



User Guide for the Cisco Network Analysis Module Traffic Analyzer, 4.1

August 2009

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-19530-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for the Cisco Network Analysis Module Traffic Analyzer, 4.1

© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

About This Guide	xv
Chapter Overview	xvi
Audience	xvi
Conventions	xvii
Notices	xvii
OpenSSL/Open SSL Project	xvii
License Issues	xvii
Obtaining Documentation and Submitting a Service Request	xix
	iii-xix

CHAPTER 1

Overview of the NAM Traffic Analyzer	1-1
Introducing the NAM Traffic Analyzer	1-1
Using the NAM Graphical User Interface	1-1
A Closer Look at Some User Interface Components	1-3
Common Navigation and Control Elements	1-4
Getting Started	1-6
Understanding How the NAM Works	1-9
Understanding How the NAM Uses SPAN	1-10
Understanding How the NAM Uses VACLs	1-11
Understanding How the NAM Uses NDE	1-12

CHAPTER 2

User and System Administration	2-1
User Administration	2-2
Recovering Passwords	2-2
Changing Predefined NAM User Accounts on the Switch or Router	2-3
User Administration GUI	2-3
Creating a New User	2-4
Editing a User	2-5
Deleting a User	2-6
Establishing TACACS+ Authentication and Authorization	2-6
Configuring a TACACS+ Server to Support NAM Authentication and Authorization	2-7
Configuring a Cisco ACS TACACS+ Server	2-8
Viewing the Current User Sessions Table	2-9
System Administration	2-10

System Resources	2-11
Setting and Viewing Network Parameters	2-12
Setting and Viewing the NAM SNMP System Group	2-13
Working with NAM Community Strings	2-14
Creating NAM Community Strings	2-14
Deleting NAM Community Strings	2-15
NAM System Time	2-16
Synchronizing the NAM System Time with the Switch or Router	2-17
Synchronizing the NAM System Time Locally	2-17
Configuring the NAM System Time with an NTP Server	2-17
E-Mail Configuration	2-18
FTP Configuration	2-19
Capture Data Storage	2-19
Creating NFS Storage Locations	2-20
Editing NFS Storage Locations	2-22
Creating iSCSI Storage Locations	2-22
Editing iSCSI Storage Locations	2-23
Web Publication	2-24
Response Time Export	2-25
Diagnostics	2-25
Viewing System Alerts	2-25
Viewing the Audit Trail	2-26
Monitor and Capture Configuration Information	2-27
Viewing Technical Support	2-28

CHAPTER 3

Setting Up the Application 3-1

Chassis Parameters	3-2
Viewing the Switch Information	3-2
Setting Up NBAR Protocol Discovery	3-3
Enabling and Disabling Port Stats (Mini-RMON)	3-5
Configuring Switch Login	3-8
Router Parameters	3-8
Applying Router System Information	3-8
Managed Device Parameters	3-9
Data Sources	3-10
SPAN Sessions	3-12
Creating a SPAN Session	3-14
Editing a SPAN Session	3-15
Deleting a SPAN Session	3-16

Deduplication	3-17
VLAN Data Sources	3-19
Deleting a VLAN Data Source	3-20
Understanding NetFlow Interfaces	3-21
Understanding NetFlow Flow Records	3-21
Configuring NetFlow on Devices	3-22
Configuring VACL on a WAN Interface	3-24
Configuring VACL on a LAN VLAN	3-25
Managing NetFlow Devices	3-26
Adding NetFlow Devices	3-26
Editing NetFlow Devices	3-27
Deleting NetFlow Devices	3-27
Testing NetFlow Devices	3-27
Creating Custom Data Sources	3-28
Selecting a NetFlow Device	3-29
Selecting the Interfaces	3-29
Using the Listening Mode	3-30
Testing the Router Community Strings	3-33
Setting Up an Interface	3-33
Understanding Wide Area Application Services	3-34
ART Monitoring from WAAS Data Sources	3-35
Managing WAAS Devices	3-36
Adding a WAAS Device	3-37
Configuring WAAS Data Sources	3-38
Deleting a WAAS Data Source	3-40
Auto-Config New WAAS Devices	3-41
Managing a WAAS Monitored Server	3-42
Adding a WAAS Monitored Server	3-42
Deleting a WAAS Monitored Server	3-43
Setting Up a WAAS Analysis Report	3-44
MPLS Data Sources	3-47
Automatic Discovery of MPLS VPN Labels	3-47
Setting Up Layer 3 VRF Data Sources	3-48
Setting Up Layer 2 Virtual Circuit Data Sources	3-49
Setting Up MPLS Label Data Sources	3-50
Creating a VRF/VC Configuration File	3-51
Importing a VRF/VC Configuration File	3-51
Exporting a VRF/VC Configuration File	3-52
Importing Log	3-52
ERSPAN	3-52

Sending ERSPAN Data to Layer 3 Interface	3-52
Sending ERSPAN Data Directly to the NAM Management Interface	3-53
Monitoring	3-54
Monitoring Core Data	3-54
Enabling Mini-RMON Collection	3-56
Monitoring Voice Data	3-57
Monitoring RTP Stream Traffic	3-58
Monitoring Response Time Data	3-60
Setting Up Response Time Configuration	3-61
Setting Up Response Time Data Monitoring	3-62
Creating a Response Time Monitoring Collection	3-63
Editing a Response Time Monitoring Collection	3-63
Deleting Response Time Data Collections	3-64
Monitoring DiffServ Data	3-64
Setting Up the DiffServ Profile	3-65
Creating a DiffServ Profile	3-65
Editing a DiffServ Profile	3-66
Deleting a DiffServ Profile	3-66
Monitoring URL Collection Data	3-67
Enabling a URL Collection	3-67
Changing a URL Collection	3-68
Disabling a URL Collection	3-69
Protocol Directory	3-69
Individual Applications	3-70
Creating a New Protocol	3-70
Editing a Protocol	3-72
Deleting a Protocol	3-73
Setting Up Encapsulation	3-74
Setting Up Application Groups	3-75
Creating an Application Group	3-75
Editing an Application Group	3-75
Deleting an Application Group	3-76
Setting Up Autolearned Protocols	3-76
Setting Up URL-Based Applications	3-77
Creating a URL-Based Application	3-78
Editing a URL-Based Application	3-80
Deleting a URL-based Application	3-81
Setting Up Alarm Events and Thresholds	3-81
Setting Up Alarm Events	3-82

Setting Alarm Thresholds	3-84
Alarm Thresholds - Selecting a Variable	3-84
Alarm Thresholds - Selecting Parameters	3-85
Editing an Alarm Threshold	3-87
Deleting a NAM MIB Threshold	3-87
Setting Up Voice/Video Stream Thresholds	3-88
Setting Up the NAM Syslog	3-90
Setting Chassis or Managed Device Thresholds	3-90
Creating Chassis or Managed Device Thresholds	3-91
Editing Chassis or Managed Device Thresholds	3-92
Deleting Chassis or Managed Device Thresholds	3-93
Setting NAM Trap Destinations	3-93
Creating a NAM Trap Destination	3-93
Editing a NAM Trap Destination	3-94
Deleting a NAM Trap Destination	3-94
Setting NAM Alarm Mail	3-94
Setting Global Preferences	3-94

CHAPTER 4

Monitoring Data 4-1

Overview of Data Collection and Data Sources	4-2
Configuring Multiple Collections	4-2
Protocol Auto Discovery	4-4
NDE Flow Masks and V8 Aggregation Caches	4-5
Viewing the Monitor Overview Charts	4-6
Data Source Persistence	4-9
Viewing Individual Applications Data	4-9
Viewing the Applications	4-9
Displaying Details from the Applications Table	4-10
Capturing Application Protocol Data from the Application Table	4-11
Viewing Real-Time Data from the Application Table	4-11
Viewing Reports from the Applications Table	4-11
Viewing the Top N Applications Chart	4-11
Viewing the Applications Cumulative Data Table	4-13
Displaying Details from the Applications Table	4-14
Viewing Application Groups	4-14
Viewing the Application Groups Current Rates Table	4-14
Displaying Details from the Application Group Table	4-15
Viewing Real-Time Data from the Application Group Table	4-16
Viewing Reports from the Application Group Table	4-16

Viewing the Top N Application Group Chart	4-16
Viewing the Application Groups Cumulative Data Table	4-17
Viewing Collected URLs	4-18
Viewing Collected URLs	4-18
Filtering a URL Collection List	4-19
Creating a URL-based Application from a Collected URL	4-20
Viewing the TCP/UDP Port Table	4-21
Viewing the TCP/UDP Port Table Current Rates	4-21
Viewing the TCP/UDP Port Table TopN Chart	4-21
Viewing the TCP/UDP Port Table Cumulative Data	4-22
Viewing Voice and Video Data	4-23
Active Calls	4-23
MOS Quality Chart	4-23
Alarm Threshold Chart	4-24
Active Calls Table	4-26
Terminated Calls	4-28
Overview	4-28
Worst N Calls	4-29
Viewing Known Phones	4-30
Viewing RTP Stream Traffic	4-32
Monitoring Hosts	4-34
Viewing the Network Hosts Current Rates Table	4-34
Viewing Network Host Details	4-35
Capturing Network Host Data from the Network Host Table	4-36
Viewing Real-Time Traffic Statistics from the Hosts Table	4-36
Viewing Reports from the Network Hosts Table	4-37
Viewing the Network Hosts Top N Chart	4-37
Viewing the Network Hosts Cumulative Data Table	4-38
Viewing the MAC Stations Current Rates Table	4-39
Viewing the MAC Stations Top N Chart	4-40
Viewing the MAC Stations Cumulative Data Table	4-41
Viewing Conversations Data	4-42
Viewing Network Hosts	4-43
Viewing the Network Host Conversations Current Rates Table	4-43
Viewing the Network Host Conversations Top N Chart	4-45
Viewing the Network Host Conversations Cumulative Data Table	4-46
Viewing the Application Hosts	4-47
Viewing MAC Stations	4-48
Viewing the MAC Station Conversations Current Rates Table	4-49

Viewing the MAC Conversations Top N Chart	4-49
Viewing the MAC Station Conversations Cumulative Data Table	4-51
Viewing VLAN Data	4-51
Viewing the VLAN Traffic Statistics Current Rates Table	4-52
Viewing Reports from the VLAN Traffic Statistics Table	4-53
Viewing the VLAN Traffic Statistics Top N Chart	4-53
Viewing VLAN Traffic Statistics Cumulative Data Table	4-54
Viewing the VLAN Priority (COS) Statistics Current Rates Table	4-55
Viewing the VLAN Priority (COS) Statistics Top N Chart	4-56
Viewing the VLAN Priority (COS) Statistics Cumulative Data Table	4-57
Viewing DiffServ Data	4-57
Viewing the DiffServ Traffic Statistics Current Rates Table	4-58
Viewing Real-Time Traffic Statistics from the DiffServ Traffic Statistics Table	4-59
Viewing Reports from the DiffServ Traffic Statistics Table	4-59
Viewing the DiffServ Traffic Top N Chart	4-59
Viewing the DiffServ Traffic Statistics Cumulative Data Table	4-60
Viewing the DiffServ Application Statistics Current Rates Table	4-61
Displaying Application Conversation Details From Application Statistics Table	4-62
Viewing Real-Time Traffic Statistics from the DiffServ Application Statistics Table	4-62
Viewing Reports from the DiffServ Application Statistics Table	4-63
Viewing the DiffServ Application Statistics Top N Chart	4-63
Viewing the DiffServ Application Statistics Cumulative Data Table	4-64
Viewing the DiffServ Host Statistics Current Rates Table	4-65
Displaying Host Conversation Details From the DiffServ Host Statistics Table	4-66
Viewing Real-Time Data from the DiffServ Host Statistics Table	4-66
Viewing Reports from the DiffServ Host Statistics Table	4-67
Viewing the DiffServ Host Statistics Top N Chart	4-67
Viewing the DiffServ Host Statistics Cumulative Data Table	4-68
Monitoring Response Time Data	4-69
Server Application Responses	4-72
Viewing Server Application Responses	4-72
Viewing Server Application Transactions	4-77
Server Network Response Time	4-80
Server-Client Application Response Times	4-84
Viewing Server-Client Application Response Time	4-84
Viewing the Server-Client Transactions	4-88
Viewing the Server-Client Network Response Time	4-89
Viewing Response Time across Multiple WAAS Segments	4-92
Viewing Port/Interface Statistics Data	4-93

Viewing the Port Stats Current Rates Table	4-93
Viewing the Interface Stats Current Rates Table	4-95
Viewing Port/Interface Details	4-96
Viewing Real-Time Traffic Data from the Port/Interface Stats Table	4-96
Viewing Reports from the Port/Interface Stats Table	4-97
Viewing the Top N Port Stats Chart	4-97
Viewing the Top N Interface Stats Chart	4-99
Viewing the Port Stats Cumulative Data Table	4-100
Viewing the Interface Stats Cumulative Data Table	4-101
Viewing Interface Details	4-102
Viewing System Health	4-103
Switch Health	4-103
Switch Health	4-103
Switch Information	4-104
Crossbar Switching Fabric	4-106
Ternary Content Addressable Memory Information	4-107
Router Health	4-108
Router Health	4-108
Router Information	4-110
Viewing NBAR	4-111
Viewing the NBAR Current Rates Table	4-111
Viewing the Top N NBAR Chart	4-112
Viewing the NBAR Cumulative Data Table	4-113
Viewing MPLS Traffic Statistics	4-115
Viewing VRF Statistics	4-115
Viewing Virtual Circuit Statistics	4-116
Viewing All Labels	4-117

CHAPTER 5

Creating and Viewing Reports 5-1

Basic Reports	5-2
Creating a Basic Report	5-4
Creating an Applications Report	5-6
Creating an Application Groups Report	5-8
Creating a Hosts Report	5-8
Creating a Conversations Report	5-10
Creating a VLANs Report	5-11
Creating a DiffServ Report	5-12
Creating a Response Time Report	5-13
Creating a Switch Port Report	5-14

Creating a Switch Health Report	5-15
Creating a Router Interface Report	5-16
Creating a Router Health Report	5-17
Creating an MPLS Stats Report	5-18
Creating a Voice Over IP/RTP Stream Report	5-19
Viewing Basic Reports	5-20
Viewing Report Details	5-21
Viewing Report Options	5-22
Disable Reports and Errors	5-22
Viewing the System Event Log	5-23
Enabling Reports	5-24
Disabling Reports	5-25
Renaming a Report	5-25
Deleting a Report	5-25
Custom Reports	5-25
Creating a Custom Report	5-26
Creating a New Folder	5-26
Editing a Custom Report	5-27
Deleting a Custom Report	5-27
Viewing a Custom Report	5-27
Moving a Custom Report to a Different Folder	5-27
Scheduled Exports	5-28
Scheduling a Report Export	5-28
Editing a Report Export	5-30

CHAPTER 6

Capturing and Decoding Packet Data 6-1

Buffers	6-2
Configuring Capture Settings	6-3
Capturing Using an Address Filter	6-8
Capturing Using a Protocol Filter	6-9
Capturing Using a Port Filter	6-10
Capturing Using a Custom Filter	6-10
Using Alarm-Triggered Captures	6-10
Viewing Packet Decode Information	6-11
Browsing Packets in the Packet Decoder	6-12
Filtering Packets Displayed in the Packet Decoder	6-13
Viewing Detailed Protocol Decode Information	6-14
Hardware Assisted Capture Sessions	6-15
Configuring the Hardware Assisted Capture Session	6-16

Configuring Hardware Filters	6-18
Configuring Software Filters	6-22
Files	6-22
Analyzing Capture Files	6-23
Decoding Capture Files	6-24
Renaming or Merging Capture Files	6-25
Renaming Capture Files	6-25
Merging Capture Files	6-25
Downloading Capture Files	6-26
Deleting a Capture File	6-26
Deleting All Capture Files	6-27
Custom Capture Filters	6-27
Creating Custom Capture Filters	6-27
Tips for Creating Custom Capture Filter Expressions	6-29
Editing Custom Capture Filters	6-30
Deleting Custom Capture Filters	6-30
Custom Display Filters	6-31
Creating Custom Display Filters	6-31
Tips for Creating Custom Decode Filter Expressions	6-33
Editing Custom Display Filters	6-35
Deleting Custom Display Filters	6-35

