td>
</tr>
</tbody>
</table>

**Note**  Capture files on the Prime NAM appliances are stored in native NAM format. You can convert the capture file format to .pcap using the Convert/Rename/Merge button on the Capture > Packet Capture/Decode > Files window.
Chapter 4  Capturing and Decoding Packet Data

Analyzing Capture Files

The Capture Files window (Capture > Packet Capture/Decode > Files) enables you to obtain various statistics including traffic rate (bytes/second) over a capture period, lists of hosts, conversations, and applications 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 4-8 describes the different areas of the capture analysis window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Overview</td>
<td>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)</td>
</tr>
<tr>
<td>Traffic over Time</td>
<td>Displays a graphic image of network traffic (KB/second)</td>
</tr>
<tr>
<td>Protocol Statistics</td>
<td>Displays packets and bytes transferred for each protocol</td>
</tr>
<tr>
<td>Hosts Statistics</td>
<td>Displays packets and bytes transferred for each host address</td>
</tr>
</tbody>
</table>

**Error Scan**

**Note**
This feature is available for .pcap files, but not for .capture files.

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 (select a row in the table and click the Decode Packet button).

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 is shown in Figure 4-4.

![Figure 4-4 Error Scan](image)

The fields are described in Table 4-9.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet ID</td>
<td>ID of the packet in the capture file.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol the packet arrived on.</td>
</tr>
<tr>
<td>Severity</td>
<td>Warn: Warning; for example, an application returned an unusual error code</td>
</tr>
<tr>
<td></td>
<td>Error: A serious problem, such as malformed packets</td>
</tr>
<tr>
<td>Group</td>
<td>Checksum: A checksum was invalid</td>
</tr>
<tr>
<td></td>
<td>Sequence: Protocol sequence is problematic</td>
</tr>
<tr>
<td></td>
<td>Response Code: Problem with the application response code</td>
</tr>
<tr>
<td></td>
<td>Request Code: An application request</td>
</tr>
<tr>
<td></td>
<td>Undecoded: Dissector incomplete or data can’t be decoded</td>
</tr>
<tr>
<td></td>
<td>Reassemble: Problems while reassembling</td>
</tr>
<tr>
<td></td>
<td>Malformed: Malformed packet or dissector has a bug; dissection of this packet aborted</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the error or warning</td>
</tr>
</tbody>
</table>

### 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.
Deleting a Capture File

To delete a capture file:

Step 1 Choose Capture > Packet Capture/Decode > Files.
Step 2 Click 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 the Delete All button 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.

Capture Data Storage

The Cisco Prime Network Analysis Module 5.1(3) on all platforms offers external storage connectivity for extended capture durations and higher capture bandwidths. All platforms support iSCSI data storage. Only NAM-3 platforms support SAS and FCoE in addition to iSCSI.

On NAM-3, iSCSI, SAS, and FCoE connectivity can be used simultaneously. See Figure 4-5 for an overview of external data storage setup.

This section covers:

- Capturing to Data Storage
- Recovering Data Storage
Chapter 4  Capturing and Decoding Packet Data

Capture Data Storage

For instructions on installing and configuring external storage, see your platform-specific guides on Cisco.com or related documentation in the Cisco NAM Documentation Overview.

Capturing to Data Storage

In the NAM, external storage management is performed under the NAM menu Capture > Packet Capture/Decode > Data Storage. This window lists detected storage devices, including the internal hard drive.

This release supports 32 external data storage targets (LUNs combined).

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

Prepare LUNs

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, go Capture > Packet Capture/Decode > Data Storage.

New LUNs which have not been used by the NAM will show a status of “Unformatted.” To prepare these LUNs for capture use, select the LUN and click the Format button. After a few minutes, the status should change to “Ready.”

User labels can be applied to the LUNs to help with differentiating between them. To label a LUN, select it and click the Label button. The Label dialog will appear with information about the current Label and the last time the LUN was formatted.
## Use LUNs

To use a LUN for a capture session:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to <strong>Capture &gt; Packet Capture/Decode &gt; Sessions.</strong></td>
</tr>
<tr>
<td>2</td>
<td>Under the Capture Sessions table, click the <strong>Create</strong> button.</td>
</tr>
<tr>
<td>3</td>
<td>Fill in the appropriate fields for creating a session, and for “Storage Type” choose the “Files” option.</td>
</tr>
<tr>
<td>4</td>
<td>Use the “File Location” drop-down 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.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>Submit</strong> to create the session, or <strong>Cancel</strong> to return to the previous window.</td>
</tr>
</tbody>
</table>

When a session is created, the associated LUN state will change 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.

## Decoding Files

Files captured to external storage can be decoded in the same manner as with internal **Capture > Packet Capture/Decode > Files** page. This page has a drop-down to select the LUN of focus. The files table will show all capture files on that particular LUN.

## 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 NAM that the device will be disconnected, and the NAM will perform important cleanup procedures. After this is done, the storage target will show up as **Unmounted** in the status column, and it is safe to remove the external storage device. External storage is automatically disconnected in this manner when the NAM-3 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 run 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 an iSCSI recovery example:

root@nam.cisco.com# remote-storage iscsi list
Storage ID: 16
  Label:
    Status: Unformatted
    Protocol: iSCSI
    Target IP: 172.20.122.81
    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: 172.20.122.81
  Target IQN: iqn.2011-09:celeros.target16
  Model: IET VIRTUAL-DISK
  LUN: 5
  Capacity: 24.98GB
  Available: 16.47GB

Active iSCSI Sessions:

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: 172.20.122.81
    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: 172.20.122.81
  Target IQN: iqn.2011-09:celeros.target16
  Model: IET VIRTUAL-DISK
  LUN: 5
  Capacity: 24.98GB
  Available: 16.47GB

Active iSCSI Sessions:
Viewing Packet Decode Information

After some packets or files have been captured, you can use the Packet Decoder to view the packet contents.

The Packet Decoder window has four parts:

- Packet Decoder operations
- Packet browser pane
- Protocol decode (see Viewing Detailed Protocol Decode Information, page 4-29)
- Packet hexadecimal dump

To view packet decode information:

**Step 1** Choose **Capture > Packet Capture/Decode > Sessions**, or **Capture > Packet Capture/Decode > Files** (depending on which type you would like to decode).

**Step 2** Choose a capture session or file, and then click the **Decode** button. The Packet Decoder window displays. 

Table 4-10 describes the packet decoder operations on the NAM - Packet Decoder window.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Stop packet loading</td>
</tr>
<tr>
<td>Prev</td>
<td>Load and decode the previous block of packets from the NAM</td>
</tr>
<tr>
<td>Next</td>
<td>Load and decode the next block of packets from the NAM</td>
</tr>
<tr>
<td>Go To</td>
<td>Load and decode a block of packets starting from the specified packet number.</td>
</tr>
<tr>
<td>TCP Stream</td>
<td>Follow the TCP stream of the selected TCP packet. This might take a long time depending on the traffic pattern.</td>
</tr>
</tbody>
</table>

Table 4-11 describes the columns displayed in the packet browser pane.
Table 4-11  Packet Browser

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkt</td>
<td>Packet numbers, listed numerically in capture sequence. If the decode (display) filter is active, the packet numbers might not be consecutive.</td>
</tr>
<tr>
<td>Time</td>
<td>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.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the packet, in bytes.</td>
</tr>
<tr>
<td>Source</td>
<td>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.</td>
</tr>
<tr>
<td>Destination</td>
<td>Packet destination, which might be displayed as hostname, IP, IPX, or MAC address.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Top-level protocol of the packet.</td>
</tr>
<tr>
<td>Info</td>
<td>Brief text information about the packet contents.</td>
</tr>
</tbody>
</table>

Browsing Packets in the Packet Decoder

You can use the packet browser to browse the list of captured packets and do the following:

- Filter by protocol, IP address, MAC address, and custom display filter.
- Use the Next, Previous, and Go To buttons to load packets from the capture session.

Note  The capture must be paused or stopped for you to use these features.

Filtering Packets Displayed in the Packet Decoder

To filter packets displayed in the packet decoder:

Step 1  From the Packet Decoder window, click the Display Filter button. The Packet Decoder - 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 address filters on IP address.
  - MAC Address filter 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 travelling in both directions.
- Define a Protocol Filter.
– Click **Match any** to display packets that match any of the protocols or fields or
– Click **Match all** 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.
  - Choose a **Custom Filter**. See **Custom Display Filters, page 4-30** for how to set up a custom display filter.

**Step 3**
Click **OK** to apply the filter and close the window.
Click **Submit** to apply the filter and keep the window open.
Click **Clear Filter** to clear all of the fields.
Click **Cancel** to close the window without any action.

---

**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, the 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.
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** Create an alarm event from the Setup > Alarms > Alarm Events window.
Configure an Alarm Event for the type of event for which you want to capture data. See Alarm Action Configuration, page 2-45, for more information.

**Step 2** Set a threshold for the event from the Setup > Alarms > Alarm Thresholds window.
Configure the threshold of parameters of interest in the associated Alarm Event. See Thresholds, page 2-47, for more information.

**Step 3** Set up a capture session from the Capture > Packet Capture/Decode > Sessions window. Click Create.
Choose the Start Event and/or the Stop Event for the associated Alarm Event. See Configuring Capture Sessions, page 4-4, for more information.