CHAPTER 7

Viewing Alarms 7-1

Viewing NAM Threshold Alarms	7-2
Viewing Chassis Threshold Alarms	7-2

APPENDIX A

Troubleshooting A-1

General NAM Issues	A-1
CPU Usage Percentage	A-2
Username and Password Issues	A-2
Login Issues	A-3
SPAN Related Issues	A-5
Packet Capturing Issues	A-6
Alarm and Interface/Port Stats Issues	A-8
NetFlow and NBAR Monitoring Problems	A-8
Report Problems	A-12
Image Upgrade and Patch Issues	A-13
Web Browser Response Time and Display Issues	A-13

NAM Switch Date and Time Synchronization Issues	A-14
Diagnostic Error Message Issues	A-14
Hostname Resolution Issues	A-15
Data Mismatch Issues	A-16
HTTPS/Security Certificate Issues	A-16
SNMP Issues	A-17
Protocol Support Issues	A-18
Voice Monitoring Issues	A-19
WAAS Application Response Time Issues	A-20

APPENDIX B**Supported MIB Objects B-1**

Supported MIBs	B-1

INDEX



About This Guide

Revised: July 2, 2009, OL-19530-02

This guide describes how to use Cisco Network Analysis Module Traffic Analyzer 4.1 (NAM 4.1) software. This preface has the following sections:

- [Chapter Overview, page xvi](#)
- [Audience, page xvi](#)
- [Conventions, page xvii](#)
- [Notices, page xvii](#)
 - [OpenSSL/Open SSL Project, page xvii](#)
- [Obtaining Documentation and Submitting a Service Request, page xix](#)

NAM 4.1 software supports the following NAM models (SKU):

- NAM2220
- NAM2204-RJ45
- NAM2204-SFP
- WS-SVC-NAM-1
- WS-SVC-NAM-1-250S
- WS-SVC-NAM-2
- WS-SVC-NAM-2-250S
- NME-NAM-80S
- NME-NAM-120S

NAM 4.1 virtual blade software also supports the following WAAS appliances:

- WAVE-574
- WAE-674

Throughout this guide we use NAM SKUs to indicate a specific NAM model and the following general references:

- A reference to a *NAM-1 or NAM-2 device* indicates any of the following modules:
 - WS-SVC-NAM-1
 - WS-SVC-NAM-1-250S
 - WS-SVC-NAM-2

- WS-SVC-NAM-2-250S
- A reference to *an NME-NAM device* indicates any of the following modules:
 - NME-NAM
 - NME-NAM-80S
 - NME-NAM-120S

Chapter Overview

This user guide contains the following chapters and appendices:

- [Chapter 1, “Overview of the NAM Traffic Analyzer”](#) provides an overview of the NAM Traffic Analyzer, describes the GUI, and provides information about how to use various components of the NAM Traffic Analyzer.
- [Chapter 2, “User and System Administration”](#) provides information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance.
- [Chapter 3, “Setting Up the Application”](#) provides information about setting up the NAM Traffic Analyzer applications.
- [Chapter 4, “Monitoring Data”](#) provides information about options for viewing and monitoring various types data.
- [Chapter 5, “Creating and Viewing Reports”](#) provides information about the NAM Traffic Analyzer reports function which allows you to store and retrieve short and medium-term historical data about the network traffic monitored by the NAM.
- [Chapter 6, “Capturing and Decoding Packet Data”](#) provides information about how to set up multiple buffers for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets.
- [Chapter 7, “Viewing Alarms”](#) provides information about how to set up alarms to warn of predefined conditions based on a rising data threshold, a falling data threshold, or both. You can set thresholds for the NAM MIB, NAM voice-monitoring, and switch thresholds.
- [Appendix A, “Troubleshooting,”](#) provides information about how to troubleshoot some common issues you might encounter while using the NAM Traffic Analyzer.
- [Appendix B, “Supported MIB Objects,”](#) provides information about the MIB objects supported in the NAM Traffic Analyzer.

Audience

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

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

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences



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 following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



CHAPTER 1

Overview of the NAM Traffic Analyzer

These topics provide information about using the various components of the NAM Traffic Analyzer:

- [Introducing the NAM Traffic Analyzer, page 1-1](#)
 - [Using the NAM Graphical User Interface](#)
 - [A Closer Look at Some User Interface Components, page 1-3](#)
 - [Common Navigation and Control Elements, page 1-4](#)
 - [Getting Started, page 1-6](#)
- [Understanding How the NAM Works, page 1-9](#)
 - [Understanding How the NAM Uses SPAN, page 1-10](#)
 - [Understanding How the NAM Uses VACLs, page 1-11](#)
 - [Understanding How the NAM Uses NDE, page 1-12](#)

Introducing the NAM Traffic Analyzer

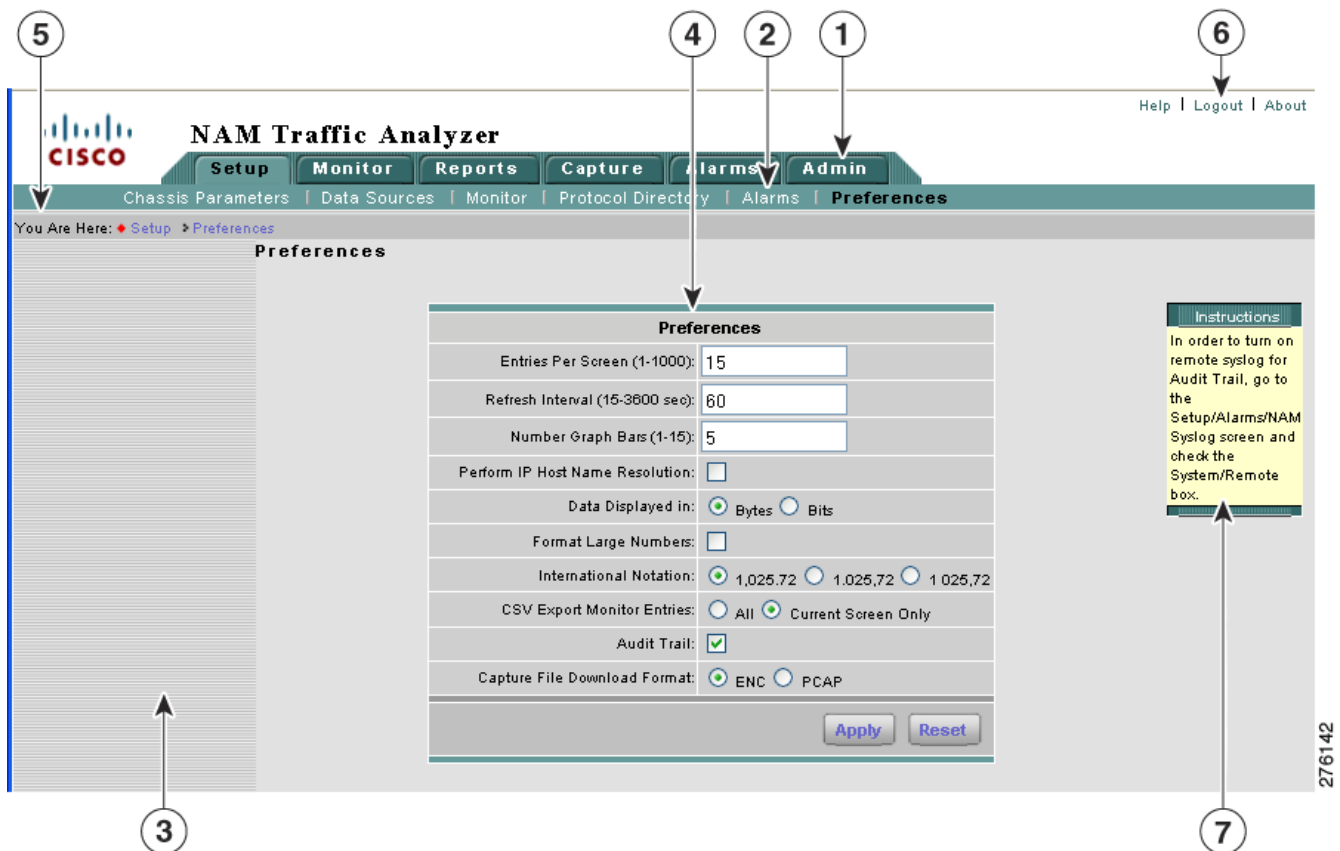
The Cisco Network Analysis Module (NAM) Traffic Analyzer software enables network managers to understand, manage, and improve how applications and services are delivered to end-users. The NAM offers flow-based traffic analysis of applications, hosts, and conversations, performance-based measurements 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. The Cisco NAM includes an embedded, web-based Traffic Analyzer GUI that provides quick access to the configuration menus and presents easy-to-read performance reports on Web, voice, and video traffic.

Using the NAM Graphical User Interface

The Cisco NAM Traffic Analyzer supports browser-based access to the NAM graphical user interface (GUI). To access the NAM GUI, enter a machine name and its domain or an IP address in your browser address field. The NAM GUI prompts you for your user name and password. After you enter your user name and password, click **Login** to access the NAM GUI.

Figure 1-1 shows an example of the NAM Traffic Analyzer GUI.

Figure 1-1 NAM Traffic Analyzer GUI



1	Tabs for accessing main functions; tabs are displayed in every window in user interface (except in the detail pop-up windows).	5	Context line that shows path to the current function. Click any link in this area to go back to the associated window.
2	Options associated with each tab; functions change in each tab depending on context.	6	Toolbar to access global functions such as online help, logging out, learning more about the application.
3	Content Menu shows links to functions from the current window. Click any link in the menu to go to the corresponding window.	7	Instruction box provides helpful information about how to use this GUI window.
4	Content area where graphs, tables, dialog boxes, charts, and instruction boxes are displayed.		

**Note**

All times in the Traffic Analyzer are typically displayed in 24-hour clock format. For example, 3:00 p.m. is displayed as 15:00.

A Closer Look at Some User Interface Components

Context Line



The Context line shows where you are in the hierarchy of operations. In this case, you would be viewing the Response Time Client/Server Table.

You can click:

- **Response Time** to return to the Response Time Server Table.
- **Monitor** to return to the Monitor Overview window.

Contents



The contents (present in only some windows) displays options that are subordinate to the options within the individual tabs. The example above displays after you click **Setup > Monitor**.

Toolbar

Help | Logout | About

The toolbar is displayed in the upper right corner of every window of the user interface.

- Click **Logout** to log out of the NAM Traffic Analyzer.
- Click **Help** for context-sensitive information (information relevant to the current function). Help is displayed in a separate browser window.
- Click **About** to see information about the NAM Traffic Analyzer.

Common Navigation and Control Elements

[Common Navigation and Control Elements](#) (Table 1-1) describes the common navigation and control elements in the user interface.

Table 1-1 Common Navigation and Control Elements

Element	Description
	Starts an action.
	Stops an action, such as the active capturing of packets.
	Temporarily suspends an action.
	Creates a new record, user, capture, filter, and so on.
	Deletes a record, user, capture, filter, and so on.
	Edits a record, user, capture, filter, and so on.
	Jumps to a group of records, beginning at a specific line number.
	Displays the previous group of records.
	Displays the next group of records
	Displays information based on different criteria (for example, IP address versus protocol).
	Applies changes; current window continues to display.
	Applies changes; goes to different window.
	Resets (clears) any changes you made in a dialog box.
	Closes the window.
	Sorts the column information in descending order.
	Tests a function (such as read and write access to the router).
	Creates a report for the selected variable.

Table 1-1 Common Navigation and Control Elements (continued)

Element	Description
	Displays real-time statistics for the selected variable.
	Captures the packets to the buffer.
	Exports the data on the screen to a .csv text file. If you want to export more data, you must increase the rows per page setting for the table. The default setting is 15 rows per page.
	Exports the data on the screen to a PDF file.
	Opens a printer friendly window of the data on the screen. You can print the window using the Print command from your web browser. If you want to print more data, you must increase the rows per page setting for the table. The default setting is 15 rows per page.
	Starts the online help.

In addition to the common navigation and control elements, you can use these navigation aids:

Pop-up help—To expand abbreviated protocol encapsulation information in some links, move your mouse over the link. The full protocol encapsulation name is displayed.

	Protocol	Packets/s
1.	nov-spx	9200
2.	sccp	1700
3.	ether2.ip.tcp.sccp	900
4.	http	100

Links—Slide your mouse over text. If the text color changes from blue to red, and the cursor changes to a pointing finger, the text is a link.

Aggregate Statistics					
Protocol	Calls Monitored	Avg Pkt Loss (%)	Avg Jitter (ms)	Worst Pkt Loss (%)	Worst Jitter (ms)
sccp	0	0	0	0	0
http	0	0	0	0	0

Instructions box—Some windows contain an instructions box in the content area that explains what you are expected to do.

Instructions
 You must save the capture buffer to a file before downloading it.

 (It might take several minutes to save and download captured packets.)

Getting Started

To use the NAM Traffic Analyzer effectively, you must perform a specific sequence of tasks:

- Step 1** Use the Setup tab (Figure 1-2) to configure and enable monitoring collections on the NAM. For more information, see [Chapter 3, “Setting Up the Application.”](#)

Figure 1-2 Setup Tab



These options are available from the Setup tab.

- Chassis Parameters—To verify there is connectivity between the NAM-1 or NAM-2 device and the switch.
- Router Parameters—To set up the parameters to be used by the NAM to communicate with the router



Note The Router Parameters options are for NM-NAM or NME-NAM devices only.

- Managed Device Parameters—To set up the parameters to be used by the NAM appliance to communicate with the managed device, a switch or router to which you connect the NAM appliance to receive and monitor traffic.



Note The Managed Device Parameters options are for Cisco 2200 Series NAM appliances only. NAM appliances are the following SKUs: NAM2220, NAM2204-RJ45, and NAM2204-SFP.

- Data Sources—To specify the network traffic to be collected from the switch or router to this NAM for monitoring. Also used to create NetFlow data sources.
- Monitor—To specify the types of traffic statistics to be collected and monitored.
- Protocol Directory—To specify protocol groups and URL-based protocols.
- Alarms—To set up alarm conditions and thresholds.
- Preferences—To establish global preferences for *all* NAM Traffic Analyzer users. These preferences determine how data displays are formatted.

- Step 2** Use the **Admin** tab (Figure 1-3) to create, edit, or delete NAM Traffic Analyzer accounts. You must have the required permissions to perform these tasks.

For more information, see [Chapter 2, “User and System Administration.”](#)

Figure 1-3 Admin Tab

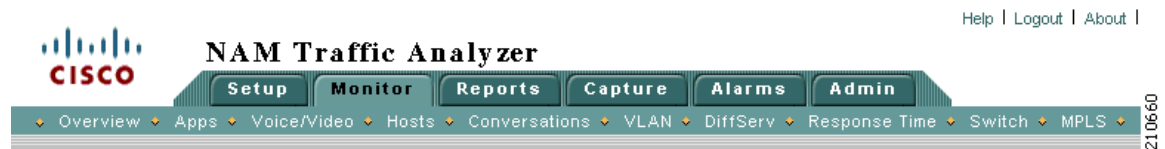
These options are available from the Admin tab.

- Users—To add, delete, and edit NAM Traffic Analyzer users and TACACS+ authentication and authorization.
- System—To establish system and network parameters and NAM community string settings.
- Diagnostics—To generate information used for troubleshooting NAM problems.

Step 3 Use the Monitor tab([Figure 1-4](#)), Reports tab([Figure 1-5](#)), Capture tab([Figure 1-6](#)), and Alarms tab([Figure 1-7](#)) in any sequence to set up real-time data displays, capture data using specific criteria, and configure notifications.

Monitor Tab

The Monitor tab provides tools for configuring specific monitoring collections on the NAM except for capture buffers and alarms. Examples include conversation collections, protocol collections, and voice collections. For more information, see [Chapter 4, “Monitoring Data.”](#)

Figure 1-4 Monitor Tab

These options are available from the Monitor tab.

- Overview—To see several types of statistics, including most active applications, most active hosts, protocol suites, and server response times.
- Apps—To see the distribution of packets and bytes based on the application protocol.
- Voice/Video—To view troubleshooting data collected from any enabled voice protocols on the NAM (including SCCP, SIP, H.323 and MGCP).
- Hosts—To view results from any active hosts collections in the RMON1 and RMON2 host tables per network host.
- Conversations—To view conversations data collected per pairs of network hosts.
- VLAN—To view VLAN data collected on the NAM based on VLAN ID or priority.