Custom Display Filters

Use custom display filters to create and save customized filters to use in the Decode window to limit which packets are to be displayed.

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

- Creating Custom Display Filters, page 4-30
- Editing Custom Display Filters, page 4-33
- Deleting Custom Display Filters, page 4-33

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 Custom Decode Filter Dialog Box, Table 4-12, displays.

**Step 3** Enter information in each of the fields as appropriate.
Chapter 4  Capturing and Decoding Packet Data

Viewing Packet Decode Information

Table 4-12  Custom Decode Filter Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>The name of the capture filter.</td>
<td>Enter the name of the filter to be created.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the capture filter.</td>
<td>Enter a description of the filter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol to match with the packet.</td>
<td>Choose a protocol from the list. (Select All to match all packets regardless of protocol.)</td>
</tr>
<tr>
<td>Address (MAC or IP)</td>
<td>Indicates whether to filter by MAC or IP address.</td>
<td>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.</td>
</tr>
<tr>
<td>Both Directions</td>
<td>Indicates whether the filter is applied to traffic in both directions.</td>
<td>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.</td>
</tr>
<tr>
<td>Offset</td>
<td>The offset (in bytes) from the Base where packet data-matching begins.</td>
<td>Enter a decimal number.</td>
</tr>
<tr>
<td>Base</td>
<td>The base from which the offset is calculated.</td>
<td>Choose absolute or a protocol.</td>
</tr>
<tr>
<td>Data Pattern</td>
<td>The data to be matched with the packet.</td>
<td>Enter ( hh \ hh \ hh \ldots ), where ( hh ) are hexadecimal numbers from 0-9 or a-f. Leave blank if not applicable.</td>
</tr>
<tr>
<td>Filter Expression</td>
<td>An advanced feature to set up complex filter conditions.</td>
<td>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 \texttt{ipx}. See Tips for Creating Custom Decode Filter Expressions, page 4-32.</td>
</tr>
</tbody>
</table>

**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 4-13.

### Table 4-13 Logical and Comparison Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>and</td>
<td>Logical AND</td>
</tr>
<tr>
<td>or</td>
<td>Logical OR</td>
</tr>
<tr>
<td>xor</td>
<td>Logical XOR</td>
</tr>
<tr>
<td>not</td>
<td>Logical NOT</td>
</tr>
<tr>
<td>==</td>
<td>Equal</td>
</tr>
<tr>
<td>!=</td>
<td>Not equal</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
</tr>
</tbody>
</table>

You can also group subexpressions within parentheses. You can use the following fields in filter expressions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Filter By</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth.addr</td>
<td>MAC address</td>
<td>hh:hh:hh:hh:hh, where h is a hexadecimal number from 0 to 9 or a to f.</td>
</tr>
<tr>
<td>eth.src</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth.dst</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip.addr</td>
<td>IP address</td>
<td>n.n.n.n or 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.</td>
</tr>
<tr>
<td>ip.src</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip.dst</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp.port</td>
<td>TCP port number</td>
<td>A decimal number from 0 to 65535.</td>
</tr>
<tr>
<td>tcp.srcport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp.dstport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>udp.port</td>
<td>UDP port number</td>
<td>A decimal number from 0 to 65535.</td>
</tr>
<tr>
<td>udp.srcport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>udp.dstport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol</td>
<td>Click the Protocol list in the Custom Decode Filter dialog box to see the list of protocols on which you can filter.</td>
</tr>
<tr>
<td>protocol[offset:length]</td>
<td>Protocol data pattern</td>
<td>hh:hh:hh:hh..., where hh is a hexadecimal number from 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.</td>
</tr>
<tr>
<td>frame.pkt_len</td>
<td>Packet length</td>
<td>A decimal number that represents the packet length, not the truncated capture packet length.</td>
</tr>
</tbody>
</table>

**Examples of Custom Decode Filter Expressions**

- To match SNMP packets from 111.122.133.144, enter:
  
  `snmp and (ip.src == 111.122.133.144)`
Cisco Prime Network Analysis Module User Guide 5.1(3)

Chapter 4  Capturing and Decoding Packet Data

Viewing Packet Decode Information

- To match IP packets from the 111.122 Class B network, enter:
  \[ \text{ip.addr} == 111.122.0.0/16 \]

- To match TCP packets to and from port 80, enter:
  \[ \text{tcp.port} == 80 \]

- The TOS value is stored in byte 1 (the second byte) in the IP header. To match the IP packet with the TOS value 16 (0x10), enter:
  \[ \text{ip[1:1]} == 10 \]

- The TCP acknowledgement number is stored in bytes 8 through 11 in the TCP header. To match the TCP packet with acknowledgement number 12345678 (0xBC614E), enter:
  \[ \text{tcp[8:4]} == 00:BC:61:4E \]

**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 Custom Display Filters**

To edit custom display filters:

**Step 1** Choose Capture > Packet Capture/Decode > Display Filters.

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

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

**Step 4** Do one of the following:
- To apply the changes, click **Submit**.
- To clear the page of your changes, click **Reset**.
- To exit the page without applying the changes, click **Cancel**.

**Deleting Custom Display Filters**

To delete custom display filters:

**Step 1** Choose Capture > Packet Capture/Decode > Display Filters.

**Step 2** Choose the filter to delete, then click **Delete**.

**Step 3** In the confirmation dialog box, do one of the following:
- To delete the filter, click **OK**.
- To cancel, click **Cancel**.
Performing User and System Administration

This chapter provides information about performing user and system administration tasks in Cisco Prime Network Analysis Module 5.1(3) and generating diagnostic information for obtaining technical assistance.

This chapter contains the following sections:

- **System Administration, page 5-1**, describes menu options that enable you to perform system administrative tasks and manage the NAM.
- **Diagnostics, page 5-11**, describes menu options that help you diagnose and troubleshoot problems.
- **User Administration, page 5-13**, describes how you configure either a local database or provide information for a ACS/TACACS+ database for user authentication and authorization. This section also describes the current user session window.

**System Administration**

The System option of the Administration menu provides access to the following functions:

- **Resources, page 5-2**
- **Network Parameters, page 5-2**
- **SNMP Agent, page 5-3**
- **System Time, page 5-6**
- **E-Mail Setting, page 5-8**
- **Web Data Publication, page 5-9**
- **Syslog Setting, page 5-9**
- **SNMP Trap Setting, page 5-10**
- **Preferences, page 5-11**
Resources

Choose **Administration > System > Resources** to view the System Overview window. **Table 5-1** describes the fields of the System Overview window.

**Table 5-1 System Overview**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Current date and time synchronized with the switch, router, or NTP server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>NAM hostname.</td>
</tr>
<tr>
<td>IP Address</td>
<td>NAM IP address.</td>
</tr>
<tr>
<td>System Uptime</td>
<td>Length of time the host has been running uninterrupted.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Percentage of CPU resources being consumed by the NAM. Average, at top, indicates the average CPU usage of all CPUs. Each individual CPU in a multi-CPU platform is listed separately.</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Percentage of memory resources being consumed by the NAM.</td>
</tr>
<tr>
<td>Memory Total</td>
<td>Total amount of system memory.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>Shows root, config, and data partitions with their total and free space.</td>
</tr>
<tr>
<td>Data Files</td>
<td>Shows the amount of disk space used up by the performance data base files (DB) and the packet capture to disk (capture files).</td>
</tr>
<tr>
<td>NIC Statistics</td>
<td>Shows the health and usage information on the data ports, where the NAM receives most of the traffic to be analyzed. It shows the number of packets received (rx pkts), number of bytes received (rx bytes) and number of packets lost or dropped (rx lost). The first number shows cumulative counts since the start of the NAM, and the second one shows the same counters for the last ten seconds.</td>
</tr>
</tbody>
</table>

**Network Parameters**

To view and set network parameters such as your site’s name servers:

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

The **Network Parameters** window displays.

**Step 2** Enter or change the information detailed in **Table 5-2**.
Note
NAM 5.1(x) does not support using IPv6 for the network parameter IP address.

Table 5-2  Network Parameters Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>NAM IP address.</td>
</tr>
<tr>
<td>IP Broadcast</td>
<td>NAM broadcast address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>NAM subnet mask.</td>
</tr>
<tr>
<td>IP Gateway</td>
<td>NAM IP gateway address.</td>
</tr>
<tr>
<td>Host Name</td>
<td>NAM hostname.</td>
</tr>
<tr>
<td>Domain name</td>
<td>NAM domain name.</td>
</tr>
<tr>
<td>Nameservers</td>
<td>NAM nameserver address or addresses.</td>
</tr>
</tbody>
</table>

Step 3
Do one of the following:
- To save the changes, click Submit.
- To cancel the changes, click Reset.

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 stats. 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 5-3.

**Table 5-3 System SNMP Dialog Box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>The name of the person responsible for the NAM.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the NAM.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the switch or router in which the NAM is installed.</td>
</tr>
</tbody>
</table>

**Step 3** Do one of the following:
- To save the changes, click Submit.
- To cancel the changes, click Reset.

**Step 4** Set the NAM community strings. See Working with NAM Community Strings, page 5-4.

---

### 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** At the bottom of the window, the NAM Community Strings Dialog Box displays.

**Step 3** Click Create.

**Step 4** The SNMP Agent Dialog Box displays.

**Step 5** 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** Do one of the following:
- To make the changes, click Submit.
- To reset, click Reset.
Deleting NAM Community Strings

To delete the NAM community strings:

**Step 1** Choose Administration > System > SNMP Agent.
At the bottom of the window, the NAM Community Strings Dialog Box displays.

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

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

The community string is deleted.

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.
System Time

The NAM gets the UTC (GMT) time from several sources, depending on its the NAM type. All NAMs can be set up to get their time from an external NTP server.

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 wrong, then the data shown in the GUI will be wrong.

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.

```
root@nam.localdomain# sho time ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xec:44:76:ff:fe:5d:12:0
  Parent Port Number: 6
```

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

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

- **Synchronizing the NAM System Time with the Switch or Router, page 5-6**
  
  This option is valid only for WS-SVC-NAM-1, WS-SVC-NAM-2, WS-SVC-NAM-3, NME-NAMs, and SM-SREs.

- **Synchronizing the NAM System Time Locally, page 5-7**
  
  This option is valid for Cisco Prime NAM appliances, Nexus 1010 VSB, and WAAS Virtual Blade NAM.

- **Configuring the NAM System Time with an NTP Server, page 5-7**

- **Configuring the NAM System Time with Precision Time Protocol (IEEE 1588), page 5-7**
  
  This option is valid for WS-SVC-NAM-3.

Synchronizing the NAM System Time with the Switch or Router

**Note**

This section is valid only for WS-SVC-NAM-1, WS-SVC-NAM-2, and NME-NAMs.

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

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

**Step 2** Choose the Switch or Router radio button.

**Step 3** Select the Region and local time zone from the lists.

**Step 4** Do one of the following:

- To save the changes click **Submit**.
- To leave the configuration unchanged, click **Reset**.
Synchronizing the NAM System Time Locally

Note
This section is valid for Cisco NAM appliances, Nexus, and WAAS NAM.

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

Step 1 Log into the NAM appliance 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 NAM appliance 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 Do one of the following:
   • To save the changes click Submit.
   • To leave the configuration unchanged, choose Reset.

Configuring the NAM System Time with an NTP Server

To configure the NAM system time with an NTP server:

Step 1 On the NAM appliance GUI, 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.

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, as well as a PTP master connected to the switch.

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.
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.
System Administration

Chapter 5  Performing User and System Administration

Displaying Precision Time Protocol Status

Step 1 Configure PTP using the Configuring the NAM System Time with Precision Time Protocol (IEEE 1588) steps above (this must be done before the status can successfully be displayed).

Step 2 Choose Administration > System > System Time.

Step 3 Make a selection from the drop-down menu and click the Show button. The pop-up window that appears will give you detailed information about the selection you chose:
- clock
- foreign-master-record
- parent
- time-property

E-Mail Setting

You can configure the NAM to provide e-mail notification of alarms and to e-mail reports. To configure the NAM for e-mail notifications:

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

Step 2 The Mail Configuration Window displays. Table 5-4 describes the Mail Configuration Options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Mail</td>
<td>Enables e-mail of reports and notification of alarms</td>
</tr>
<tr>
<td>External Mail Server</td>
<td>Distinguished name of external mail server</td>
</tr>
<tr>
<td>Send Test Mail</td>
<td>List e-mail addresses for up to three e-mail recipients</td>
</tr>
<tr>
<td>Mail Alarm to</td>
<td>This recipient will receive alarm notifications and scheduled exports.</td>
</tr>
</tbody>
</table>

Step 3 Check the Enable Mail check box.

Step 4 Enter the distinguished name of the External Mail Server.

Step 5 Put an e-mail address in the Send Test Mail field (optional). A test e-mail will be sent to this recipient.

Step 6 Put an e-mail address in the Mail Alarm to field. Alarm notifications and Exports will be sent to this recipient.

Step 7 Click Submit to save your modifications, or click Reset to clear the dialog of any characters you entered or restore the previous settings.
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.

Syslog Setting

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.

Note  Prime NAM sends syslog alerts for audit trail events and configured alarm threshold events. Prime NAM does not send syslog alerts about its own physical state (temperature levels or interface status changes). For a list of user activities logged in the audit trail window, see Audit Trail, page 5-12.

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.

### SNMP Trap Setting

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.

These topics help you set up and manage NAM traps:
- Creating a NAM Trap Destination, page 5-10
- Editing a NAM Trap Destination, page 5-10
- Deleting a NAM Trap Destination, page 5-11

### Creating a NAM Trap Destination

To create a NAM trap destination:

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

The SNMP Trap Setting window displays.

**Step 2**  Click the Create button.

**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.

### Editing a NAM Trap Destination

To edit a NAM trap destination:

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

The NAM Trap Destinations page displays.

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

The Edit Trap dialog box displays.

**Step 3**  Make the necessary changes.

**Step 4**  Click Submit to save your changes, or click Reset to remove any entry.
Deleting a NAM Trap Destination

To delete an existing trap, simply select it from the Traps table, then click Delete.

Preferences

Choose Administration > System > Preferences to configure characteristics for the NAM such as NAM display, audit trail, and file format preferences. Table 5-5 describes the fields of the Preferences window.

<table>
<thead>
<tr>
<th>Table 5-5 Preferences</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Interval (60-3600 sec)</td>
<td>Amount of time between refresh of information on dashboards.</td>
<td></td>
</tr>
<tr>
<td>Top N Entries (1-10)</td>
<td>Number of colored bars on the Top N charts.</td>
<td></td>
</tr>
<tr>
<td>Perform IP Host Name Resolution</td>
<td>Wherever an IP address is displayed, it will get translated to a hostname via DNS lookup.</td>
<td></td>
</tr>
<tr>
<td>Data Displayed In</td>
<td>Data displayed in Bytes or Bits.</td>
<td></td>
</tr>
<tr>
<td>International Notation</td>
<td>Choose the way you would like numbers displayed.</td>
<td></td>
</tr>
<tr>
<td>Audit Trail</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Capture File Download Format</td>
<td>Choose ENC (.enc) or PCAP (.pcap) format for captured files.</td>
<td></td>
</tr>
</tbody>
</table>

Diagnostics

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, page 5-11
- Audit Trail, page 5-12
- Tech Support, page 5-12

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.

The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NDE 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:

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 limit.

Tech Support

The NAM syslog records NAM system alerts that contain event descriptions and date and time stamps, 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, page 5-12.

This information is unlikely to be meaningful to the average user. It is intended to be used by the Cisco TAC for debugging purposes. You are not expected to understand this information; instead, you should save the information and attach it to an email message to the Cisco TAC.

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 Editing a User, page 5-15.

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 tech support:

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

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window.

**Step 2** To save the information, either select **File > Save As...** from the browser menu, or scroll to the bottom, click on **NAM-logs.tar.bz2**, and save it to your local PC.

**Downloading Core Files**

To download core files from the Tech-Support page, scroll down to the Core Files section and click on the filename and follow the instructions.

---

**User Administration**

The User Administration option of the **Administration** menu provides the following options:

- Local Database, page 5-13
- Establishing TACACS+ Authentication and Authorization, page 5-16
- Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 5-17
- Current User Sessions, page 5-21

**Local Database**

When you first install the NAM, you 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, you can create additional accounts, enabling or disabling different levels of access independently for each user.

**Table 5-6** provides information about **User Privileges** and describes each privilege.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccountMgmt</td>
<td>Enables a user to create, delete, and edit user accounts.</td>
</tr>
<tr>
<td>SystemConfig</td>
<td>Enables a user to edit basic NAM system parameters such as IP address,</td>
</tr>
<tr>
<td></td>
<td>gateway, HTTP port, and so on.</td>
</tr>
<tr>
<td>Capture</td>
<td>Enables a user to perform packet captures and manage capture sessions Use</td>
</tr>
<tr>
<td></td>
<td>the NAM protocol decode.</td>
</tr>
<tr>
<td>AlarmConfig</td>
<td>Enables a user to create, delete, and edit alarms on the switch/router and</td>
</tr>
<tr>
<td></td>
<td>NAM.</td>
</tr>
</tbody>
</table>
User Administration

Chapter 5 Performing User and System Administration

User Administration

For additional information about creating and editing users, see Creating a New User, page 5-14 and Editing a User, page 5-15.

Resetting Passwords

You can recover passwords by using CLI commands on the switch or router. A user with appropriate privileges can reset the NAM CLI and passwords to the factory default state.

For information on resetting the NAM passwords, see your platform installation guide on Cisco.com.