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

- DiffServ—To view the distribution of packets and bytes based on the Differentiated Services (DiffServ) data collected on the NAM.
- Response Time—To view client-server application response times.
- Switch—To view various data collected per switch port.

- Router—To view router interface statistics, health and NBAR.



Note NME-NAM devices have an Interface Stats option used to view various data collected per router interface.

- MPLS—To view traffic statistics per MPLS tag.



Note MPLS data is not available on NM-NAM or NME-NAM devices.

Reports Tab

Use the **Reports** function (Figure 1-5) to store and retrieve short- and medium-term historical data about the network traffic monitored by the NAM. For more information, see [Chapter 5, “Creating and Viewing Reports.”](#)

Figure 1-5 Reports Tab



These options are available from the Reports tab:

- Basic Reports—To set up and view reports
- Custom Reports—To set up and view multiple basic reports
- Scheduled Export—To set up a report to be generated and exported automatically

Capture Tab

The Capture tab (Figure 1-6) provides windows to set up and display capture buffer data. For more information, see [Chapter 6, “Capturing and Decoding Packet Data.”](#)

Figure 1-6 Capture Tab



These options are available from the Capture tab:

- Buffers—Set up and manage capture buffers (including capture filters); start and stop captures; view and decode captured packets.
- Files—Save packets in capture buffers to files; decode and download files.
- Custom Filters—Customized capture and display filters.

Alarms Tab

The Alarms tab ([Figure 1-7](#)) provides mechanisms for displaying alarms generated from thresholds established in the Setup tab. For more information, see [Chapter 7, “Viewing Alarms.”](#)

Figure 1-7 **Alarms Tab**



These options are available from the Alarms tab:

- NAM—To display all threshold events for NAM MIB thresholds and NAM voice-monitoring thresholds.
- Chassis—To display the RMON logTable from the switch mini-RMON MIB.



Note The Chassis option is not available on NME-NAM devices.

Understanding How the NAM Works

This section describes how the Catalyst 6500 series switch or Cisco 7600 series router Network Analysis Module (NAM) operates. This section contains these subsections:

- [Understanding How the NAM Uses SPAN, page 1-10](#)
- [Understanding How the NAM Uses VACLs, page 1-11](#)
- [Understanding How the NAM Uses NDE, page 1-12](#)

The NAM monitors and analyzes network traffic using remote monitoring (RMON), RMON extensions for switched networks (SMON), and other management information bases (MIBs). For more information, see the [“Supported MIB Objects” section on page 5-16](#).

The NAM monitors, analyzes, and views NetFlow on remote devices and supports these RMON groups:

- RMON groups defined in RFC 2819
- RMON2 groups defined in RFC 2021
- DSMON groups defined in RFC 3287
- High-capacity RMON groups defined in RFC 3273 (except the media Independent Group)
- SMON groups defined in RFC 2613
- All groups defined in the Application Response Time MIB
- NetFlow Version 9 records; the NetFlow listening mode now shows data sources using NetFlow Version 9

The NAM can also monitor individual Ethernet VLANs, which allows it to serve as an extension to the basic RMON support provided by the Catalyst 6500 series supervisor engine.

You can use any other IETF-compliant RMON application to access link, host, protocol, and response-time statistics for capacity planning, departmental accounting, and real-time application protocol monitoring. You also can use filters and capture buffers to troubleshoot the network.

The NAM can analyze Ethernet VLAN traffic from the following sources:

- Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN or RSPAN source port.

For more information about SPAN and RSPAN, refer to the “Configuring SPAN, RSPAN, and the Mini Protocol Analyzer” chapter in the *Catalyst 6500 Series Switch Software Configuration Guide*.

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/span.html>

- NetFlow Data Export (NDE).

For more information about NDE, refer to the *Catalyst 6500 Series Switch Software Configuration Guide*.

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/nde.html>

Table 1-2 summarizes the traffic sources that are used for NAM monitoring.

Table 1-2 Summary of Traffic Sources for NAM Monitoring

Traffic Source	LAN		WAN	
	Ports	VLANs	Ports	VLANs
VACL capture	Yes	Yes	Yes	N/A
NetFlow Data Export NDE (local)	Yes	Yes	Yes	Yes
NetFlow Data Export NDE (remote)	Yes	Yes	Yes	Yes
SPAN	Yes	Yes	No	No
ERSPAN	Yes	Yes	No	No

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 multiple SPAN sessions in a switched network.

The WS-SVC-NAM-1 platform provides a single destination port for SPAN sessions. The WS-SVC-NAM-2 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 1-3.

Table 1-3 SPAN Port Names

Module	Cisco IOS Software	Catalyst Operating System Software
NAM-1	data-port 1	module number:3
NAM-2	data-port 1 and data-port 2	<module number/7> or <module #/8>

Each of these ports is independent. You might create data-port collections that are populated by only the traffic from one of the ports or by traffic from both ports. You can still create VLAN-based collections with packets from either port that match the specified VLAN populating such collections.

For more information about SPAN and how to configure it on the Catalyst 6500 series switches, use this URL:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/span.html>

For more information about SPAN and how to configure it on the Cisco 7600 series router, use this URL:

<http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/span.html>

The NAM supports Encapsulated Remote SPAN (ERSPAN) traffic on the management port and uses that traffic as a data source. All collection types are supported on the ERSPAN traffic.

ERSPAN is an extension of SPAN where packets are encapsulated in a generic routing encapsulation (GRE) packet and sent to an ERSPAN destination. The ERSPAN sources and destinations are usually Supervisor Engine 720 with a PFC5 or later releases. Because the ERSPAN traffic uses IP or GRE to encapsulate the packets sent across the routers, the de encapsulated traffic can then be sent to the 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.

Once 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 in to 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.

For details on how to configure a VACL with Cisco IOS software, refer to the *Network Analysis Module for Catalyst 6500 Series and Cisco 7600 Series Command Reference*. For details on how to configure security ACLs with the Catalyst operating system, refer to the *Catalyst 6500 Series Software Configuration Guide* and the *Catalyst 6500 Series Command Reference*.

Understanding How the NAM Uses NDE

NetFlow Data Export (NDE) is a remote device that allows you to monitor port traffic on the NAM. To use an NDE data source for the NAM, you must configure the remote device to export the NDE packets to UDP port 3000 on the NAM. You may need to configure the device on a per-interface basis. A screen has been added to the web application user interface for specifying NDE devices (an NDE device is identified by its IP address). By default, the switch's local supervisor engine is always available as an NDE device.

You can define additional NDE devices by specifying the IP addresses and (optionally) the community strings. Community strings are used to upload convenient textual strings for interfaces on the remote devices that are monitored in NetFlow records.

For more information about the NDE data sources of the NAM, go to the NAM Traffic Analyzer online help menu and choose the **Setup > Data Sources > NetFlow Devices**.

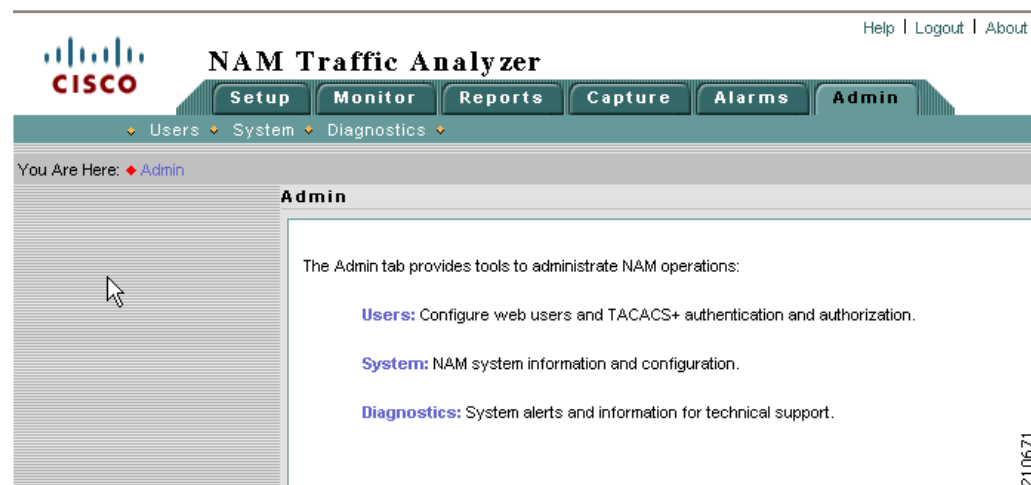


CHAPTER 2

User and System Administration

This chapter provides information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance. The top-level Admin window displays after you click the **Admin** tab on the NAM GUI. [Figure 2-1](#) shows the top-level Admin window.

Figure 2-1 Top-Level Admin Window



This chapter has the following major sections:

- [User Administration, page 2-2](#), describes how you configure either a local database or provide information for a TACACS+ database for user authentication and authorization. This section also describes the current user session window.
- [System Administration, page 2-10](#), describes menu options that enable you to perform system administrative tasks and manage the NAM.
- [Diagnostics, page 2-25](#), describes menu options that help you diagnose and troubleshoot problems.

User Administration

When you first install the NAM Traffic Analyzer, 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. You do this by assigning privileges that correspond to tasks each user can perform, such as configuring RMON collections, configuring system parameters, viewing RMON data, and so on.

Table 2-1 provides information about [User Privileges](#) and describes each privilege.

Table 2-1 **User Privileges**

Privilege	Access Level
Account Mgmt	Enables a user to create, delete, and edit user accounts.
System Config	Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.
Capture	Enables a user to perform packet captures and manage capture buffers Use the NAM Traffic Analyzer protocol decode.
Alarm Config	Enables a user to create, delete, and edit alarms on the switch/router and NAM.
Collection Config	Enables a user to create, delete, and edit the following: • Collections and reports • Protocol directory entries • Protocol groups • URL-based applications
Collection View	Enables a user to view monitoring data and reports (granted to all users).

For additional information about creating and editing users, see [Creating a New User, page 2-4](#) and [Editing a User, page 2-5](#).

Recovering 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 on 6500 Series NAMs, see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note*:

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/switch/configuration/guide/swconfig.html

For information on resetting the NAM passwords on NM-NAM devices, see the *Network Analysis Module (NM-NAM) feature module*.

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xd/feature/guide/nm_nam.html#wp1060820

For information on resetting the NAM passwords on NME-NAM devices, see the *Network Analysis Module (NME-NAM) Installation and Configuration Note*.

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/branch_router/configuration/guide/BR_incfig.html#wp1314123

For information on resetting the NAM passwords on a Cisco NAM 2200 Series Appliance, see the *Installation and Configuration Guide for the NAM 2204 Appliance* or the *Installation and Configuration Guide for the NAM 2220 Appliance*

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_appliance/2204/installation/guide/instcfg.html

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_appliance/2220/installation/guide/instcfg.html

If you have forgotten NAM Traffic Analyzer administrator password, you can recover it using one of these methods:

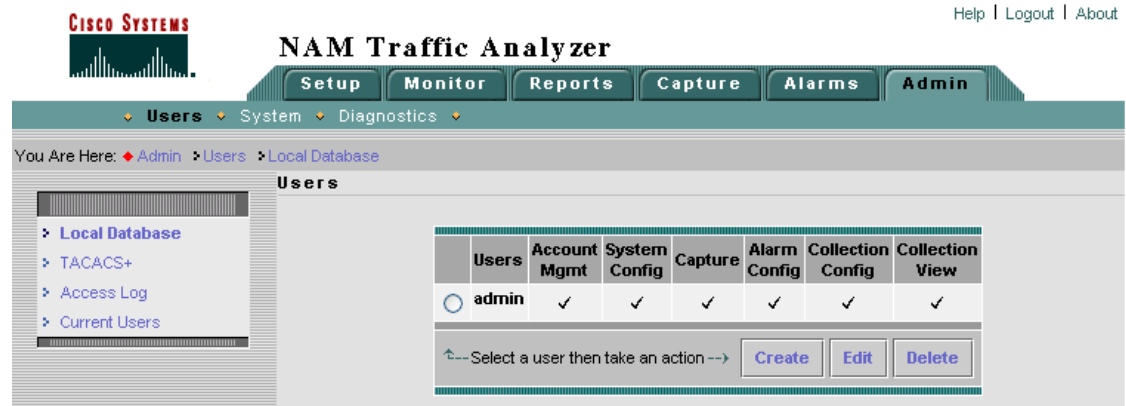
- If other users have account management permission, delete the user for whom you have forgotten the password; then create a new one by logging in as that other user by clicking the Admin tab, then clicking **Users**.
- If no other local users are configured other than the user for whom you have forgotten the password, use the NAM **rmwebusers** CLI command; then enable http or https to prompt for the creation of a NAM Traffic Analyzer 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 Traffic Analyzer. You cannot change these static accounts nor can you add other CLI-based users with the NAM Traffic Analyzer.

User Administration GUI

The User Administration GUI enables you to manage users. [Figure 2-2](#) shows the top-level User Admin GUI window.

Figure 2-2 User Admin GUI

158220

Creating a New User

To create a new user:

- Step 1** Choose **Admin > Users**.

The GUI displays the users in the local database, as shown in [Figure 2-3](#). Checks indicate the privileges each user has for the functions listed.

Figure 2-3 Users Table

	Users	Account Mgmt	System Config	Capture	Alarm Config	Collection Config	Collection View
	Guest	✓	✓	✓	✓	✓	✓
	admin	✓	✓	✓	✓	✓	✓
Select a user then take an action --> <button>Create</button> <button>Edit</button> <button>Delete</button>							

68047

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

The GUI displays the [New User Dialog Box](#) ([Figure 2-4](#)).

Figure 2-4 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 2-1](#) for an explanation of user privileges. [Table 2-2](#) describes the fields in the [New User Dialog Box](#).

Table 2-2 New User Dialog Box

Field	Description	Usage Notes
Name	The account name	Enter the user's account name.
Password Verify Password	The account password	Enter a password that adheres to your site security policies.
Privileges	Privileges associated with this account	Select each privilege to grant to the user.

Usernames and passwords cannot exceed 32 characters, can be alphanumeric, and can contain special characters except the following:

- Greater than (>)
- Less than (<)
- Comma (,)
- Period (.)
- Double quote (")
- Single quote (')

- Step 4** Click **Submit** to create the user or **Reset** to clear the dialog of any characters you entered.

Editing a User

To edit a user's configuration:

- Step 1** Choose **Admin > Users**.

The Users table displays.

Step 2 Select the username.

Step 3 Click **Edit**.

Step 4 In the Modify Users dialog box, change whatever information is necessary. See the [New User Dialog Box \(Figure 2-4\)](#) for a description of each field.

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

Deleting a User

To delete a user:

Step 1 Choose the **Admin > Users**.

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 Traffic Analyzer, TACACS+ determines if the username and password are valid and what the access privileges are.

To establish TACACS+ authentication and authorization:

Step 1 Choose **Admin > Users**.

Step 2 In the content menu, click **TACACS+**.

The TACACS+ Authentication and Authorization Dialog Box ([Figure 2-5](#)) displays.

Figure 2-5 TACACS+ Authentication and Authorization Dialog Box

Step 3 Enter or select the appropriate information in the [TACACS+ Authentication and Authorization Dialog Box](#) (Table 2-3).

Table 2-3 TACACS+ Authentication and Authorization Dialog Box

Field	Usage Notes
Enable TACACS+ Authentication and Authorization	Determines whether TACACS+ authentication and authorization is enabled. - To enable, select the check box. - To disable, clear the check box.
Primary TACACS+ Server	Enter the IP address of the primary server.
Backup TACACS+ Server	Enter the IP address of the backup server (optional). Note If the primary server does not respond after 30 seconds, the backup server will be contacted.
Secret Key	Enter the TACACS+ password.
Verify Secret Key	Reenter the TACACS+ password.

Step 4 Do one of the following:

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

**Tip**

If you cannot log into the NAM Traffic Analyzer with TACACS+ configured, verify that you entered the correct TACACS+ server name and secret key. [For more information, see the “Username and Password Issues” section on page A-2.](#)

Configuring a TACACS+ Server to Support NAM Authentication and Authorization

In addition to enabling the TACACS+ option from the Admin tab, you must configure your TACACS+ server so that it can authenticate and authorize NAM Traffic Analyzer users.