If you have forgotten the NAM administrator password, you can recover it using one of these methods:

- If other users have account management permission, delete the user for whom you have forgotten the password; then create a new one by logging in as that other user by choosing Admin > Users > Local Database.
- If no other local users are configured other than the user for whom you have forgotten the password, use the NAM rmwebusers CLI command; 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 5-6 for an explanation of user privileges. Table 5-7 describes the fields in the New User Dialog Box.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>MonitorConfig</td>
<td>Enables a user to create, delete, and edit the following:</td>
</tr>
<tr>
<td></td>
<td>- Collections and reports</td>
</tr>
<tr>
<td></td>
<td>- Protocol directory entries</td>
</tr>
<tr>
<td></td>
<td>- Protocol groups</td>
</tr>
<tr>
<td></td>
<td>- URL-based applications</td>
</tr>
<tr>
<td>MonitorView</td>
<td>Enables a user to view monitoring data and reports (granted to all users).</td>
</tr>
</tbody>
</table>
Usernames and passwords cannot exceed 32 characters and can be alphanumeric. The following special characters are not allowed:

- Greater than (<)
- Less than (>)
- Comma (,)
- Period (.)
- Double quote ("")
- Single quote ('')
- Left or right parentheses
- Other special characters (!,@,$,%,^,&,*)

**Table 5-7 New User Dialog Box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The account name</td>
<td>Enter the user’s account name.</td>
</tr>
<tr>
<td>Password Verify</td>
<td>The account password</td>
<td>Enter a password that adheres to your site security policies.</td>
</tr>
<tr>
<td>Privileges</td>
<td>Privileges associated with this account</td>
<td>Select each privilege to grant to the user.</td>
</tr>
</tbody>
</table>

Users can edit their configuration by following these steps:

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

**Step 2**
Select the username.

**Step 3**
Click **Edit**.

**Step 4**
In the Modify Users dialog box, change whatever information is necessary.

Click **Submit** to save your changes, or click **Reset** to clear the dialog of any characters you entered.

**Deleting a User**

To delete a user:

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

The Users table displays.
**Step 2** Select the username.

**Step 3** Click **Delete**.

---

**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.

---

**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 the **TACACS+ Authentication and Authorization Dialog Box** (Table 5-8).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TACACS+ Authentication and Authorization</td>
<td>Determines whether TACACS+ authentication and authorization is enabled.</td>
</tr>
<tr>
<td></td>
<td>• To enable, check the check box.</td>
</tr>
<tr>
<td></td>
<td>• To disable, uncheck the check box.</td>
</tr>
<tr>
<td>Primary TACACS+ Server</td>
<td>Enter the IP address of the primary server.</td>
</tr>
<tr>
<td>Backup TACACS+ Server</td>
<td>Enter the IP address of the backup server (optional).</td>
</tr>
<tr>
<td>Note</td>
<td>If the primary server does not respond after 30 seconds, the backup server will be contacted.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the TACACS+ secret key.</td>
</tr>
<tr>
<td>Verify Secret Key</td>
<td>Reenter the TACACS+ secret key.</td>
</tr>
</tbody>
</table>
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 5.1 and later releases support 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.

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**, page 5-17.
- Add a NAM user or user group. See **Adding a NAM User or User Group for Version 4.2**, page 5-18.

### 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.
Chapter 5  Performing User and System Administration

User Administration

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.

- 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, page 5-19.
- Add a NAM user or user group. See Adding a NAM User or User Group for Version 5.x, page 5-19.
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.

**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, page 5-19** 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) and 5.2 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 select the checkbox **Permit any command that is not in the table below**.
Step 2  Click **Submit** when you have completed entering the NAM command sets (see . Ensure you include all of the following commands:

- permit capture
- permit system
- permit collection
- permit account
- permit alarm
- permit view

![Figure 5-1  NAMFullAccess Command Set Example](image)

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

Go to **Access Policy > Access Services > namAdmin > Authorization**. Replace namAdmin with the service you created in this step.

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 4  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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>shell</td>
</tr>
<tr>
<td>cmd</td>
<td>web</td>
</tr>
<tr>
<td>cmd-arg</td>
<td>One or more the following: accountmgmt system capture alarm collection view</td>
</tr>
<tr>
<td>password authentication method—Password Authentication Protocol (PAP)</td>
<td>pap</td>
</tr>
</tbody>
</table>

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 5-9) displays.
Out-of-Band Management

There are several tasks for which you should use the Prime NAM 2300 series appliances’ management interface known as the Cisco Integrated Management Controller (CIMC). You can use this out-of-band management GUI tool by connecting to LAN port 1 (which provides external system console access to both the CIMC and NAM management port).

Table 5-10 provides details about the tasks you can use the CIMC to perform. You can also access the CIMC online help by selecting the help button on the window’s task menu.

Table 5-10 When to Use CIMC

<table>
<thead>
<tr>
<th>CIMC Menu</th>
<th>Management Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power On Server</td>
<td>Power on the appliance</td>
</tr>
<tr>
<td>Power Off Server</td>
<td>Power off the appliance</td>
</tr>
<tr>
<td>Shut Down Server</td>
<td>Shut down the appliance</td>
</tr>
<tr>
<td>Power Cycle Server (instead of pulling out the power plug)</td>
<td>Immediately power off the server and power it on again.</td>
</tr>
<tr>
<td>Hard Reset Server—reboots the appliance.</td>
<td>Reboot the appliance.</td>
</tr>
</tbody>
</table>
| Launch KVM Console                       | • View the serial console remotely without any connection to a terminal server  
                                            | • Perform a recovery/ISO install                      |
| Turn On Locator LED/Turn Off Locator LED | Locate the physical appliance in a rack using a blinking LED. |
| See Server Properties in the Server Summary view. | Access appliance information such as the serial number, product ID, and BIOS version. |

For additional details, see the Cisco Integrated Management Controller online help. We recommend you use the CIMC GUI, but if desired you can access the CIMC CLI. For details on other CIMC documentation, see the Documentation Overview.

To review CIMC setup details, see the Cisco Prime NAM 2300 Series Appliances Installation and Configuration Guide.
Understanding NAM Deployment

This chapter describes information 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 5.1(3). This chapter contains the following sections:

- Network Performance Management Lifecycle, page 6-1
- Places in the Network Where NAMs Are Deployed, page 6-2
- Use Cases, page 6-7

Network Performance Management Lifecycle

In any network, the administrator must define normal and abnormal behavior patterns. Once this is accomplished, the goal is to maintain the network in its normal state and take any actions needed to prevent it from going into an abnormal state. When such an abnormal situation occurs, such as an outage, tools must be available to quickly isolate and fix the problem.

*Figure 6-1 The Network Performance Management Lifecycle*
Figure 6-1 depicts the Operational Network cycle that is at the center of where the network should ideally be at all times. The other two cycles indicate the process of repairing a network problem and the process of planning a change to the network. The following is a brief outline of the performance management lifecycle:

1. **Recognize and list your network performance goals**—This includes setting expected limits for response time, expected ranges for MOS values, bandwidth usage per application, and utilization on critical WAN links. The importance of these metrics is closely related to your specific network; for example, an enterprise with a large number of branches and a small main campus might focus on WAN utilization, whereas an enterprise with one main campus and one large branch with users that use collaboration tools across the two will likely focus on application performance metrics such as response time measurements.

2. **Create a baseline of current network performance metrics**—The NAM can help document a variety of these baseline 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. These measurements might meet or exceed your expectations in step 1. It might be worthwhile to revisit the expectations set in step 1 and check whether some refinements are necessary (for example, 80 percent utilization on the WAN link may be quite acceptable, whereas the real reason behind application delays seems to be bursts of unrecognized traffic. In this case, one might be lenient on WAN link utilization and focus more on QoS-related issues).

3. **Enforce policies using alarms, syslogs, traps, and email alerts**—NAM can provide alerts by email, traps and syslogs. These tools must be configured such that the normal functioning range of the network is demarcated. If any of the tracked metrics show values that are outside this normal range, then the NAM can be used to send alerts as appropriate. The information stored on the NAM is openly available to applications. It is recommended that any enterprise-wide network management tools and monitoring applications be configured to receive alerts from NAM. The NAM is then able to act as a network sentinel and warn proactively about a host of issues and also provide access to rapid troubleshooting when problems occur.

The goal is for all important network metrics to be within the normal ranges. But knowing the normal range of the network is a constant learning process, and as the network evolves and grows, it can be a moving target. Therefore the lifecycle described above is a continuous process of fine-tuning the network and the metrics that are most important to normal behavior.

**Places in the Network Where NAMs Are Deployed**

Because NAM is available in various form factors, it allows significant flexibility in deployment. At the same time, the available NAMs must be deployed in locations that are most effective in helping you monitor, measure, and report on the network’s health. Any location that is the ingress or egress point of a logical network boundary (aggregation layer, core, campus edge, and so on) can offer valuable insights into the network activity within that partition. Therefore, such boundary locations are usually good choices for NAM deployment.

Figure 6-2 shows various possible locations at which NAMs can be deployed. The access and distribution layers, the data center, WAN edge, and branch office are all valid choices, and you should make deployment decisions based on the specific issue at hand. The following is a list of common places in the network where NAMs are deployed and the information available at each place:
Chapter 6  Understanding NAM Deployment

Places in the Network Where NAMs Are Deployed

- **Data center**—Over the past few years, data center consolidation has been a common theme across enterprises. The centralized data center becomes a critical hub of activity within the enterprise network and helps cut costs, focus IT efforts in one location, and offer a rich variety of services across the enterprise. Placing a NAM in such data centers offers excellent visibility into the most business-critical applications and transactions.

- **Server farms**—Place near server farms (web, FTP, and Domain Name System [DNS], for example), data centers, or near IP telephony devices (Cisco Unified Communications Manager), IP phones, and gateways where the Cisco NAM can monitor request-response exchanges between servers and clients and provide rich traffic analysis, including IAP.

- **Campus and WAN edge**—This location is very often a good choice—it offers visibility into traffic entering and exiting the campus. It provides a central point from which to measure voice quality of all streams leaving the campus and going across the WAN. The WAN is typically the smallest bandwidth link, and therefore, call metrics such as latency, jitter, and so on might require close monitoring for deterioration in quality. It is also an excellent location to measure WAN utilizations and health metrics of various branch routers using NetFlow. Place Cisco NAMs at the WAN edge to gather WAN statistics from the Optical Services Module (OSM) or FlexWAN interfaces or to collect NetFlow statistics on remote NetFlow-enabled routers. This can provide usage statistics for links, applications (protocol distributions), hosts, and conversations, which can be useful for trending data and capacity planning.

- **Branch office**—Place Cisco NAMs at the edge of the branch office to troubleshoot issues at remote sites. This place offers the advantage of visibility into all traffic crossing the branch boundary. Headquarters personnel can troubleshoot issues remotely through the NAM GUI.

- **Distribution layer**—The distribution layer is typically a convergence point for traffic from smaller networks; for example, three buildings of a company might feed into a distribution layer switch. Placing the Cisco NAMs at the distribution layer allows visibility into the application trends specific to that set of buildings. In troubleshooting situations, you might start working with an edge NAM and then log in to a distribution NAM to isolate and fix the problem. Also, it is a good location to capture RTP voice streams. If phone calls in one building in the campus need to be monitored for quality, the aggregation layer is a good choice, as the switch in this layer will typically “catch” all calls being made in that building.

- **Access layer**—The access layer is the layer closest to users and is not a typical location for NAMs. However, with the rapid increase in network traffic over the years, it has become somewhat common to have Cisco Catalyst 6500 Series Switches in the closet of each floor. Cisco NAMs can be very useful, especially for those access layer switches that serve critical companywide meetings or conferences and other business-critical needs. Once again, close monitoring of IP phones is a good application in this layer as well.
Choice of Hardware and Software Platforms for a Given Place in the Network

Depending on the usage scenario and the location in which the NAM will be deployed, you must make a decision on the type of NAM platform to deploy. This section provides the necessary background and details to make such deployment decisions. See Table 1 for a summary of NAM platforms. Please refer to http://www.cisco.com/en/US/products/ps5740/Products_Sub_Category_Home.html for further information regarding the different platforms.
### Table 6-1 NAM Platforms

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Description</th>
<th>Related Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NAM-1/-2 blade</td>
<td>The NAM-1 and NAM-2 blade fits into any slot on a Catalyst 6500 or Cisco 7600. The NAM-2 blade has two data ports. These ports connect directly to the switching fabric and are not externally visible. Each port can support one SPAN session. Therefore, the NAM-2 blades support a total of two SPAN sessions, while the NAM-1 blades support one SPAN session.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product types:</td>
<td>- WS-SVC-NAM-2-250S</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- WS-SVC-NAM-1-250S</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- WS-SVC-NAM3-6G-K9</td>
</tr>
<tr>
<td></td>
<td>Typical PINs: Data center, core, and distribution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note If required, currently owned NAM-1 and NAM-2 (without -250S suffix) cards can be upgraded using a memory upgrade kit. The kit essentially provides an upgrade to the RAM on your NAM cards and offers an easy way to meet the performance needs of NAM software while allowing continued use of the existing NAM hardware investment. The memory kit only upgrades RAM and not the hard drive.</td>
<td></td>
</tr>
<tr>
<td>Cisco NAM-3</td>
<td>The NAM-3 blade fits into any slot on a Catalyst 6500.</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td>The NAM-3 blade has two data ports. These ports connect directly to the switching fabric and are not externally visible. Each port can support one SPAN session. Therefore, the NAM-3 blades support a total of two SPAN sessions.</td>
<td>- WS-SVC-NAM3-6G-K9</td>
</tr>
<tr>
<td></td>
<td>Typical PINs: Data center, core, and distribution</td>
<td></td>
</tr>
<tr>
<td>Cisco NAM Branch module</td>
<td>The NAM on SM-SRE takes up a module slot on a Cisco 2900 or Cisco 3900 Integrated Services Router (ISR G2). The NME-NAM takes up a module slot on a Cisco 2800 or Cisco 3800 Integrated Services Router (ISR). The NME-NAM (with adapter) takes up a module slot on a Cisco 2900 or Cisco 3900 Integrated Services Router (ISR G2). This module has one internal and one external port. The internal interface receives traffic forwarded from router interfaces, while the external interface can be used to connect to wire taps.</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SM-NAM-SW-5.1-K9 - Cisco Prime NAM Software for ISR G2 SRE – NAM on SM-SRE 700 and SM-SRE 900</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- NME-NAM-120S</td>
</tr>
<tr>
<td></td>
<td>Typical PINs: Campus edge, branch edge, WAN edge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note Because the network modules have an internal and an external port, they provide the flexibility to monitor packets from a router interface or directly tap into traffic from an external device using the external Ethernet port.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6      Understanding NAM Deployment

Places in the Network Where NAMs Are Deployed

A Note on the Cisco NAM Appliances

In addition to the existing platforms on which the NAM can be installed, the NAM software is also available as an appliance. The addition of the appliance to the NAM product line provides increased flexibility and higher performance. The appliances are available in two varieties. The Cisco NAM 2x20 Appliance offers the best performance in the NAM product line. The product contains two 10-Gigabit Ethernet ports that are ideally suited to the high-bandwidth data center and core environments. The Cisco NAM 2x04 Appliance contains four 1-Gigabit Ethernet ports, available both in copper and fiber, and allows flexible deployment in a variety of locations across the network.

The NAM appliance serves as a complement to the network module implementations of the NAM. The network modules (or cards) reside within an ISR, Catalyst 6500 Series Switch, or Cisco 7600 Series Router, and offer an integrated solution. Such integration saves rack space and power, eliminates the need for additional cabling, and efficiently monitors device traffic with no network overhead. Still, there are situations where an appliance is preferred. For example, you may wish to monitor a Catalyst 4500 Series Switch or a Nexus 7000 Series Switch that does not support NAM network modules. Or, you may wish to connect the NAM to multiple switches in parallel as you build a new segment in the network. This can be achieved easily with the NAM 2204 Appliance, which has four ports that can each be connected to different devices. Or, you may want to monitor traffic from a couple of core routers that feed into the data center, and therefore require 10-Gigabit Ethernet ports. The Cisco 2320 Appliance might be ideally suited for this scenario. The addition of the appliances to the NAM product line provides users with additional flexibility in deploying the appropriate NAM hardware depending on the location in the network.

Table 6-1       NAM Platforms

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Description</th>
<th>Related Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NAM 2304/2204 Appliance</td>
<td>The midrange appliance has four 1 Gigabit Ethernet ports, available either as copper or optical interfaces. Appliances offer the flexibility to deploy NAMs with any Cisco device irrespective of platform. 1 rack unit.</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM2304-RJ45 - Cisco NAM 2304 Appliance, four 1 GB Ethernet, RJ-45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM2304-SFP - Cisco NAM 2304 Appliance, four 1 GB Ethernet, SFP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Typical PINs: Data center, core, campus edge</td>
</tr>
<tr>
<td>Cisco NAM 2320/2220 Appliance</td>
<td>The NAM high-end appliances offer two 10 Gigabit Ethernet ports. 2 rack unit.</td>
<td>Product type—NAM2320 – Cisco NAM 2320 Appliance, two 10 GB Ethernet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The 2320 appliance is NAM’s high-end hardware platform and is best suited to handle the high performance required in data center and core networks.</td>
</tr>
<tr>
<td>Cisco PRIME NAM Virtual Blade on WAAS</td>
<td>The NAM Virtual Blade is software residing on a Cisco WAVE-574 and WAE-674 appliances</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM-WAAS-VB – VB on WAAS appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAAS-VB-NAM5.1-K9 – software for WAAS 574/674</td>
</tr>
<tr>
<td>Cisco PRIME NAM Virtual Service Blade on Nexus 1010</td>
<td>NAM Virtual Service Blade is a software that resides in Nexus 1010 providing visibility into Nexus 1000V switch.</td>
<td>Product type—N1K-C1010NAM51-K9 - Cisco Prime NAM Software 5.1 for Nexus 1010</td>
</tr>
</tbody>
</table>
Enhanced performance also provides other deployment benefits. For example, the number of voice streams supported by the NAM is an important consideration while planning for voice over IP quality monitoring. Other limits include the number of NetFlow records processed per second, buffer sizes available for packet capture, number of WAE devices that send WAN optimization data to NAM, and in general, monitoring performance under load.

The appliances are not integrated into the Cisco infrastructure, but they do support some of the features that the integrated NAM modules bring. On the integrated Catalyst 6500 NAM cards, you may have used the ability to poll MIBs on the supervisor and collect statistics on important aspects such as switch CPU health, interface traffic, utilization, and so on. The appliance defines the concept of a “managed device” that achieves the same result for the device being monitored. You will need to choose one of the Cisco devices (supported platforms include Catalyst 6500, Cisco 7600, and Catalyst 4500 Series devices) being monitored by the appliance as your managed device. The NAM appliance will be able to poll MIBs on this managed device and obtain relevant performance troubleshooting information just like the NAM cards. Also available is the ability to configure SPAN sessions on the managed device through the NAM GUI on the appliance. Credentials to access the managed device need to be configured in order for these capabilities to be enabled.