**Note**

Configuration methods vary depending on the type of TACACS+ server you use.

Configuring a Cisco ACS TACACS+ Server

For Windows NT and 2000 Systems

To configure a Cisco ACS TACACS+ server:

-
- Step 1** Log into the ACS server.
 - Step 2** Click **Network Configuration**.
 - Step 3** Click **Add Entry**.
 - Step 4** For the Network Access Server, enter the NAM hostname and IP address.
 - Step 5** Enter the secret key.

**Note**

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

-
- Step 6** In the Authenticate Using field, select **TACACS+**.
 - Step 7** Click **Submit/Restart**.
-

Adding a NAM User or User Group

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** Select **User Setup**.
 - Step 6** Enter a user password.
 - Step 7** If necessary, assign a user group.
 - Step 8** 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 9 In Unlisted Arguments, select **Deny**.

Configuring a Generic TACACS+ Server

To configure a generic TACACS+ server:

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

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



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

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

Parameter	Enter
service	shell
cmd	web
cmd-arg	One or more the following: <pre> accountmgmt system capture alarm collection view </pre>
password authentication method—Password Authentication Protocol (PAP)	pap

Viewing the Current User Sessions Table

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 **Admin > Users**.

Step 2 In the contents, click **Current Users**.

The [Current User Sessions Table](#) (Table 2-4) displays.

Table 2-4 **Current User Sessions Table**

Field	Description
User ID	The user ID used to log in to the NAM.
From	The name of the machine the user logged in from.
Login Time	The time the user logged in.
Last Activity	The time stamp of the last user activity.

System Administration

The System option of the Admin tab provides access to the following functions:

- [System Resources, page 2-11](#)
- [Setting and Viewing Network Parameters, page 2-12](#)
- [Setting and Viewing the NAM SNMP System Group, page 2-13](#)
- [NAM System Time, page 2-16](#)
- [E-Mail Configuration, page 2-18](#)
- [FTP Configuration, page 2-19](#)
- [Capture Data Storage, page 2-19](#)
- [Web Publication, page 2-24](#)
- [Response Time Export, page 2-25](#)

System Resources

Choose **Admin > System** to view the System Overview window as shown in [Figure 2-6](#).

Figure 2-6 System Overview Window

System Overview			
Date:	Thu 18 Jun 2009, 12:36:19 PDT		
Hostname:	appliance-92.cisco.com		
IP Address:	172.20.122.92		
System Uptime:	3 days, 2 hours, 31 minutes		
CPU Utilization:	Average	16.2%	
	CPU0	0.0%	
	CPU1	1.0%	
	CPU2	5.5%	
	CPU3	23.5%	
	CPU4	31.0%	
	CPU5	33.0%	
	CPU6	34.5%	
	CPU7	1.0%	
Memory Utilization:	20%		
Memory Total:	16035 MB		
Disk Usage :	Partitions	Total	Free
	Root	19.69 G	18.27 G
	Config	1,011.42 M	922.00 M
	Data	543.84 G	516.61 G

[Table 2-5](#) describes the fields of the System Overview window for a NAM with multiple CPUs such as the Cisco NAM 2220 appliance.

Table 2-5 System Overview

Field	Description
Date	Current date and time synchronized with the switch, router, or NTP server.
Hostname	NAM hostname.
IP Address	NAM IP address.
System Uptime	Length of time the host has been running uninterrupted.
CPU Utilization	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.
Memory Utilization	Percentage of memory resources being consumed by the NAM.
Disk Usage	Shows root , config , and data partitions with their total and free space.

Setting and Viewing Network Parameters

To view and set network parameters:

- Step 1

Choose **Admin > System**.
- Step 2

In the contents, click **Network Parameters**.
The [Network Parameters Dialog Box](#) (Figure 2-7) displays.

Figure 2-7 Network Parameters Dialog Box

Network Parameters	
IP Address:	172.20.98.161
IP Broadcast:	172.20.98.191
Subnet Mask:	255.255.255.192
IP Gateway:	172.20.98.129
Host Name:	namlab-pik8
Domain Name:	cisco.com
Nameservers:	171.69.2.133
	171.69.2.134
Apply Reset	

- Step 3

Enter or change the information in the [Network Parameters Dialog Box](#) (Table 2-6):



Note NAM 4.1 does not support using IPv6 for the network parameter IP address.

Table 2-6 Network Parameters Dialog Box

Field	Description
IP Address	NAM IP address.
IP Broadcast	NAM broadcast address.
Subnet Mask	NAM subnet mask.
IP Gateway	NAM IP gateway address.
Host Name	NAM host name.
Domain name	NAM domain name.
Nameservers	NAM nameserver address or addresses.

- Step 4** Do one of the following:
- To save the changes, click **Apply**.
 - To cancel the changes, click **Reset**.

Setting and Viewing the NAM SNMP System Group

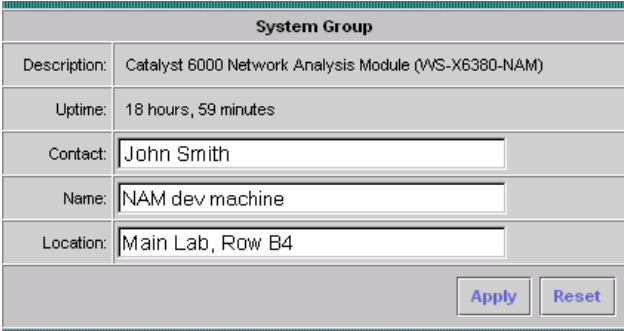
To view and set the NAM SNMP system group:

- Step 1** Choose **Admin > System**.

- Step 2** In the contents, click **NAM SNMP**.

At the top of the window, the [SNMP System Group Dialog Box](#) (Figure 2-8) and [NAM Community Strings Dialog Box](#) (Figure 2-9) are displays.

Figure 2-8 *SNMP System Group Dialog Box*



The screenshot shows the 'System Group' dialog box. It has a title bar 'System Group'. Below the title bar, there are five rows of information, each with a label on the left and a text field on the right. The first row is 'Description: Catalyst 6000 Network Analysis Module (VWS-X6380-NAM)'. The second row is 'Uptime: 18 hours, 59 minutes'. The third row is 'Contact: John Smith'. The fourth row is 'Name: NAM dev machine'. The fifth row is 'Location: Main Lab, Row B4'. At the bottom right of the dialog box, there are two buttons: 'Apply' and 'Reset'. A small number '68048' is visible at the bottom right corner of the dialog box.

System Group	
Description:	Catalyst 6000 Network Analysis Module (VWS-X6380-NAM)
Uptime:	18 hours, 59 minutes
Contact:	John Smith
Name:	NAM dev machine
Location:	Main Lab, Row B4
Apply Reset	

- Step 3** Enter or change the information in the [System SNMP Dialog Box](#) (Table 2-7).

Table 2-7 *System SNMP Dialog Box*

Field	Description
Contact	The name of the person responsible for the NAM.
Name	The name of the NAM.
Location	The physical location of the switch or router in which the NAM is installed.

- Step 4** Do one of the following:
- To save the changes, click **Apply**.
 - To cancel the changes, click **Reset**.

Working with NAM Community Strings

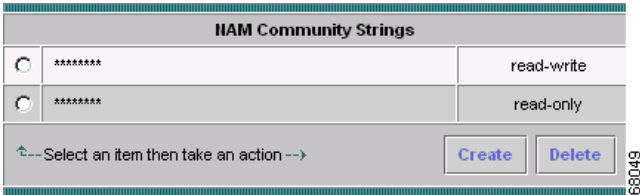
You use community strings so that other applications can send SNMP get and set requests to the NAM, set up collections, poll data, and so on.

Creating NAM Community Strings

To create the NAM community strings:

- Step 1** Choose **Admin > System**.
- Step 2** In the contents, click **NAM SNMP**.
At the bottom of the window, the **NAM Community Strings Dialog Box** displays (Figure 2-9).

Figure 2-9 NAM Community Strings Dialog Box



- Step 3** Select an entry, then click **Create**.
The **Create Community String Dialog Box** (Figure 2-10) displays.

Figure 2-10 Create Community String Dialog Box



- Step 4** Enter the community string (use a meaningful name).
- Step 5** Enter the community string again in the Verify Community field.
- Step 6** 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 7** Do one of the following:
 - To make the changes, click **Submit**.
 - To cancel, click **Reset**.

Deleting NAM Community Strings

To delete the NAM community strings:

Step 1 Choose **Admin > System**.

Step 2 In the contents, click **NAM SNMP**.

At the bottom of the window, the NAM Community Strings Dialog Box ([Figure 2-9](#)) displays.

Step 3 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.

NAM System Time

The NAM gets the UTC (GMT) time from one of two sources, depending on its the NAM type. All NAMs can be set up to get their time from an external NTP server. Following is the second option per NAM type:

- NAM-1 and NAM-2 can get their time from the switch.
- NME-NAMs can get their time from the router.
- Cisco 2200 Series appliances can get their time from a local CLI **clock set** command.

After the NAM acquires the time, you can set the local time zone using the NAM System Time configuration screen. [Figure 2-11](#) shows the [NAM System Time Configuration Screen for NAM-1, NAM-2, and NME-NAMs](#). 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 2-17](#)
This option is valid only for NAM-1, NAM-2, and NME-NAMs.
- [Synchronizing the NAM System Time Locally, page 2-17](#)
This option is valid only for Cisco NAM 2200 Series appliances.
- [Configuring the NAM System Time with an NTP Server, page 2-17](#)

Figure 2-11 NAM System Time Configuration Screen for NAM-1, NAM-2, and NME-NAMs

NAM System Time Configuration	
Current NAM System Time:	Thu 03 Mar 2005, 21:04:29 UTC
Synchronize NAM System Time With:	☒ Router ☐ NTP Server
NTP Server Name/IP Address:	
NAM local time zone:	Region: UTC Zone: None
Apply Reset	

[Figure 2-12](#) shows the [Cisco NAM 2200 Series Appliance System Time Configuration Screen](#).

Figure 2-12 Cisco NAM 2200 Series Appliance System Time Configuration Screen

NAM System Time Configuration	
Current NAM System Time:	Mon 06 Jul 2009, 15:06:17 PDT
Synchronize NAM System Time With:	☐ Local ☒ NTP Server
NTP Server Name/IP Address:	171.68.10.150
NAM local time zone:	Region: US Zone: Pacific
Apply Reset	

Synchronizing the NAM System Time with the Switch or Router

**Note**

This section is valid only for NAM-1, NAM-2, and NME-NAMs.

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

-
- Step 1** Click the Switch or Router radio button.
- Step 2** Select the Region and local time zone from the lists.
- Step 3** Do one of the following:
- To save the changes click **Apply**.
 - To leave the configuration unchanged, click **Reset**.
-

Synchronizing the NAM System Time Locally

**Note**

This section is valid only for Cisco NAM 2200 Series appliances.

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

-
- Step 1** Log in to 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, click **Admin > System**.
- Step 4** Click NAM System Time in the contents menu.
- Step 5** Click the **Local** radio button.
- Step 6** Select the Region and local time zone from the lists.
- Step 7** Do one of the following:
- To save the changes click **Apply**.
 - To leave the configuration unchanged, click **Reset**.
-

Configuring the NAM System Time with an NTP Server

To configure the NAM system time with an NTP server:

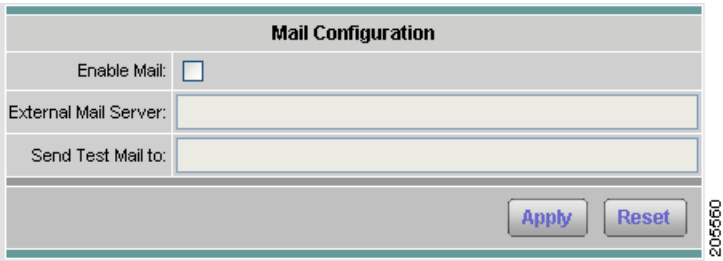
-
- Step 1** On the NAM appliance GUI, click **Admin > System**.
- Step 2** Click NAM System Time in the contents menu.
- Step 3** Click the **NTP Server** radio button.

- Step 4** Enter one or two NTP server names or IP address in the NTP server name/IP Address text boxes.
- Step 5** Select the Region and local time zone from the lists.
- Step 6** Do one of the following:
 - To save the changes click **Apply**.
 - To leave the configuration unchanged, click **Reset**.

E-Mail Configuration

You can configure the NAM to provide E-Mail notification of alarms and to E-Mail reports. [Figure 2-13](#) shows the [Mail Configuration Window](#). For information about how to configure a report to send using E-Mail, see [Table 5-18, Scheduled Exports Window Options](#), in section [Scheduled Exports](#), page 5-28.

Figure 2-13 Mail Configuration Window



The following procedure describes how to configure the NAM for E-Mail notifications.

- Step 1** Choose **Admin > System**.
- Step 2** Click **E-Mail Configuration**.

The Mail Configuration Window ([Figure 2-13](#)) displays. [Table 2-8](#) describes the [Mail Configuration Options](#).

Table 2-8 Mail Configuration Options

Field	Description
Enable Mail	Enables E-Mail of reports and notification of alarms
External Mail Server	Distinguished name of external mail server
Send Test Mail	List E-Mail addresses for up to three E-Mail recipients

- Step 3** Check **Enable EMail**.
- Step 4** Enter the distinguished name of the **External Mail Server**.
- Step 5** Click **Apply** to save your modifications, or click **Reset** to clear the dialog of any characters you entered or restore the previous settings.

FTP Configuration

You can configure the NAM to provide FTP notification of alarms and to EMail reports. [Figure 2-14](#) shows the [FTP Configuration Window](#). For information about how to configure a report to be transferred using FTP, see [Table 5-18, Scheduled Exports Window Options](#), in section [Scheduled Exports](#), [page 5-28](#).

Figure 2-14 *FTP Configuration Window*

[Table 2-9](#) describes the fields used for FTP configuration.

Table 2-9 *FTP Configuration Options*

Field	Description
External FTP Server	Host name or IP address of FTP server
FTP Directory	Full directory pathname of location to store FTP files
Authentication	User name and password fields used to for authentication with external FTP server.

Capture Data Storage

Use the Capture Data Storage option to set up remote file systems to store capture data. You must set up the capture data storage locations prior to setting up data captures. Choose **Admin > Capture Data Storage** to open the Capture Data Storage window (shown in [Figure 2-15](#)).

Figure 2-15 Capture Data Storage Window

Capture Data Storage Table					
	Type	Name	Server Address	NFS Directory / iSCSI Target Name	Free Storage (Mbytes)
☐	nfs	namlab-pc1	namlab-pc1.cisco.com	/home (soft,timeo=2,udp,nfsvers=2,retrans=2)	1584
☐	nfs	namlab-pc8	namlab-pc8.cisco.com	/home/kluu (soft,timeo=4,tcp,nfsvers=3,retrans=2)	522632

←-- Select an entry then take an action -->

Create NFS Create iSCSI Edit Delete

This section provides the following:

- [Creating NFS Storage Locations, page 2-20](#)
- [Editing NFS Storage Locations, page 2-22](#)
- [Creating iSCSI Storage Locations, page 2-22](#)
- [Editing iSCSI Storage Locations, page 2-23](#)

Creating NFS Storage Locations

The NFS server must be configured properly to allow NAM to write data to it. The NAM accesses the NFS directories with UID=80 (www) and UID=0 (root). The NFS directories must be fully accessible by these UIDs.

One way to do this is to use the NFS option *all_squash* to map these UIDs to *anonuid=<userID>*, where *<userID>* is a local user ID with full access rights to the NFS directories.

Configuring the NFS Server

The following example shows how to set up an NFS directory (**/home/SomeUserName**) in a Linux server for a NAM (at IP address 1.1.1.2) to store capture data. To setup an NFS server directory to store capture data:

Step 1 Locate a UID that has read and write access to the target NFS directory.

For example, if the target NFS directory is **/home/SomeUserName**, open the **/etc/passwd** file and search for a user entry that contains something like the following:

```
SomeUserName:x:503:503::/home/SomeUserName:/bin/tcsh
```

In this example, the UID is 503.