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

Use Cases

The following 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 Chapter 1, “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 the following categories:

- Data Center
- Campus
- Branch
- General Usage Scenarios
- NAM Integrations with Monitoring and Reporting Applications

Data Center

- Monitoring the Nexus 1000V Switch Environment, page 6-29
- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-16
Deployment Examples

**Campus**

- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Using NAMs to Monitor VoIP Quality, page 6-9

**Branch**

- Visibility in the Branch, page 6-15
- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-16
- Using NAMs to Monitor VoIP Quality, page 6-9

**General Usage Scenarios**

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

- Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment, page 6-12
- Using NAM for Historical Trends via Interactive Report, page 6-26
- Using NAM for Problem Isolation, page 6-33
- Creating Custom Applications, page 6-12
- Autodiscovery Capabilities of NAM, page 6-11
- Using NAM for SmartGrid Visibility, page 6-33

**NAM Integrations with Monitoring and Reporting Applications**

- Integrating NAM with LMS, page 6-14
- Integrating NAM with Third Party Reporting Tools, page 6-14

**Deployment Examples**

- Using NAMs to Monitor VoIP Quality, page 6-9
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 Multiprotocol 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 (as shown in Figure 6-3) 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 in Figure 6-3 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 6-4, 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.
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.


Autodiscovery Capabilities of NAM

If you are an existing NAM 4.x user, you will not need to configure the SPAN sessions, and they will be autocreated 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 Data Sources, page 2-13.
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 Applications, page 2-74.

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

Cisco Prime NAM has the capability for users to define a site, with which you can aggregate and organize performance statistics. A site is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems. 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). 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 6-5 shows a centralized NAM deployment analyzing multiple data sources from different locations in the network.

For this deployment, multiple sites can be created such as SanJose-Campus, SanJose-Datacenter, NewYork-NDE-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.
Figure 6-6 shows a list of the sites configured for this deployment.

**Figure 6-6 Sites Table**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Unclassified hosts</td>
<td>Catches All Unclassified Hosts</td>
</tr>
<tr>
<td>N1K-ERSSPAN</td>
<td></td>
<td>192.168.154.8/24 ERSSPAN-192.168.154.18-ID-1</td>
</tr>
<tr>
<td>New York - NDE</td>
<td></td>
<td>2.0.0.08 NDE-192.168.192.2-ID-0</td>
</tr>
<tr>
<td>New York-WAAS-Eloig2</td>
<td></td>
<td>WAAS client side</td>
</tr>
<tr>
<td>San Jose-Campus</td>
<td></td>
<td>192.168.6.015 DATA PORT 3</td>
</tr>
<tr>
<td>San Jose-Datacenter</td>
<td></td>
<td>192.168.154.8/24 DATA PORT 3</td>
</tr>
<tr>
<td>VOIP-RTP</td>
<td></td>
<td>1.0.0.08 DATA PORT 3</td>
</tr>
<tr>
<td>VOIP-San Jose</td>
<td></td>
<td>2.0.0.08 DATA PORT 3</td>
</tr>
<tr>
<td>WAAS Senet</td>
<td>WAAS server side</td>
<td>WAES-192.168.156.205-SWYAN ...</td>
</tr>
<tr>
<td>WAASServerPassthru</td>
<td></td>
<td>WAAS Sener Passthru</td>
</tr>
<tr>
<td>WAASServerPassthru</td>
<td></td>
<td>192.168.156.205-Seidentifier Passthru</td>
</tr>
</tbody>
</table>

The interactive dashboard can be used to drill down into either San Jose or New York sites to see Top applications, hosts, VLANs, DSCP, and application response time (as seen in Figure 6-7).

**Figure 6-7 Traffic Summary Dashboard**

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, conversation and VLAN traffic.
Figure 6-8 shows the contextual drilldowns from the Top N Applications and Top N Hosts charts.

Figure 6-8  Applications and Hosts Drilldowns

See Sites, page 2-65.
See Site Definition Rules, page 2-66.

Integrating NAM with Third Party Reporting Tools

Prime NAM 5.1(3) integrates with the CA NetQoS SuperAgent for the purpose of aggregating Application Response Times. Prime NAM 5.1(3) also integrates with CompuWare Vantage and InfoVista 5View for Host, Conversation, RTP, and Response Time.

See the NAM 5.1 API Programmer’s Guide for configuring NAM and exporting data from the NAM (ask your Cisco representative).
See Response Time Summary.

Integrating NAM with LMS

The NAM GUI can be placed on the LMS (LAN Management Suite) 4.0 dashboard and accessed through the LMS GUI. See technical documentation for LMS on http://www.cisco.com.

Currently, this functionality includes:
• NAM discovery as part of the network topology that LMS builds
• NAM alarms persistent in LMS
• Ease of software updates to multiple NAMs via LMS
• Portal Integration to bring in NAM GUI inside of LMS

You can also check out supported devices for LMS to see what features of FCAPS are covered by what type of NAM:

Chapter 6 Understanding NAM Deployment

Deployment Examples

See Figure 6-9 for a view of the NAM GUI being accessed through LMS GUI.

**Figure 6-9 NAM GUI Available In the LMS GUI**

Visibility in the Branch

There are three options for providing visibility in the branch:

1. A purpose-built NME-NAM-120S that works in Cisco Integrated Service Router Generation 1
2. NAM as an application, running in SM-SRE-7xx or SM-SRE-9xx for Cisco Integrated Service Router Generation 2 (ISR G2) deployment
3. Using Performance Agent (PA), a Cisco IOS feature available on ISR G2 that encapsulates traffic statistics as well as application response statistics. Underlying Netflow v9 can be exported to a central NAM in a Data Center (DC) or Campus. PA complements WAAS Express (another IOS feature) and when used together, delivers end-to-end visibility before and after WAN Optimization using only one traffic source, as compared to two traffic sources NetFlow and WAAS Flow Agent from the traditional WAAS deployment in the branch. See the scenario Monitoring Cisco WAAS and Measuring Its Impact, page 6-16.
The first two options are similar and provide visibility for the local branch as well as branch to branch and the ability to capture all traffic going in and out of the branch.

Ideal deployment for these branch NAM modules would be a small number of remote sites or an empowered branch. The third option provides visibility only for the local branch and is more scalable than deploying NAM modules in multiple remote locations e.g. 100's/1000's remote sites. Based on network monitoring and troubleshooting requirements, a hybrid option can be considered such as deploying NAM modules and PA in empowered branches and PA in smaller branches. In this model, a central NAM in the DC can provide end to end visibility from DC to branch and offers the ability to capture branch to branch traffic on super branches (empowered branch).

For further details on installing NAM on NME-NAM-120S or SM-SRE, see the Installation Guides on Cisco.com. For further details on configuring PA, see Chapter 2, “Setting Up the Cisco NAM”. For further details about the NAM 5.1(3) release, see the Cisco Prime NAM 5.1(3) Release Notes on www.cisco.com.

See related content Response Time Summary and Analyze, Response Time.

### 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 or Performance Agent (PA) as data sources. 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 or NAM-2 blade 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, or PA with WAAS Express from an ISR G2 branch router. If NME-NAMs are available, deploying one at the remote branch site is very useful. This NME-NAM can provide user experience at the site before WAAS is enabled and then contrast it to user experience after WAAS is enabled. See Figure 6-10.
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**. As shown in **Figure 6-11**, this will display such data as utilization, concurrent connections, and average transaction time for top applications, network links, clients, and servers that are possible candidates for optimization.

**Figure 6-11  Top Talker Detail -- Non-Optimized**

**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 6-12 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 6-12  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.
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 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.

See related content WAN Optimization.

Monitoring

- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Using NAM for Historical Trends via Interactive Report, page 6-26
Real-Time Traffic Monitoring and Analysis

One of your Network Operations Center (NOC) responsibilities is to monitor the campus network and two branch offices and follow up on any abnormalities that you find in these networks.

The following steps lead you through managing a NAM-2 blade located in the Cisco Catalyst 6500 Series Switch at the campus edge. There is local SPAN and remote NDE traffic being monitored by this NAM. You have defined sites based on those data sources.

**Step 1**
On the Traffic Summary dashboard (Monitor > Overview > Traffic Summary), use the Interactive Report and the Filter button on the left side of the screen to narrow the data on the dashboard to a particular site. Then, you will be able to view the Top Applications, Hosts, VLANs, and DSCP for that site. Take note of the Top Host, or in other words, top bandwidth generator (see Figure 6-14).

**Step 2**
Click on the Top Applications graph to drill down to see all the hosts using the GRE application. Notice that this application traffic is being generated by three hosts (see Figure 6-15).
Step 3 Go back to Traffic Summary > Top N Hosts In and Out and click on the host (in the example shown in Figure 6-15, “192.168.152.10”).

Step 4 Select Analyze > Traffic > Host to see how long this host and application have been generating this traffic. The Time Range can be changed using the Interactive Report and the Filter button on the left; a shorter or longer period of time may be needed to understand the pattern and trend.

Step 5 Based on those patterns, thresholds can be configured to alert via e-mail, trap, and syslog. The alert can be used to start a packet capture as well. On the context menu (found by left-clicking on the colored bar), there is an option to initiate a packet capture if desired (see Figure 6-17).
Chapter 6  Understanding NAM Deployment

Monitoring

Figure 6-17  One-click Packet Capture

Although the NAM was deployed at the campus edge, other possible locations that offer similar information include the core, distribution (NAM-2 or appliance), and branch office (NME-NAM). This use case illustrates some of the benefits of real-time analysis. You were able to study applications and conversations in real time and were able to take a capture of a particular stream that was of interest. See Application Response Time, page 3-22.

See Alarm Actions, page 2-44.

See Thresholds, page 2-47.

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 6-18). The voice template can be used to monitor whether voice traffic is marked properly. Figure 6-20 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 6-18 Default DSCP Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>DSCP Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF_EF</td>
<td>DSCP 10, DSCP 12, DSCP 14, DSCP 18, DSCP 20, DSCP 22, DSCP 26, DSCP 28, DSCP 30, DSCP 34, DSCP 36, DSCP 38, DSCP 46</td>
</tr>
<tr>
<td>CiscoVoice</td>
<td>DSCP 25, DSCP 46</td>
</tr>
<tr>
<td>ToS0</td>
<td>DSCP 0, DSCP 1, DSCP 2, DSCP 3, DSCP 4, DSCP 5, DSCP 6, DSCP 7</td>
</tr>
<tr>
<td>ToS1</td>
<td>DSCP 8, DSCP 9, DSCP 10, DSCP 11, DSCP 12, DSCP 13, DSCP 14, DSCP 15</td>
</tr>
<tr>
<td>ToS2</td>
<td>DSCP 16, DSCP 17, DSCP 18, DSCP 19, DSCP 20, DSCP 21, DSCP 22, DSCP 23</td>
</tr>
<tr>
<td>ToS3</td>
<td>DSCP 24, DSCP 25, DSCP 26, DSCP 27, DSCP 28, DSCP 29, DSCP 30, DSCP 31</td>
</tr>
<tr>
<td>ToS4</td>
<td>DSCP 32, DSCP 33, DSCP 34, DSCP 35, DSCP 36, DSCP 37, DSCP 38, DSCP 39</td>
</tr>
<tr>
<td>ToS5</td>
<td>DSCP 40, DSCP 41, DSCP 42, DSCP 43, DSCP 44, DSCP 45, DSCP 46, DSCP 47</td>
</tr>
<tr>
<td>ToS6</td>
<td>DSCP 48, DSCP 49, DSCP 50, DSCP 51, DSCP 52, DSCP 53, DSCP 54, DSCP 55</td>
</tr>
</tbody>
</table>

DSCP: Differentiated Service Code Point
Step 2  Choose Analyze > Traffic > DSCP to find any misclassified traffic. In Figure 6-19, the RTP protocol is displayed for ToS0 classification.

Figure 6-19  DSCP Group - ToS0

Step 3  Click on the All DSCP button to view all DSCP and applications.
Step 4  In Figure 6-20, 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.

![All DSCP Table](image)

Step 5  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 6-21, 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.
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 rollouts, 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 HTML format. See Figure 6-22.
Figure 6-22 Interactive Report

Figure 6-23 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 6-23 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 an NME-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 6-24).

![Figure 6-24 A Stream with a Mildly Increasing Trend](image)

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 6-25). 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 6-25 The Trend Shown with a Granularity of 1 month](image)

Studying historical trends is a valuable exercise in planning and baselining 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 3-22.
See Thresholds, page 2-47.

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

The NAM monitors RTP streams: When a phone call ends, the endpoints calculate the information and send it to the Call Manager. If a NAM is along that path, it will intercept it.

The NAM monitors and analyzes RTP streams and voice calls statistics from the endpoint. The voice calls statistics from the endpoint is used in conjunction with the RTP stream to correlate the phone number with the IP address of the endpoint. Alerting is based on analysis of the RTP streams for MOS, Jitter, and Packet Loss.

See Table 2-40, Voice Monitor Setup Window.

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 6-26.

The Nexus 1000V switch can also be monitored by other NAM platforms running the NAM 5.1 software.

In this scenario, there are two options:

- You are deploying applications in the virtualized 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.
- You have a NAM-2 deployed in the data center switch and a Nexus 1000V switch for the virtualized environment, and you want to monitor the virtual switch traffic.
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.

To monitor the Nexus 1000V environment:

**Step 1** Install and configure either the NAM VSB on the Nexus 1010 Virtual Services Appliance or the Nexus switch to the NAM-2. See the Installation and Configuration Guides for the NAM on Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html

**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. Figure 6-27 shows the Traffic Summary window, which displays Top N information such as applications, hosts, protocol, and server response time. Navigation is provided to view and display details for each of the categories listed.
4. Using the Interactive Report on the left side of the window, configure reports for trending on the application response time, hosts, and conversation traffic patterns.
5. The physical and virtual interfaces table provides VM-to-VM traffic utilization (Figure 6-28). 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.

Step 3: For other NAM platforms running version 5.1 (NAM-2):

1. Configure the Nexus 1000V Switch to direct ERSPAN or NetFlow to the NAM-2.
2. Verify that ERSPAN or NetFlow are configured on the Cisco 1000V Switch Virtual Supervisor Module (VSM) that is providing data to NAM by choosing Setup > Traffic > NAM Data Sources.
3. Create a site for this data source using Setup > Network > Sites (Figure 6-29).
4. Choose Monitor > Overview > Traffic Summary (as shown in Figure 6-30) and Monitor > Overview > Response Time Summary.

**Troubleshooting**

- Using NAM for Problem Isolation, page 6-33
- Using NAM for SmartGrid Visibility, page 6-33
- Real-Time Traffic Monitoring and Analysis, page 6-20
Using NAM for Problem Isolation

The alarm details (found in the Cisco Prime Network Analysis Module 5.1(3) 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:

2010 SEPT 28 9:17:0:Application:Exceeded rising value(1000);packets;60653;Site(San Jose), Application(http)

After receiving this alarm, you can access the NAM GUI to view the application in site San Jose 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: Response Time Summary, page 3-5.
See Analyze: 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.
Troubleshooting

This appendix addresses some common issues you might encounter while using Cisco Prime Network Analysis Module 5.1(3).

It contains the following sections:

- General NAM Issues, page A-1
- Error Messages, page A-2
- Packet Drops, page A-2
- NAM Not Responding, page A-2
- NAM Behavior, page A-3
- WAAS Troubleshooting, page A-3
- Performance Agent (PA), page A-4

General NAM Issues

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 is seated correctly in chassis
- Reset NAM
- Reset into maintenance image or helper
- Clear the configuration
- Reinstall the application image (possibly with the repartition option --install)
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 (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.

Q. What does the message “Client or NAM time is incorrect” mean?
A. The browser or client time and the NAM time must be synched to avoid this error.