Step 2 Edit the **/etc/exports** file and add a line like the following:

```
/home/SomeUserName 1.1.1.2/255.255.255.255(rw,all_squash,anonuid=503)
```

Step 3 Activate the change:

```
/usr/bin/exportfs -a
```

**Note**

If the NFS directory contains subdirectories that are not writable by the NAM, these subdirectories will not be listed in NAM capture screens.

Configuring the NFS Storage Location on the NAM

The following procedure describes how to create an NFS storage location by specifying a remote file system partition.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window ([Figure 2-15](#)) displays and lists any capture data storage locations already configured.

Step 2 Click **Create NFS**.

Step 3 Enter the requested parameters in the New NFS Storage window.

[Table 2-10](#) describes the NFS Storage location parameters.

Table 2-10 NFS Storage Location Parameters

Field	Description
Name	Name of the remote file system entry
Server	DNS name of the remote file system entry
Directory	Pathname of the remote file system partition
Basic NFS Options	Each fields shows a default value. If you need to use values other than those available in the menus, use Advanced NFS Options.
Protocol	Choose TCP or UDP
Timeout	You can set the timeout to a value from 0.1 seconds to 1.0 seconds
NFS Version	Choose from NFS versions 1-4
Retries	Choose from 1-5 retries
Advanced NFS Options	This field contains the default values for creating an NFS storage location. You can edit the text to use NFS options that are outside the ranges in the pull-down menus of the Basic NFS Options.

Step 4 Click **Submit** to create the NFS storage location. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

Editing NFS Storage Locations

The following procedure describes how to edit an existing NFS storage location.

**Note**

If you have set up capture sessions that use the NFS file system entry you want to edit (or modify), you must delete those capture sessions before editing the NFS file system entry. You can find active capture buffers by clicking **Capture > Buffers**, then choose each capture that is *running* and click **Status**. If the capture is using the filesystem to be edited, click **Clear**.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window ([Figure 2-15](#)) displays and lists any capture data storage locations already configured.

Step 2 Click to select the NFS storage location you want to modify and click **Edit**.

The Edit Remote Storage Entry window displays the parameters of the select NFS storage location.

Step 3 Modify the parameters as desired.

[Table 2-10](#) describes the NFS Storage location parameters.

Step 4 Click **Submit** to change the parameters of the NFS storage location. Otherwise click **Reset** to remove all of the entries, or click **Cancel** to cancel the change.

Creating iSCSI Storage Locations

The following procedure describes how to create an iSCSI storage location for storing NAM capture data.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window ([Figure 2-15](#)) displays and lists any capture data storage locations already configured.

Step 2 Click **Create iSCSI**.**Step 3** Enter the requested parameters in the New iSCSI Storage window.

[Table 2-11](#) describes the iSCSI Storage location parameters.

Table 2-11 *iSCSI Storage Location Parameters*

Field	Description
Name	Name of the remote storage entry
Server	DNS host name or IP address of the iSCSI server.

Table 2-11 iSCSI Storage Location Parameters

Field	Description
Target Name	iSCSI target name configured on the remote iSCSI server
Format Disk:	Check Format a new partition to cause the NAM to format the iSCSI target into a single Linux partition. Check Use existing partition# when the remote iSCSI target disk has already been formatted and has a partition table.

- Step 4** Click **Submit** to create the iSCSI storage location. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

**Note**

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

Editing iSCSI Storage Locations

The following procedure describes how to edit an existing NFS storage location.

**Note**

If you have set up capture sessions that use the iSCSI file system entry you want to edit (or modify), you must delete those capture sessions before editing the iSCSI file system entry. You can find active capture buffers by clicking **Capture > Buffers**, then choose each capture the is *running* and click **Status**. If the capture is using the filesystem to be edited, click **Clear**.

- Step 1** Choose **Admin > Capture Data Storage**.
- The Capture Data Storage window ([Figure 2-15](#)) displays and lists any capture data storage locations already configured.
- Step 2** Click to select the iSCSI storage location you want to modify and click **Edit**.
- The selected iSCSI storage location parameters window displays
- Step 3** Modify the parameters as desired.
- [Table 2-11](#) describes the iSCSI storage location parameters.
- Step 4** Click **Submit** to change the iSCSI storage location parameters. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

**Note**

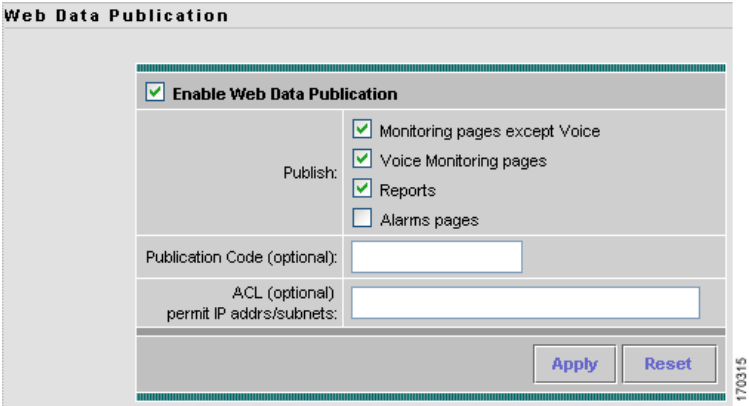
Before the changes to the iSCSI storage entry take effect, you must reboot the NAM system.

Web Publication

Web publication allows general web users and web sites to access (or link to) selected NAM monitor and report screens without a login session.

Web 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. [Figure 2-16](#) shows the [Web Data Publication Window](#).

Figure 2-16 Web Data Publication Window



To enable web publishing:

- Step 1

Choose **Admin > System**.
- Step 2

In the System menu, click **Web Publishing**.
- Step 3

Check each item you want to make available for web publishing.

[Table 2-12](#), [Web Data Publication Properties](#), describes the fields of the Enable Web Publishing window.

Table 2-12 Web Data Publication Properties

Field	Description
Monitoring pages except Voice	Check to publish all Monitor screens except Voice
Voice Monitoring pages	Check to publish Voice Monitoring screens
Reports	Check to publish all reports
Alarms pages	Check to publish NAM and Switch Alarms pages
Publication Code	Pass code required in a URL’s cookie to access the published page. For example, a publication code set to <i>abc123</i> could access the published Monitor > PortStat window: <code>http://<nam-hostname>/monitor/sup/ether/supetherstats.php?sortCol=utilization&publicationcode=abc123</code>
ACL permit IP addr/subnets	No entry provides open access to all. Enter IP addresses or subnets to permit only those IP addresses or subnets access to web publications.

- Step 4** Click **Apply** to enable web publishing or **Reset** to clear the dialog of any characters you entered.
-

Response Time Export

You can enable response time data export to an external reporting console such as NetQoS SuperAgent. This window works in conjunction with the **Setup > Data Sources > WAAS--Devices > Add/Config** window. After you enable Response Time Export there, the **Export Passthru to External Console** option appears on the Add/Config WAAS Device window.

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

-
- Step 1** From the NAM GUI, choose **Admin > System > Response Time Export**.
The Export window displays.
- Step 2** Enter the IP address of the external reporting console in the IP Address field.
- Step 3** Optionally, enter the UDP port number of the external console.
- Step 4** Click **Export** to enable the NAM to export data.
- Step 5** Optionally, click **Export Non-WAAS Traffic**.
This enables the export of SPAN and other data as well as WAAS traffic.
- Step 6** Click **Apply** to enable traffic export.
-

Diagnostics

The Diagnostics option of the **Admin** tab 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:

- [Viewing System Alerts, page 2-25](#)
- [Viewing the Audit Trail, page 2-26](#)
- [Monitor and Capture Configuration Information, page 2-27](#)
- [Viewing Technical Support, page 2-28](#)

Viewing System Alerts

You can view any failures or problems that the NAM Traffic Analyzer has detected during normal operations. To view System Alerts, choose **Admin > Diagnostics**. System Alerts is the default window. [Figure 2-17](#) shows the [System Alerts Window](#).

Figure 2-17 System Alerts Window

Tech-Support System Alerts

Current system alerts: as of Fri 09 Dec 2005, 07:51:35 PST

☒ Auto Refresh

	Date	Time	Message
1.	08 Dec	14:54:55	%NAM-5-CONFIG_CHANGE: Configuration changed
2.	08 Dec	14:51:54	%NAM-5-CONFIG_CHANGE: Configuration changed
3.	07 Dec	18:11:09	%NAM-5-CONFIG_CHANGE: Configuration changed
4.	06 Dec	15:14:54	%NAM-5-CONFIG_CHANGE: Configuration changed
5.	06 Dec	15:14:09	Completed capture KluuNfs1
6.	06 Dec	15:14:09	Close capture file KluuNfs1
7.	06 Dec	15:14:06	Open capture file KluuNfs1
8.	06 Dec	15:14:06	Close capture file KluuNfs1
9.	06 Dec	15:14:02	Open capture file KluuNfs1
10.	06 Dec	15:14:02	Close capture file KluuNfs1

158214

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.

Viewing the 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
- Creating and deleting reports
- Starting and stopping captures
- Adding and deleting users

Each log entry will contain the following:

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

To access the audit trail window:

Step 1 Choose **Admin > Diagnostics**.

Step 2 Click **Audit Trail**.

The Audit Trail Window (Figure 2-18) 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.

Figure 2-18 Audit Trail Window

Audit Trail			
Current Data: as of Thu 05 Jan 2006, 11:53:47 UTC			
		Time	Filter Clear
Time ▼	User	From	Activity
29 Dec 2005, 15:33:49	admin	10.21.122.224	User login
29 Dec 2005, 14:09:22	admin	10.82.208.159	User login
29 Dec 2005, 12:34:50	admin	10.82.208.159	User login
29 Dec 2005, 10:14:29	admin	10.82.208.159	User login
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor NBAR stats enabled
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor VLAN stats enabled
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor ether stats enabled
29 Dec 2005, 09:39:34	admin	10.24.2.108	User login
29 Dec 2005, 09:36:10	admin	10.82.208.159	User login
28 Dec 2005, 15:36:35	admin	10.21.122.224	User login
28 Dec 2005, 15:32:36	admin	10.82.208.159	User login
28 Dec 2005, 15:23:52	admin	10.82.208.159	User login
28 Dec 2005, 15:18:24	admin	10.82.208.159	User login
28 Dec 2005, 15:06:57	-	10.82.208.159	Application statistics disabled on datasource ALL SPAN
28 Dec 2005, 15:02:05	admin	10.82.208.159	User login
28 Dec 2005, 14:16:19	-	10.82.208.159	Address Mapping enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	Host Conversation statistics enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	MAC Hosts statistics enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	Network Conversation statistics enabled on datasource ALL SPAN

158212

Monitor and Capture Configuration Information

The Monitor and Capture Configuration window contains information about NAM data collections configured by NAM Traffic Analyzer and other management applications. To view the Monitoring and Capturing Configuration information window:

Step 1 Choose **Admin > Diagnostics**.

Step 2 In the contents menu, click **Monitor and Capture Configuration**.

The NAM displays the [Monitor and Capture Configuration Window](#) (Figure 2-19). Each line in the Monitor and Capture Configuration window represents an internal configuration statement for NAM collections, captures, filters, data sources, and alarms. Your configuration might have dozens of statements like these.

**Note**

This information does not mean much to the casual user, but it is valuable when you consult with Cisco TAC personnel or when you require technical support.

Figure 2-19 Monitor and Capture Configuration Window

Monitor and Capture Configuration					
Current Data: as of Tue 19 Aug 2008, 00:52:23 UTC					
	Collection	Index	Data Source	Owner	Settings
1.	prdist	1	"Internal"	LocalMgr	
2.	hlhost	1	"Internal"	LocalMgr	nl-max 100 al-max -1
3.	addrmap	1	"Internal"	LocalMgr	
4.	prdist	8816	"External"	LocalMgr	
5.	hlhost	39071	"External"	LocalMgr	nl-max 100 al-max -1

Step 3 To save the information, choose **File > Save As...** from your browser menu.

Step 4 Select an output destination, filename, and format, then click **Save**.

If the name LocalMgr is displayed in the Owner column, the collection was configured by the NAM Traffic Analyzer.

Viewing Technical Support

The NAM syslog records NAM system alerts that contain event descriptions and date and timestamps, indicating unexpected or potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs.

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 **Admin > Users** page. For more information on editing user privileges, see the [“Editing a User” section on page 2-5](#).

**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*, for NM-NAM or NME-NAM devices, the *Network Analysis Module (NM-NAM or NME-NAM) feature module*.

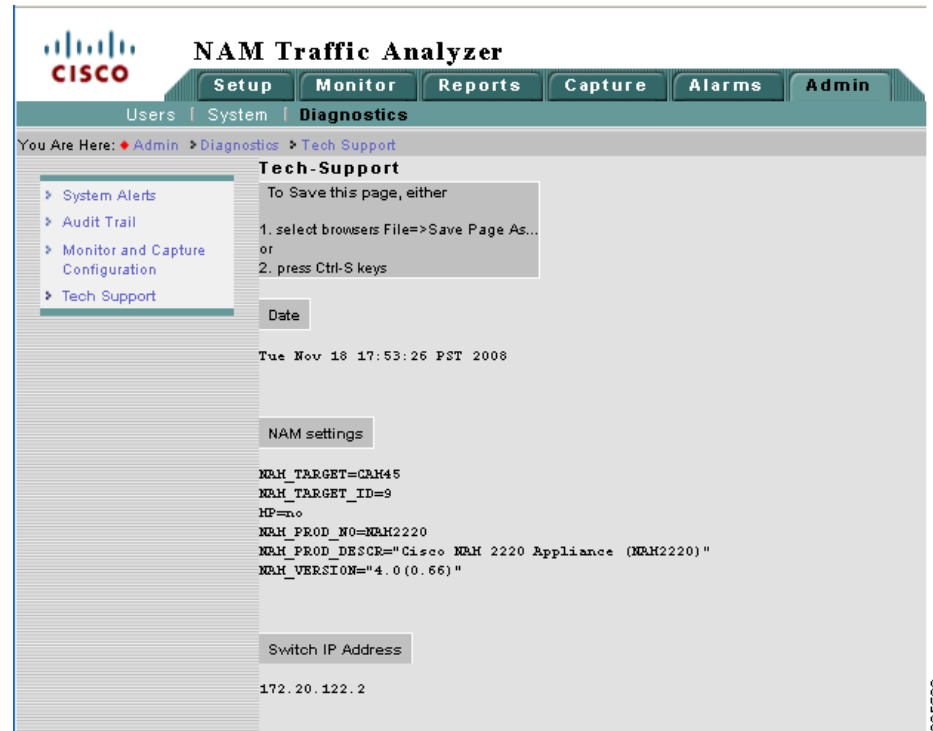
To view tech support:

Step 1 Choose **Admin > Diagnostics**.

Step 2 In the contents, click **Tech Support**.

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window (Figure 2-20).

Figure 2-20 *Diagnostics Tech Support Window*



Step 3 To save the information, select **File>Save As...** from the browser menu.

If you are using Internet Explorer, you can click the **Save This Page** button at the top of the page to download the Tech-Support page as a text file.

Step 4 Select an output destination, filename, and file format, then click **Save**.

Downloading Core Files

To download core files from the Tech-Support page, scroll down to the Core Files section and click on the filename.

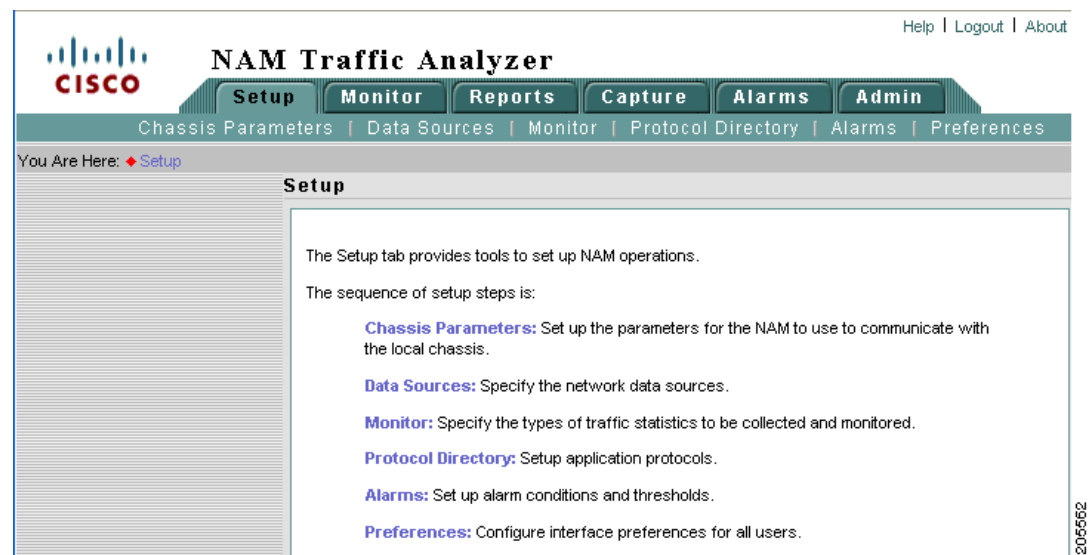


CHAPTER 3

Setting Up the Application

Use the Setup window, [Figure 3-1](#), to set up and configure the NAM application. Set up the NAM application in the sequence shown.

Figure 3-1 Setup Window



Note

The Setup window does not support IPv6 except for the setting of alarm events and thresholds.

This chapter contains the following sections:

- [Chassis Parameters, page 3-2](#)
- [Router Parameters, page 3-8](#)
- [Managed Device Parameters, page 3-9](#)
- [Data Sources, page 3-10](#)
- [Monitoring, page 3-54](#)
- [Protocol Directory, page 3-69](#)
- [Setting Up Alarm Events and Thresholds, page 3-81](#)
- [Setting Global Preferences, page 3-94](#)

Chassis Parameters

From the Chassis Parameter window, you can view the switch system information, enable and disable NBAR, enable and disable port stats (mini-Rmon), and configure switch login configuration.

- [Viewing the Switch Information, page 3-2](#)
- [Setting Up NBAR Protocol Discovery, page 3-3](#)
- [Enabling and Disabling Port Stats \(Mini-RMON\), page 3-5](#)
- [Configuring Switch Login, page 3-8](#)

Viewing the Switch Information



Note

This section applies to WS-SVC-NAM-1 and WS-SVC-NAM-2 devices only.

To view the [Switch Information, Table 3-1](#), choose **Setup > Chassis Parameters**.

Table 3-1 Switch Information

Field	Description
SNMP Test information	Displays the IP address of the NAM and the switch that the SNMP test occurred on.
Name	Name of the switch.
Hardware	Hardware description of the switch.
Supervisor Software Version	Current software version of the Supervisor.
System Uptime	Total time the switch has been running.
Location	Physical location of the switch.
Contact	Contact name of the network administrator for the switch.
SNMP read from switch	SNMP read test result.
SNMP write to switch	SNMP write test result.
Mini-RMON on switch	For Catalyst OS devices, displays the status if Mini-RMON is enabled (Available) or not (Unavailable) For Cisco IOS devices, displays the status if there are any ports with Mini-RMON configured (Available) or not (Unavailable).
NBAR on switch	Displays if NBAR is available on the switch.
VLAN Traffic Statistics on Switch	Displays if VLAN data is Available or Unavailable. Note Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.

Table 3-1 Switch Information (continued)

Field	Description
NetFlow Status	For Catalyst OS devices, if <i>remote</i> NetFlow is configured on the switch, Remote export to <address> on port <number> displays. If <i>local</i> NetFlow is configured on the switch, Local export to module(s) <mod number> displays. For Catalyst 6500 Series devices running Cisco IOS, if NetFlow is configured on the switch, Remote export to NAM <address> on port <number> displays, otherwise the status will display Configuration unknown.

Setting Up NBAR Protocol Discovery

**Note**

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

From the Chassis Parameter window, you can view the NBAR Status information and enable or disable NBAR on all interfaces.

To set up NBAR protocol discovery:

Step 1

Choose **Setup > Chassis Parameters > NBAR Protocol Discovery**.

**Note**

If your switch does not support NBAR, a message displays indicating that NBAR is not supported on your switch.

The NBAR Status window appears with the following options:

- **Details**—Click to display the NBAR Interface Details.
- **Save**—Click to save the device's running configuration.
- **Enable**—Click to enable NBAR on all available interfaces.
- **Disable**—Click to disable NBAR on all interfaces.

**Note**

The Save button is only available on switches running Cisco IOS. Changes occur immediately on switches running Catalyst OS.

The NBAR Interfaces window displays. [Figure 3-2](#) shows an example of the NBAR Interfaces window.

Figure 3-2 NBAR Interfaces Window

NBAR (interfaces)

NBAR Interfaces

Interface Name

☐ All Showing 1-15 of 53 interfaces

Enable	Interface	Interface Description
☒	Fa0/0	FastEthernet0/0
☐	Se0/0	Serial0/0
☒	Fa0/1	FastEthernet0/1
☐	An1/0	Analysis-Module1/0
☒	Fa2/0	FastEthernet2/0
☒	Fa2/1	FastEthernet2/1
☐	Fa2/2	FastEthernet2/2
☐	Fa2/3	FastEthernet2/3
☐	Fa2/4	FastEthernet2/4
☐	Fa2/5	FastEthernet2/5
☐	Fa2/6	FastEthernet2/6
☐	Fa2/7	FastEthernet2/7
☐	Fa2/8	FastEthernet2/8
☐	Fa2/9	FastEthernet2/9
☐	Fa2/10	FastEthernet2/10

205554

The NBAR Interfaces window lists known interfaces by name and type. Check its check box to enable an interface.

You must enable the NBAR Interfaces feature for the NAM to provide information about ethernet ports on the **Monitor > NBAR** window. Select the ports you want to enable, then click **Submit** to turn on NBAR for those ports.

The **All** check box affects only the ports displayed on the current screen. Click the **All** check box to select all ports displayed on the current window. Clear the **All** check box to deselect all ports displayed on the current window. The **Reset** button resets the any changes you might have made to the NBAR window and it reverts to its previous settings.

To view details on an individual Port Stat, click on the **Port Name**. A Port Statistics detail window displays with the following information:

- Alias—User defined port name
- Description—Description of the port
- Type—Type of port
- Mtu—Maximum packet size, in bytes, that the port can handle
- Speed—Speed of the port in bits per second
- Physical Address—Physical address of the port in the switch
- Operational Status—Current operational status of the port
- Admin Status—Current administrative status of the port

**Tip**

To view data for a specific Interface (NBAR) Details table, enter the port name or port type in the text box, then click **Filter**.

**Note**

The Save button is only available on switches running Cisco IOS. Changes occur immediately on switches running Catalyst OS.

Table 3-2 NBAR Interface Details

Field / Operation	Description
NBAR Enabled	Check indicates that NBAR is enabled.
Interface	Name of the interface. Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the Virtual Switch software (VSS), a port name might be displayed as Gi1/2/1to represent a Gigabit port on switch 1, module2, port 1.
Interface Description	Description of the interface.

**Tip**

To view data for a specific interface name or interface type in the Interface Details table, enter the interface name or interface type in the text box, then click **Filter**. To clear the Filter text box, click **Clear**.

Enabling and Disabling Port Stats (Mini-RMON)

**Note**

This section applies to WS-SVC-NAM-1 and WS-SVC-NAM-2 devices only.

You must enable the Mini-Rmon switch feature for the NAM to provide information about ethernet ports on the **Monitor > Port Stats** window. Select the ports you want to enable, then click **Submit** to turn on Mini-Rmon for those ports. Click the **All** check box to select or deselect the ports displayed on the current screen.

The **Reset** button resets the any changes you might have made to the Mini-RMON ports window and it reverts to its previous settings.

**Note**

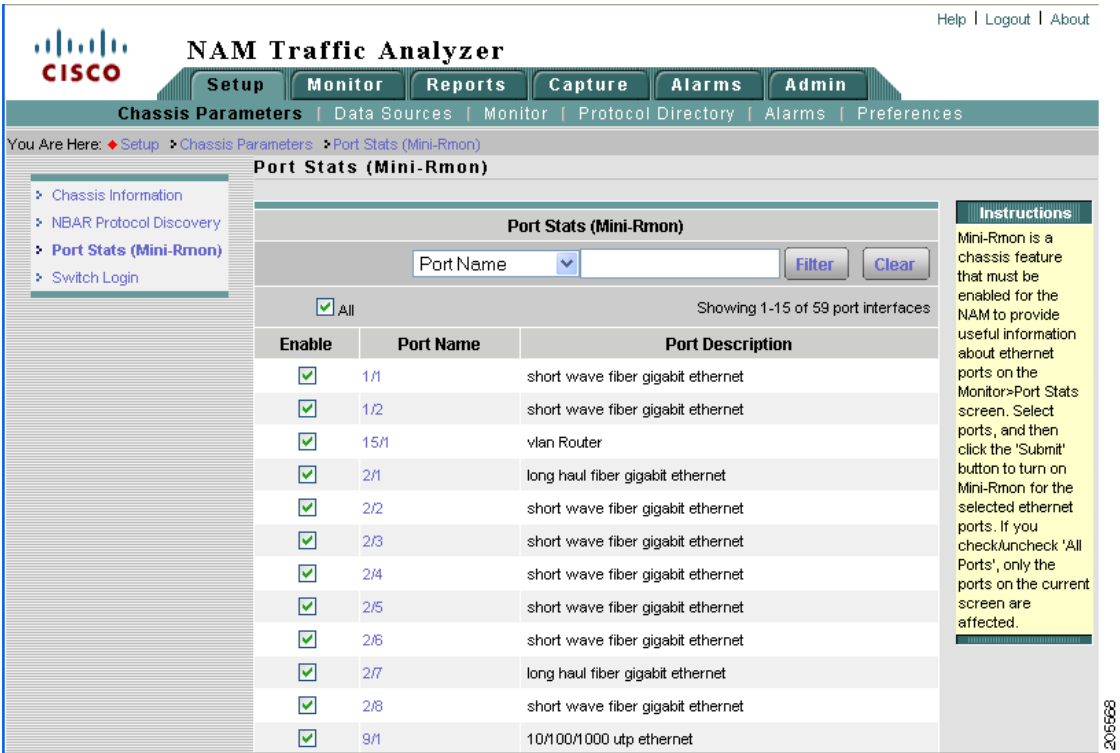
Disabling all ports will also affect any reports and alarms that exist for those ports. For devices running Catalyst OS, disabling all ports will also disable other applications that are using Mini-RMON. For devices running Cisco IOS, only the monitor owner ports will be disabled.

To enable and disable interfaces or view Port Stats details:

- Step 1
- Click **Setup > Chassis Parameters**.
- The [Switch Information](#), [Table 3-1](#), displays.
- Step 2
- From the contents, click **Port Stats (Mini-RMON)**.

The Port Stats (Mini-RMON) window displays listing known ports and their type. [Figure 3-3](#) shows an example of the top portion of the Port Statistics (Mini-RMON) window.

Figure 3-3 Port Stats (Mini-RMON) Window



205568

Port Stats (Mini-RMON) Details

Table 3-3 describes the fields of the Port Stats (Mini-RMON) window.

Table 3-3 Port Stats (Mini-RMON) Details

Field	Description
Mini-RMON Enabled	Indicates with a check mark if Mini-RMON is enabled on the port.
Port Name	Name of the port. Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1. 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 Gi1/2/1to represent a Gigabit port on switch 1, module2, port 1.
Port Description	Description of the port.

Step 3 Click the **Enable** checkbox to enable a port, or click a checked checkbox to disable a port, then click **Submit**.

After you make changes to this window, click **Submit** to apply the changes, then click **Save** to save the changes to the start-up configuration.

The **Refresh** button causes the NAM to update the switch configuration information with the current configuration. The **All** check box affects only the ports listed on this window. The **Reset** button resets the any changes you might have made to the Mini-RMON ports window and it reverts to its previous settings.

Step 4 To view details on an individual Port Stat, click on the **Port Name**.

A Port Statistics detail window displays with the following information:

- Alias—User defined port name
- Description—Description of the port
- Type—Type of port
- Mtu—Maximum packet size, in bytes, that the port can handle
- Speed—Speed of the port in bits per second
- Physical Address—Physical address of the port in the switch
- Operational Status—Current operational status of the port
- Admin Status—Current administrative status of the port

**Tip**

To view data for a specific port name or port type in the Port Stats (Mini-RMON) Details table, enter the port name or port type in the text box, then click **Filter**.

Configuring Switch Login

The NAM uses switch login information to log in to switches to monitor MPLS. You must provide a user name, password (if required), and login method, either telnet or SSH. [Table 3-4](#) describes the fields and functions of the Switch Login Configuration window.


Note

If you are not using MPLS in your network, switch login configuration is not required.

Table 3-4 **Switch Login Configuration**

Field	Description
User Name	User name of a switch administrator
Password	Password of the switch administrator (if one is required)
Verify Password	Verify password of the switch administrator (if one is required)
Login Method	Choose either telnet or SSH
Test Login	Performs a test login with current switch login configuration or with newly entered configuration even if not applied
Apply	Click to set or modify switch login configuration
Reset	Removes switch login configuration entered but not applied and restores previously saved configuration
Clear	Removes switch login configuration from the database

Router Parameters

From the Router Parameter window you can view the router information and set up NBAR Protocol Discovery.

- [Applying Router System Information](#)
- [Setting Up NBAR Protocol Discovery](#)

Applying Router System Information

This section describes how to set router parameters.


Note

This section applies only to NME-NAM devices.

Step 1 Choose **Setup > Router Parameters**.

The Router System Information displays as shown in [Table 3-5](#).

Table 3-5 Router System Information

Field	Description
Name	Name of the router.
Hardware	Hardware description of the router.
Router Software Version	Current software version of the router.
System Uptime	Total time the switch has been running.
Location	Physical location of the router.
Contact	Name of the network administrator for the router.
Router IP Address	IP address of the router.
SNMP Read-Write Community String	Name of the SNMP read-write community string configured on the router
Verify String	Verify the SNMP community string.

- Step 2** Enter the following information:
- Router IP Address
 - SNMP Read Community String
 - Verify String

Managed Device Parameters

From the Managed Device Parameters window, you can set up and view managed device information, enable and disable port stats (mini-Rmon), enable and disable NBAR, and configure managed device login configuration.

**Note**

This section applies only to the Cisco NAM 2200 Series appliance.

To view or set up managed device parameters,

- Step 1** Click **Setup > Managed Device Parameters**.

The Managed Device Parameters window appears. The Managed Device Information displays the following from the appliance's configuration:

- Managed Device Name
- Hardware type
- Managed Device Software Version
- System Uptime
- Location
- Contact Person

- Step 2** Enter the Managed Device IP address in the Managed Device IP Address field.
Enter the same IP address that was configured on the managed device.
- Step 3** Enter the SNMP Read-Write Community String.
Enter the same read-write community string that was configured on the managed device or the NAM cannot communicate via SNMP with the managed device.
- Step 4** Enter the SNMP Read-Write Community String again in the Verify String field.
- Step 5** Click **Apply** to store the information, or click **Reset** to clear the dialog of any characters you entered or restore the previous settings.

**Note**

It is a good idea to click **Test Connectivity** to test the configuration you have entered or modified.

Data Sources

There are several versions of the Cisco NAM:

- WS-SVC-NAM-1
- WS-SVC-NAM-1-250S
- WS-SVC-NAM-2
- WS-SVC-NAM-2-250S
- NME-NAM
 - NME-NAM-80S
 - NME-NAM-120S
- Cisco NAM 2200 Series Appliances
 - Cisco NAM 2204 Appliances
 - Cisco NAM 2220 Appliance

NAM 4.1 virtual blade software also supports the following WAAS appliances:

- WAVE-574
- WAE-674

Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1. 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.

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.

The following information describes how to set up NetFlow and SPAN sessions for the NAM-1 and NAM 2 devices.

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

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 the [Methods of Directing Traffic](#) table (Table 3-6).