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
```

<table>
<thead>
<tr>
<th>Time</th>
<th>hardware pkts dropped</th>
<th>FM pkts dropped</th>
<th>ART pkts dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:05</td>
<td>3548</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:10</td>
<td>3354</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:15</td>
<td>2843</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:20</td>
<td>2629</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:25</td>
<td>3592</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:30</td>
<td>3298</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:35</td>
<td>1823</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13:40</td>
<td>2549</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

NAM Not Responding

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`

Q. Why am I unable to change my capture session back to capture to disk after I switched it from disk to memory?

A. If you set up a capture session to disk and later modify the same packet session to be saved into memory, you are not be able to change the selection back to disk since the storage for packet capture is In Use state. You cannot delete the capture session because the disk for capture is not released. The only workaround is to reboot the Prime NAM.

**NAM Behavior**

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 browser that is supported with NAM 5.x (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. Can I change the type of capture storage option from disk to memory, then back again to disk?

A. If you set up a capture session to disk and later modify the same packet session to save into memory, then attempt to change it back again to disk, Prime NAM is unable to change the storage selection back to disk because it is in "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.

**WAAS Troubleshooting**

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.

**Performance Agent (PA)**

Q. Why is the NAM not receiving data from PA?

A. First troubleshoot Flexible NetFlow (FNF). Check whether FNF sent data to the NAM with `show flow exporter statistics`.

If FNF did not send data, check Performance Agent with `show mace metrics summary`. Check whether flows are exported.

If flows are not exported by PA, debug PA to identify the error with `debug mace cp`. 
Supported MIB Objects

Table B-1 lists the MIB objects supported by the NAM.

<table>
<thead>
<tr>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB-II: All groups except Exterior Gateway Protocol (EGP) and transmission.</td>
<td>RFC 1213</td>
</tr>
<tr>
<td>CDP-MIB: Cisco Discovery Protocol</td>
<td></td>
</tr>
<tr>
<td>EntityMIB</td>
<td>RFC 2737</td>
</tr>
</tbody>
</table>

Note: The CISCO-RMON-CONFIG-MIB is not currently supported in the Nexus 3K, 5K, and 7K.
INDEX

A

access policies, setting in ACS 5.x 5-19
access policy configuration, ACS v5.x 5-19
administration (see system administration) 5-1
alarm thresholds, setting
  NAM thresholds 2-47
deleting 2-56
editing 2-55
switch thresholds 2-56
syslog, setting up 5-9
ART 3-24, 3-27
Audit trail 5-12

C

capture
  error scan 4-21
Capture buffer
  maximum buffer size 4-6
capture files
  about 4-19
  analyze 4-21
  Drill-Down button 4-21
capture sessions
  about 4-2
  configuring 4-4
  viewing 4-3
capturing data 1-9, 4-1
capture buffer
downloading to a file 4-19
capture settings, configuring 4-4
custom display filters
  creating 4-30
custom display filters, setting up 4-30
deleting 4-33
editing 4-33
packet decode information, viewing 4-27
protocol decode information, viewing 4-29
cautions
  regarding
    NAM community strings, deleting 5-5
    switch string and read-write community string matching 5-5
Cisco Prime Network Analysis Module User Guide, 5.1 i-i
community switch strings, setting and viewing 5-5
configuring NAM
  community switch strings, setting and viewing 5-5
data collection, setting up
  voice data, collecting 2-84
data sources, setting up 2-13
traffic, directing for spanning 2-13
  creating a SPAN session 2-10
  deleting a SPAN session 2-13
  editing a SPAN session 2-12
  NetFlow, configuring on devices 2-25
  NetFlow records, understanding 2-24
  SPAN sources (table) 2-8
  traffic directing methods (table) 2-8
  VACL, configuring on LAN VLANs 2-22
  VACL, configuring on WAN interfaces 2-22
Consecutive Packets Loss threshold 2-6
Console
  external reporting 2-62
Continuous capture 4-6
creating
custom display filters 4-30
NAM traps 5-10
protocol 2-75
SPAN sessions 2-10
custom display filters, managing
   creating 4-30
   deleting 4-33
   editing 4-33
   setting up 4-30

D

dashboards
   Alarm Summary 3-6
   Performance Overview 3-5
   Response Time Summary 3-5
   Traffic Analysis 3-4
data collection
   setting up
      voice data 2-84
data export from NAM 2-57
data export to NAM 1-9
data sources, setting up 2-13
data storage 4-23
deleting
   custom display filters 4-33
   DiffServ profiles 2-73, 2-78
   NAM thresholds 2-56
   NAM traps 5-11
   protocols 2-77
   SPAN sessions 2-13
diagnostics, generating 5-11
   configuration information, monitoring and capturing 5-12
   system alerts, capturing 5-12
   system alerts, viewing 5-11
DiffServ profile, managing
   creating 2-72, 2-77
   deleting 2-73, 2-78
   editing 2-73, 2-78
directing traffic for spanning 2-13
   methods (table) 2-8
   NetFlow, configuring on devices 2-25
      devices running Cisco IOS 2-25
      devices supporting multi-layer switching cache 2-25
      devices supporting NDE export 2-26
      devices supporting NDE v8 aggregations 2-26
      devices supporting vi aggregations 2-26
   NAMs in a device slot 2-26
   NetFlow devices, managing
      testing 2-33
   SPAN session
      creating 2-10
      deleting 2-13
      editing 2-12
   SPAN sources (table) 2-8
   VACL, configuring on LAN VLANs 2-22
   VACL, configuring on WAN interfaces 2-22
   DSCP groups, managing
      setting up 2-71

E

editing
   custom display filters 4-33
   DiffServ profiles 2-73, 2-78
   NAM thresholds 2-55
   NAM traps 5-10
   protocols 2-76
   SPAN sessions 2-12
   EMail alarms 2-45
   Enabling
      voice monitoring 2-84
   Encapsulation 2-81
   Encapsulation Configuration 2-81
   ERSPAN 2-21
      configuring as datasource 2-15
sending data directly to NAM 2-21

External reporting console 2-62

external storage

about 4-23
capturing 4-24
LUNs 4-24

Filtering

audit trail 5-12
IP 4-18
IP and Payload Data 4-18
IP and TCP/UDP 4-18
Payload data 4-19
VLAN and IP 4-17

Filter Response Time for all Data Sources by Monitored Servers 2-88

GPRS (General Packet Radio Service) Tunneling Protocol 2-81
GREIP 2-81
GTP 2-81

G

IGMP 1-11
interface data, viewing
detail 3-11, 3-30
IPESP 2-81
IPIP4 2-81
IP tunnel encapsulations 2-81

M

Monitored servers filters 2-88
Monitoring
  Application response times 3-27
  monitoring
    port traffic 1-11
    traffic 1-9
  monitoring data
    voice 3-14
Multiple WAAS segments
  viewing response time 3-18

N

NAM
  alarm thresholds
    deleting 2-56
    editing 2-55
    setting 2-47
  community strings, working with 5-4
    creating 5-4
    deleting 5-5
  SNMP system groups, setting and viewing 5-3
  system time, setting 5-6
    configuring with an NTP server 5-7
  diagnostics, generating for technical assistance 5-11
    configuration information, monitoring and capturing 5-12
  help
    (see also troubleshooting) A-1
  configuration information, monitoring and capturing 5-12
synchronizing with switch or router 5-6, 5-7

traps
creating 5-10
deleting 5-11
editing 5-10
setting 5-10

navigation and control elements 1-3

NetFlow
configuring on devices 2-25
Cisco IOS 2-25
multi-layer switching cache 2-25
NAMs in a device slot 2-26
NDE export 2-26
NDE v8 aggregations 2-26
devices, managing
testing 2-33
exporting data 1-11
interfaces, understanding 2-23
records, understanding 2-24

NetFlow Data Export from NAM 2-57
NetFlow Data Export to NAM 2-8

network parameters, setting and viewing 5-2

overview of NAM
navigation and control elements 1-3

Packet Loss threshold 2-6
passwords, recovering 5-14
Performance Agent
aggregation 1-12, 2-40
port traffic
monitoring 1-11
protocol directory
managing

creating protocols 2-75
deleting protocols 2-77
editing protocols 2-76

recovering passwords 5-14
Refresh button
Creating SPAN session 2-12

response time
application 3-22
client 3-23
client-server 3-23
network 3-22
server 3-22

response time data, viewing
reports
server 3-25

RTP Stream Monitoring 2-6

SCCP traffic 4-29
Server Response Time table, using
reports 3-25
sessions
SPAN 1-10, 2-7, 2-14
setting
alarm thresholds
NAM thresholds 2-47
switch thresholds 2-56
syslog 5-9
community switch strings 5-5
NAM SNMP system groups 5-3
network parameters 5-2

Single WAAS segment
viewing response time 3-18

sites
Index

adding 2-68
definition rules 2-66
editing 2-70
SPAN
sessions 1-10, 2-7, 2-14
creating 2-10
deleting 2-13
editing 2-12
spanning, directing traffic for 2-13
methods (table) 2-8
NetFlow, configuring on devices 2-25
Cisco IOS 2-25
multi-layer switching cache 2-25
NAMs in a device slot 2-26
NDE export 2-26
NDE v8 aggregations 2-26
NetFlow devices, managing
testing 2-33
SPAN session
creating 2-10
deleting 2-13
editing 2-12
SPAN sources (table) 2-8
VAACL, configuring
on LAN VLANs 2-22
on WAN interfaces 2-22
SPAN states 2-10
switch
alarm thresholds
setting 2-56
Switch Remote SPAN 2-8
Switch SPAN 2-8
syslog alarm threshold, setting up 5-9
system administration 5-1
diagnostics, generating for technical assistance 5-11
overview of system administration tasks 5-1
NAM community strings, working with 5-4
NAM SNMP system group, setting and viewing 5-3
NAM system time, setting 5-6
network parameters, setting and viewing 5-2
system resources, viewing 5-2
overview of user administration tasks 5-13
passwords, recovering 5-14
predefined NAM user accounts, changing 5-14
TACACS+ authentication and authorization, establishing 5-16
TACACS+ server, configuring to support NAM 5-17
user privileges (table) 5-13
users, creating new 5-14
users, deleting 5-15
users, editing 5-15
user sessions table, viewing 5-21
system resources, viewing 5-2
system alerts
capturing 5-12
viewing 5-11

T

TAC (Technical Assistance Center)
(see also troubleshooting) A-1
TACACS+
authentication and authorization, establishing 5-16
server, configuring to support NAM 5-17
secret key, requirements for in v4.2 5-17
secret key, requirements for in v5.x 5-19
version 4.2 5-17
version 5.x 5-18
technical assistance, obtaining
(see also troubleshooting) A-1
diagnostics, generating for 5-11
diagnostics, generating for technical assistance 5-11
classification information, monitoring and capturing 5-12
system alerts, capturing 5-12
system alerts, viewing 5-11
testing NetFlow devices 2-33
traffic analysis 1-9
traffic sources
  monitoring 1-9
troubleshooting A-1
  switch, cannot communicate with 5-5

U
user
  administration (see system administration) 5-1
  privileges (table) 5-13
  sessions table, viewing 5-21

V
VACL 1-10, 2-22
  VLAN access control list 1-10, 2-22
VACL, configuring
  on LAN VLANs 2-22
  on WAN interfaces 2-22
viewing
  community switch strings 5-5
  DiffServ data 3-12
  NAM SNMP system groups 5-3
  network parameters 5-2
  response time data
    server 3-25
    system alerts 5-11
    system resources 5-2
    user sessions table 5-21
    voice data 3-14
  Viewing audit trail 5-12
WAAS
  about 2-33
  adding data sources 2-38
  ART calculations 2-34
  configuring a device 2-37
  WAAS Central Manager 2-36
  WAAS data sources 3-18

Voice signaling thresholds 2-54
VSS
  see Virtual Switch Software 2-7

W
WAAS
  about 2-33
  adding data sources 2-38
  ART calculations 2-34
  configuring a device 2-37
  WAAS Central Manager 2-36
  WAAS data sources 3-18

Virtual Switch Software (VSS) 2-65
VLAN access control list
  VACL 1-10, 2-22
voice data
  collecting 2-84
  viewing 3-14