Table 3-6 **Methods of Directing Traffic**

Method	Usage Notes
Switch SPAN	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 it is the same as selecting all physical ports comprising the EtherChannel as the SPAN source. There might be limited visibility into MPLS-tagged traffic unless a specific MPLS data source has been defined. For example, when viewing MPLS-tagged traffic in the <i>All SPAN</i> data source, many statistics such as host and conversations will not be available. These statistics are available when viewing the data using the appropriate MPLS data source. Note This method does not apply to NME-NAM devices.
Switch Remote SPAN (RSPAN)	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. There might be limited visibility into MPLS-tagged traffic unless a specific MPLS data source has been defined. For example, when viewing MPLS-tagged traffic in the <i>All SPAN</i> data source, many statistics such as host and conversations will not be available. These statistics are available when viewing the data using the appropriate MPLS data source. Note This method does not apply to NME-NAM devices.
NetFlow Data Export (NDE)	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. SPAN and NDE sources can be in effect simultaneously.

SPAN Sessions


Note

This section applies to WS-SVC-NAM-1 and WS-SVC-NAM-2 devices only.

[Table 3-7, SPAN Sources](#), describes the streams of traffic you can use as SPAN data sources.

Table 3-7 *SPAN Sources*

SPAN Source	One of the following:
Any set of physical ports	- NAM Traffic Analyzer - Switch CLI - Supervisor portCopyTable (SNMP)
Any EtherChannel	- NAM Traffic Analyzer - Switch CLI - Supervisor portCopyTable (SNMP)
Any set of VLANs configured on the local switch	- NAM Traffic Analyzer - Switch CLI - Supervisor portCopyTable (SNMP)
Packets from a remote switch arriving via RSPAN Note You can select only one RSPAN VLAN as a SPAN source.	- NAM Traffic Analyzer - Switch CLI - Supervisor portCopyTable (SNMP) <i>and</i> - Configuration on remote switch

You can also use locally generated NDE records (the NDE source) as a packet stream to populate NAM collections. You can activate only a subset of the NAM collection types defined in the NDE Collection Types Table, [Table 3-8](#), on the NDE source.


Note

These are the only collection types for which monitoring is supported on the NDE source; NDE records have insufficient information to implement other collection types.

Table 3-8 *NDE Collection Types Table*

Collection Type	Source
Protocol	RMON2 protocol distribution table.
Host	RMON2 nlHost and alHost tables.
Conversation	RMON2 nlMatrix and alMatrix tables.
DiffServ stat	DSMON statistics table for remote switches and routers.
DiffServ apps	DSMON applications table for remote switches and routers.
DiffServ hosts	DSMON host table for remote switches and routers.

Table 3-9 Active SPAN Sessions Dialog

Column	Description
Monitor Session	Monitor session of the SPAN. Note For switches running Cisco IOS software only.
Type	Type of SPAN source
Source - Direction	Source of the SPAN session and direction of the SPAN traffic. For port SPAN types, the source displays the port name and source status <i>after</i> you SPAN it—down, testing, or dormant. When creating a SPAN session, you can select all ports regardless of their state. See Table 3-10 for a description of the possible SPAN states. Note For switches running Cisco IOS software only.
Dest. Port	Destination port of the SPAN session.
Dest. Module	Destination module of the SPAN session.
Status	Status of the SPAN session: Active—Traffic at the SPAN source is being copied to the SPAN destination Inactive—Traffic at the SPAN source will not be copied to the SPAN destination Unknown—A mixture of both active and inactive status
Create	Click to create a SPAN session.
Save	Saves the current active SPAN session in the running-configuration to the startup-configuration for switches running Cisco IOS software only.
Add Dest. Port 1	Click to add NAM Port 1 to the selected SPAN session as a SPAN destination. Note This button is labeled Add Dest. Port on the NAM-1.
Add Dest. Port 2	Click to add NAM Port 2 to the selected SPAN session as a SPAN destination. Note This option is not available on the NAM-1.
Edit	Click to edit the selected SPAN session.
Delete	Click to delete the selected SPAN session.

**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 3-10](#) lists the possible SPAN states. The SPAN state displays in parenthesis in the Source - Direction column.

Table 3-10 Possible SPAN States

State	Description
Active	SPAN source is valid and traffic from the source is being copied to the SPAN destination
NotInService	SPAN source might be valid, but traffic that appears at the source will not be copied to the SPAN destination
NotReady	The SPAN source might be valid, but traffic that appears at the source will not be copied to the SPAN destination
CreateAndGo	The SPAN source might be valid, but the SPAN source is being added to the SPAN session
CreateAndWait	The SPAN source might be valid, and the SPAN source is being added to the SPAN session
Destroy	The SPAN source is being removed from the SPAN session.

Creating a SPAN Session


Note

This section does not apply to NME-NAM devices.

Creating a SPAN session on a switch running Catalyst OS software and a switch running Cisco IOS software are different. The following procedure applies to switches running both Catalyst OS and Cisco IOS software unless otherwise stated.

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

The Active SPAN Sessions Dialog ([Table 3-9](#)) displays. The SPAN session directed to the NAM is selected by default, otherwise the first radio button is selected.

Step 2 Click **Create**.

The Create SPAN Session Dialog ([Table 3-11](#)) displays. Switch Port is the default for the SPAN Type.

Step 3 Select the appropriate information.
Table 3-11 Create SPAN Session Dialog

Field	Description
Monitor Session	Monitor session of the SPAN. Note For switches running Cisco IOS or Catalyst OS 8.4 (and later) software only.
SPAN Type	- SwitchPort - VLAN - EtherChannel - RSPAN VLAN Note You can have only one RSPAN VLAN source per SPAN session.

Table 3-11 Create SPAN Session Dialog

Field	Description
Switch Module List	Lists all modules on the switch other than NAMs and Switch Fabric Modules.
SPAN Destination Interface	The NAM interface to which you want to send data.
SPAN Traffic Direction	- Rx - Tx - Both Note Not applicable to RSPAN VLAN SPAN types.
Available Sources	SPAN sources that are available for the selected SPAN type.
Add	Adds the selected SPAN source.
Remove	Removes the selected SPAN source.
Remove All	Removes all the SPAN sources.
Selected Sources	SPAN sources selected.
Refresh	Causes the NAM to update the switch configuration information with current configuration.
Submit	Creates the SPAN configuration; saves the configuration.

Step 4 To create the SPAN session, click **Submit**.

The Active SPAN Sessions window displays and the SPAN session is saved for switches running Catalyst OS software only.

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.

Editing a SPAN Session

You can only edit SPAN sessions that have been directed to the NAM.

**Note**

This section does not apply to NME-NAM devices.

To edit a SPAN session:

Step 1 Click **Setup > Data Sources**.

The Active SPAN Sessions dialog box displays.

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

The Edit SPAN Session Dialog Box, [Table 3-12](#), displays.

Step 3 Make the appropriate changes.

Table 3-12 *Edit SPAN Session Dialog Box*

Field	Description
Monitor Session	Monitor session of the SPAN.
SPAN Type	Type of SPAN session.
Switch Module List	Lists all modules on the switch other than NAMs and Switch Fabric Modules.
SPAN Destination interface	The NAM interface to which you want to send data.
SPAN Traffic Direction	Direction of the SPAN traffic. Note You cannot edit the SPAN direction on switches running Catalyst OS software. For such switches, all SPAN sources in a SPAN session must be in only one direction.
Available Sources	SPAN sources available for the selected SPAN type.
Add	Adds the selected SPAN source
Remove	Removes the selected SPAN source.
Remove All	Removes all the SPAN sources.
Selected Sources	SPAN sources selected.
Refresh	Causes the NAM to update the switch configuration information with current configuration.
Submit	Saves changes.
Reset	Clears all changes since previous Submit.

Deleting a SPAN Session



Note

This section does not apply to NME-NAM devices.

To delete a SPAN session, select it from the Active SPAN Session dialog box, then click **Delete**.
Use this anchored frame for wider illustrations that align with left edge of text block.

Deduplication



Note

This section applies only to Cisco NAM 2200 Series appliances.

NAM 4.1 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 Click **Setup > Data Sources**.

Step 2 Under SPAN in the contents menu, click **Deduplication**.

The Packet Deduplication Settings window displays as shown in [Figure 3-4](#).

Figure 3-4 Packet Deduplication Settings

Step 3 Click the Enabled check box to enable packet deduplication.

Step 4 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 120ms apart, the second packet would not be dropped. If the identical packets arrive 80 ms apart, the second packet would be dropped.

Step 5 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 and MPLS 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 6 Click **Apply** to enable the settings you have entered, or click **Reset** to cancel any change.

VLAN Data Sources

**Note**

This section applies only to Cisco 2200 Series NAM appliances.

Unlike NAM-1 and NAM-2 devices where you can choose VLAN data sources from a drop-down menu, you must create VLAN data sources for the Cisco 2200 Series NAM appliance to monitor.

Figure 3-5 shows an example of the available VLAN Data Sources window.

You must create the VLAN data sources here first or they will not be available in the **Data Source** drop-down menu on the **Setup > Monitor > Core Monitoring** window.

To create a VLAN data source:

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

The Active SPAN Sessions Dialog displays.

Step 2 Click **VLANs**.

The VLAN Data Sources window displays any VLAN data sources that have already been created.

Step 3 Click **Create**.

The VLAN Data Source window displays. This window lists available VLANs. The VLANs with check marks have data sources created. Figure 3-5 shows an example of the VLAN Data Source window.

The NAM appliance detects the available VLANs after you set up the IP address and Community String of the *managed device* on the **Setup > Managed Device Parameters** window.

Step 4 You can use the pull-down menu to choose either VLAN ID or VLAN Data Source name, then enter a string in the Filter field, and click **Filter** to find a specific VLAN data source. You can also click a check box to choose a specific VLAN ID.

Click **Refresh** to refresh the database of the device to which the appliance is connected.

Click **Submit** to create or delete VLAN data sources, depending on the data source you checked.

Figure 3-5 Available VLANs

VLAN Data Sources

Data Source Name

☐ All Showing 1-15 of 16 VLAN data sources

Enable	Data Source Name	VLAN Name	State
☒	VLAN 1	default (1)	Operational
☒	VLAN 2	probe_vlan (2)	Operational
☒	VLAN 3	ixLoadServerTraffic (3)	Operational
☒	VLAN 4	ixLoadClientTraffic (4)	Operational
☒	VLAN 10	3845_Crash_Test (10)	Operational
☐	VLAN 35	connect_to_gateway (35)	Operational
☐	VLAN 36	VLAN0036 (36)	Operational
☐	VLAN 37	VLAN0037 (37)	Operational
☐	VLAN 38	VLAN0038 (38)	Operational
☐	VLAN 39	VLAN0039 (39)	Operational
☐	VLAN 40	VLAN0040 (40)	Operational
☐	VLAN 150	VLAN0150 (150)	Operational
☐	VLAN 600	VLAN0600 (600)	Operational
☐	VLAN 890	VLAN0890 (890)	Operational
☐	VLAN 3000	VLAN3000 (3000)	Operational

Rows per page: 15

Deleting a VLAN Data Source

To delete a VLAN data source:

-
- Step 1** Choose **Setup > Data Sources**.
- The Active SPAN Sessions Dialog displays.
- Step 2** Click **VLANs**.
- The VLAN Data Sources window displays and lists VLAN data sources available on the NAM appliance.
- [Figure 3-5, Available VLANs](#), shows an example of the VLAN Data Sources window.
- Step 3** Click the check box of a VLAN data source. Then click **Delete**.
-

Understanding NetFlow Interfaces

To use a managed device as an NDE data source for the NAM, you must configure the managed 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. By default the switch's local supervisor engine is always available as an NDE device.

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.

Distinguishing among different interfaces on the remote NDE devices is a feature in this release that allows you to arbitrarily bundle groups of interfaces on each remote NDE device into a conceptual data source instead of simply grouping all flows into the same collections.

If you try to distinguish every interface on every managed device (potentially in both directions separately), this action could result in a large, unmanageable number of data sources. By using conceptual data sources, you have complete flexibility to group all interfaces in all directions into a single conceptual data source.

You could also choose to create a separate conceptual data source for each interface on the device. In general, you can combine any number of "simple flow paths" to form a conceptual data source. Each simple flow path can consist of a single interface in the input direction, the output direction, or both directions.

The following restrictions apply to creating conceptual data sources and assigning flow paths to them.

- Any interface that is specified as an input interface for a flow path cannot be specified as an input interface in another conceptual data source for the same device. It also cannot be specified as a bidirectional interface in another flow path for the same conceptual data source.
- Any interface that is specified as an output interface for a flow path cannot be specified as an output interface in another conceptual data source for the same device. It also cannot be specified as a bidirectional interface in another flow path for the same conceptual data source.
- Any interface that has been specified as a bidirectional interface for a flow path cannot be specified as a bidirectional interface in another conceptual data source for the same device. It also cannot be specified as an input or output interface in another flow path for the same conceptual data source.

Understanding NetFlow Flow Records

An NDE packet contains multiple flow records. Each flow record has two fields:

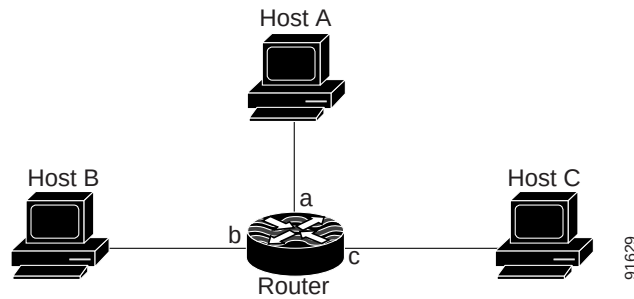
- Input SNMP ifIndex
- Output SNMP ifIndex



Note

This information might not be available because of NDE feature incompatibility with your Cisco IOS or Catalyst OS version or because of an NDE flow-mask configuration. For more information on flow-mask compatibility, see the ["NDE Flow Masks and V8 Aggregation Caches" section on page 4-5](#).

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 3-6](#), shows a sample network configuration with a NetFlow router.

Figure 3-6 Sample NetFlow Network

The Reporting Flow Records table (Table 3-13) lists the reported flows if NetFlow is enabled on interface a.

Table 3-13 Reporting Flow Records

Input Interface	Output Interface	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	No
b	a	No
c	a	No
c	b	No

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 or Catalyst OS. 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
```

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 Running Catalyst OS

Step 1 Select the version of NDE.

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



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

- Step 2** Select NDE flow mask to be full.
- ```
Prompt>(enable) set mls flow full
```
- Step 3** Enable NDE export.
- ```
Prompt>(enable) set mls nde enable
```
- Step 4** Export NDE packets to UDP port 3000 of the NAM.
- ```
Prompt>(enable) set mls nde <NAM address> 3000
```
- 

### For Devices That Support NDE Export From Bridged-Flows 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) set mls nde full
```
- Step 3** Enable NDE export.
- ```
Prompt>(enable) set mls nde enable
```
- Step 4** Export the NDE packets to the NAM.
- ```
Prompt>(enable) set snmp extendedrmon netflow enable <NAM-slot>
```
- 

## 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 LAN VACLs on Catalyst OS, the security Access Control List (ACL) feature can be used to achieve the same result. For more information on using these features, see your accompanying switch documentation.

```
Cat6509#config terminal
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface AM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

To monitor egress traffic only, get the VLAN ID that is associated with the WAN interface by using the following command:

```
Cat6509#show cwan vlan
Hidden VLAN swidb->i_number Interface
1017 94 ATM6/0/0.1
```

Once 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
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
```

## Managing NetFlow Devices

Before you can monitor NetFlow data, you must add the NetFlow devices to be monitored. The remote NDE device must also be configured to export NDE packets to the NAM. For more information on configuring NetFlow on devices, see the [“Configuring NetFlow on Devices” section on page 3-22](#) or your accompanying device documentation. The following topics help you set up and manage the devices used for NetFlow monitoring:

- [Adding NetFlow Devices, page 3-26](#)
- [Editing NetFlow Devices, page 3-27](#)
- [Deleting NetFlow Devices, page 3-27](#)
- [Testing NetFlow Devices, page 3-27](#)
- [Creating Custom Data Sources, page 3-28](#)
- [Using the Listening Mode, page 3-30](#)

### Adding NetFlow Devices

After you add a NetFlow device, NetFlow data sources are automatically created for that device. You can use the Listening Mode to verify that NDE packets are active on these data sources. For more information on using the Listening Mode, see the [“Using the Listening Mode” section on page 3-30](#).

To create a device:

---

**Step 1** Click **Setup > Data Sources**.

The Active SPAN Sessions table displays.



---

**Note** For NME-NAM devices, the Netflow Devices table displays.

---

**Step 2** In the contents, click **Netflow --Devices**.

The NetFlow Devices table displays.

**Step 3** Click **Add**.

The New Device dialog box appears.

**Step 4** Enter the device name and community string.

**Step 5** To create a NetFlow custom data source, click the Create Data Source check box.

When the check box is checked, a data source will be automatically created with a name like *NDE-ip address*. You can edit or delete the automatically created data source by going to the **Setup > Data Sources > NetFlow > Custom Data Sources** window.

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

Otherwise, click **Reset** to clear the entries in the dialog box, or click **Cancel** to leave the entries unchanged.

---



## Editing NetFlow Devices

**Note**

You cannot edit the local switch.

To edit a NetFlow device:

- 
- Step 1** Click the **Setup** tab, then click **Data Sources**.  
The Active SPAN Sessions table displays.
- Step 2** In the contents, click **Devices**.  
The NetFlow Devices table displays.
- Step 3** Select the device you wish to edit from the table and click **Edit**.  
The Edit Device window appears.
- Step 4** Make the desired changes and do one of the following:
- To save the changes, click **OK**.
  - To restore the original entries, click **Reset**,
  - To leave the configuration unchanged, click **Cancel**.
- 

## Deleting NetFlow Devices

To delete a NetFlow device:

- 
- Step 1** Click **Setup > Data Sources**.  
The Active SPAN Sessions table displays.
- Step 2** In the contents, click **Devices**.  
The NetFlow Devices table displays.
- Step 3** Select the device you wish to delete from the Devices dialog box, then click **Delete**.

**Note**

All custom NetFlow data sources that are related to the device will be deleted.

---

## 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 ([Table 3-14](#)) displays.

**Table 3-14**      **Device System Information Dialog Box**

| Field                   | Description                                                   |
|-------------------------|---------------------------------------------------------------|
| Name                    | Name of the device.                                           |
| Hardware                | Hardware description of the device.                           |
| Device Software Version | The current software version running on the device.           |
| System Uptime           | Total time the device has been running since the last reboot. |
| Location                | Location of the device.                                       |
| Contact                 | Contact information for the device.                           |
| SNMP read from device   | SNMP read test result. For the local device only.             |

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.

To view the NetFlow V9 templates, click the **V9 Templates** button. For more information, see [Table 3-17](#) in [Using the Listening Mode](#).

## Creating Custom Data Sources

A NetFlow data sources are automatically learned when you create a device in the Devices section. For more information on creating NetFlow devices, see the [“Adding NetFlow Devices” section on page 3-26](#). This option allows you to create custom data sources on NetFlow devices with specific interface information.

To create a custom data source:

- 
- Step 1**      Click **Setup > Data Sources**.
  - Step 2**      From the contents menu, choose **Custom Data Sources**.  
The NetFlow Data Sources table displays.
  - Step 3**      Click **Create**.  
The following table shows the wizard used to create or edit a NetFlow data source.

|        | Wizard Page         | References                                                                       |
|--------|---------------------|----------------------------------------------------------------------------------|
| Step 1 | Device Selection    | <a href="#">“Selecting a NetFlow Device” section on page 3-29</a>                |
| Step 2 | Interface Selection | <a href="#">“Selecting the Interfaces” section on page 3-29</a>                  |
| Step 3 | Summary             | <a href="#">“Verifying NetFlow Data Source Information” section on page 3-30</a> |

## Selecting a NetFlow Device

To select a NetFlow device:

- 
- Step 1** Select the NetFlow device from the list.
- Step 2** Enter the data source name. If none is entered, a default name will be created.
- Step 3** Click **Next**.
- 

## Selecting the Interfaces

To select an interface:

- 
- Step 1** Select the data flow direction.
- Step 2** Select the interfaces you want to add from the Available Interfaces section.



**Tip** Use Ctrl+Click to select multiple interfaces.

---

If no interfaces are listed, manually enter them in the Interface Index text box.

- Step 3** Click **Add**.
- The selected interfaces are displayed in the Selected Interfaces section.
- To remove interfaces, select them from the Selected Interfaces section, then click **Remove**.
  - To remove all interfaces from the Selected Interfaces section, click **Remove All**.
- Step 4** Click **Next**.
- 

### Special (0) Interface

NDE packets sometimes have NetFlow records reporting either (or both) input if-index and output if-index fields as being 0. This could be a result of one or more of the following reasons:

- Flows are terminated at the device.
- Configurations of the device.
- Unsupported NetFlow feature of the platform at the device.

For more information, see the accompanying documentation for your NetFlow device.

### Verifying NetFlow Data Source Information

To verify NetFlow data source information:

- 
- Step 1** Verify the information is correct.
- Step 2** Do one of the following:
- To save the configuration, click **Finish**.
  - To cancel any changes and go back to the NetFlow Data Sources table, click **Cancel**.
- 

### Editing a Custom Data Source

To edit a custom data source:

- 
- Step 1** Choose **Setup > Data Sources**.
- Step 2** Click **Custom Data Sources**.
- The NetFlow Data Sources table displays.
- Step 3** Select the data source you wish to edit, then click **Edit**.
- The wizard used to edit NetFlow data sources displays.
- Step 4** Make the desired changes and do one of the following:
- To accept the changes, click **Finish**.
  - To cancel the changes, click **Cancel**.
- 

### Deleting a Custom Data Source

To delete a data source, select it from the NetFlow Data Source table, then click **Delete**.



#### Note

You cannot delete the default data sources.

---

### Using the Listening Mode

The Listening Mode of the NAM allows you to view the IP addresses of devices sending NDE packets to the NAM, the number of NDE packets, and time that the last NDE packet was received. The NetFlow Listening Mode table only lists devices that the NAM currently receives NDE packets from.

To use listening mode:

- 
- Step 1** Choose **Setup > Data Sources**.
- Step 2** In the contents, click **Listening Mode**.
- The NetFlow Listening Mode Table ([Table 3-15](#)) displays.

**Table 3-15 NetFlow Listening Mode Table**

| Field                  | Description                                           |
|------------------------|-------------------------------------------------------|
| Start Time             | The timestamp of when the Start button was clicked.   |
| Address                | IP address of the learned device.                     |
| # Received NDE Packets | Number of NetFlow data export (NDE) packets received. |
| Last Packet Received   | Time stamp the last NDE packet was received.          |

**Step 3** Click **Start**.

**Step 4** To clear the table and stop monitoring, click **Stop**.

**Note**

Learning will automatically be disabled after 1 hour.

**Viewing Details from the NetFlow Listening Mode Table**

Select the device from the table, then click **Details**.

The Device Details Window ([Table 3-16](#)) displays.

**Table 3-16 Device Details Window**

| Field                              | Description                                                                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Added                       | Indicates if the device was added to the NAM device table.                                                                                                         |
| Interfaces Reported in NDE Packets | Lists the interfaces that NDE packets were seen on.<br>For example:<br>Special (0) (Output)<br>(1) (Input/Output)<br>(2) (Input/Output                             |
|                                    | <br><b>Note</b> Protocol-Prefix NDE packets do not have interfaces information. |

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 Details window. For more information, see:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_feature\\_guide09186a00801b0696.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a00801b0696.html)

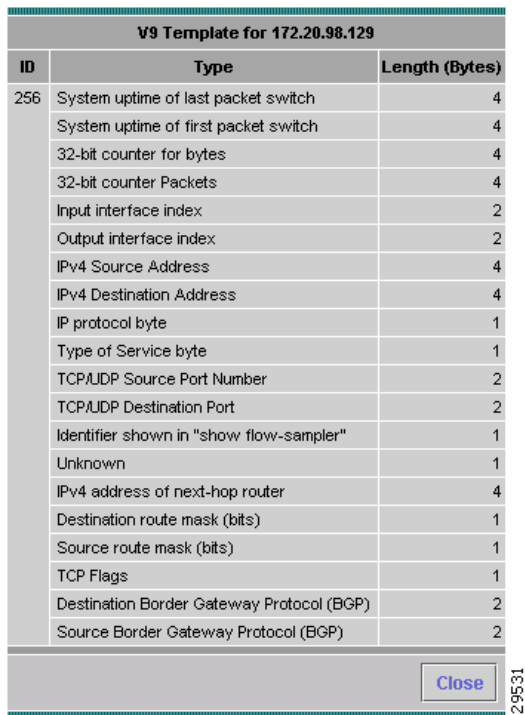
**Note**

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

To view the NetFlow V9 templates, click the **V9 Templates** button.

The V9 Templates Window ([Figure 3-7](#)) displays (see example below).

**Figure 3-7 V9 Templates Window**



| ID  | Type                                      | Length (Bytes) |
|-----|-------------------------------------------|----------------|
| 256 | System uptime of last packet switch       | 4              |
|     | System uptime of first packet switch      | 4              |
|     | 32-bit counter for bytes                  | 4              |
|     | 32-bit counter Packets                    | 4              |
|     | Input interface index                     | 2              |
|     | Output interface index                    | 2              |
|     | IPv4 Source Address                       | 4              |
|     | IPv4 Destination Address                  | 4              |
|     | IP protocol byte                          | 1              |
|     | Type of Service byte                      | 1              |
|     | TCP/UDP Source Port Number                | 2              |
|     | TCP/UDP Destination Port                  | 2              |
|     | Identifier shown in "show flow-sampler"   | 1              |
|     | Unknown                                   | 1              |
|     | IPv4 address of next-hop router           | 4              |
|     | Destination route mask (bits)             | 1              |
|     | Source route mask (bits)                  | 1              |
|     | TCP Flags                                 | 1              |
|     | Destination Border Gateway Protocol (BGP) | 2              |
|     | Source Border Gateway Protocol (BGP)      | 2              |

Close

The V9 Templates Table ([Table 3-17](#)) describes the template data.

**Table 3-17 V9 Templates Table**

| Field          | Description                       |
|----------------|-----------------------------------|
| Type           | Type of template data.            |
| Length (Bytes) | Length of template data in bytes. |

### Adding a Device To Monitor

To add a device to monitor:

- Step 1** Select the device from the table, then click **Add**.

The New Device Window displays.

- Step 2** Enter the device information and click OK.

The new device is added to the NetFlow Devices table.

## Testing the Router Community Strings

### For NME-NAM Devices Only

Before the router can send information to the NAM using SNMP, the router community strings set in the NAM Traffic Analyzer 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 > Router Parameters**.  
The Router Parameters dialog box displays.
- Step 2** Click **Test**.  
The Router Community String Test dialog box displays.
- 

## Setting Up an Interface



#### Note

This section applies to NME-NAM devices only.

Before you can view traffic statistics and the TopN traffic for applications, hosts, and conversations, you must first set up the interfaces.

Click in the check box to enable Netflow NDE on the selected interface and all of its sub-interfaces. A NAM NDE datasource will be created for each enabled sub-interface, and hosts, conversations and application NDE data sources will also be created. This action populates the **Monitor > Router** detail window with the hosts, conversations and application statistics.

In the case of parent interfaces with sub-interfaces, only the leaf child will be enabled. For example, ATM2/0.1-atm-subif has child ATM2/0.1-aal5-layer. Only the aal5-layer will be enabled. NDE will only be seen on this child interface.



#### Note

Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1. 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, module 2, port 1.

To set up interfaces to enable you to view traffic statistics:

---

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

NAM 4.1 supports up to 1,500 datasources.

**Step 2** Click **Interfaces** in the content menu.

The Interfaces window displays.

Router interfaces and SNMP Read/Write Community strings must also be configured. See [Router Parameters, page 3-8](#) for more information.

**Step 3** Check the **Enable** check box for each interface you want to enable.

---

## Understanding Wide Area Application Services

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.

WAE flow agents 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 WAAS flow agents and performs application response time 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.

Cisco WAAS helps enterprises to meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
  - Low data rates (constrained bandwidth)
  - Slow delivery of frames (high network latency)
  - Higher rates of packet loss (low reliability)

For more information about WAAS and configuring the WAAS components, see the document:



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

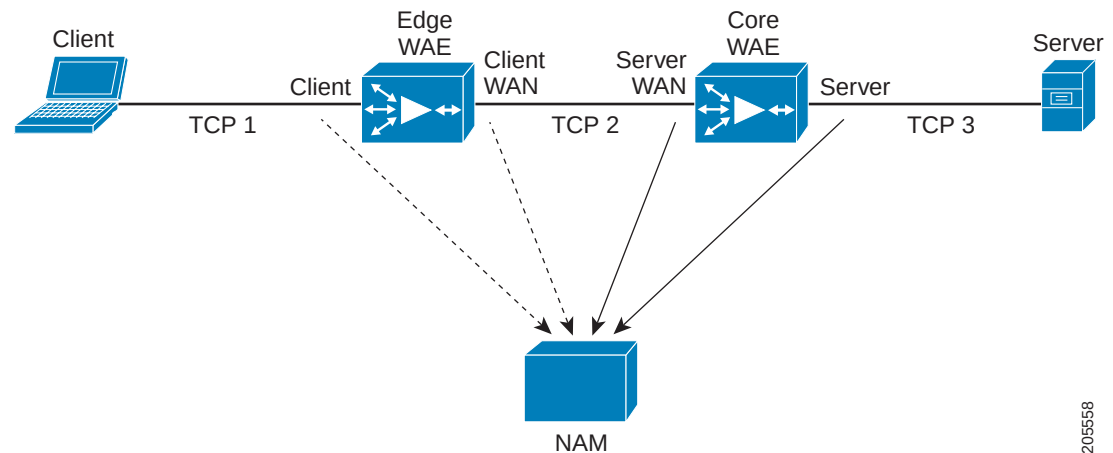
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/waas/v4019/configuration/guide/waas4cfg.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html)

## ART Monitoring from WAAS Data Sources

The NAM processes the TCP flow data exported from WAAS Flow Agents 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, four represented by a WAAS data source. [Figure 3-8](#) shows an example of the data collection points. In [Figure 3-6](#), 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 3-8 WAAS Data Sources (Data Collection Points)**



You can use the NAM GUI to configure data sources at the following locations in the network:

- **Client**—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.
- **Client WAN**— 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.
- **Server WAN**—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.
- **Server**—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.

You can also configure a data source to use Export Passthrough data. For more information about configuring WAAS data sources, see [Configuring WAAS Data Sources, page 3-38](#).

## Monitoring Client Data Sources

By monitoring the TCP connections between the client and the WAE device (Client segment in [Figure 3-8](#)), you can measure the following ART metrics:

- Total Delay (TD) as experienced by the client
- Total Transaction Time as experienced by the client
- Bandwidth usage (bytes/packets) before optimization
- Number of transactions and connections.
- Network Delay broken down into two segments: client-edge and edge-server

## Monitoring WAN Data Sources

By monitoring the TCP connections between the edge and core WAE devices (Client WAN and Server WAN segments in [Figure 3-8](#)), you can measure the following:

- Bandwidth usage (bytes/packets) after optimization
- Network Delay 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 3-8](#)), you can measure the following ART metrics:

- Application (Server) Delay (without proxy acceleration/caching server)
- Network Delay between the core WAE device and the servers

**Note**

---

NAM measures Network Delay (ND) by monitoring the TCP three-way handshake between the devices.

---

## 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 which WAAS segments you want to monitor as WAAS data sources: Client, Client WAN, Server WAN, and/or Server. See [Configuring WAAS Data Sources, page 3-38](#), for more detailed information.

You can also use the Central Manager (CM) to centrally to issue WAAS CLI commands to configure a large number of WAEs at one time.

**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 [Managing a WAAS Monitored Server, page 3-42](#), for more detailed information.

For more information about WAAS and configuring the WAAS components, see the document:

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

[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/waas/v4019/configuration/guide/waas4cfg.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html)

This section contains the following topics:

- [Adding a WAAS Device, page 3-37](#)
- [Configuring WAAS Data Sources, page 3-38](#)
- [Deleting a WAAS Data Source, page 3-40](#)

## Adding a WAAS Device

**Note**

This step is not usually necessary because export-enabled WAAS devices are detected and added automatically. See [Managing WAAS Devices, page 3-36](#), 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** Click **Setup > Data Sources**.

**Step 2** From the contents menu, choose **WAAS > Devices**.

The WAAS Custom Data Sources table displays. [Figure 3-9](#) shows an example of the WAAS Custom Data Source table.

**Figure 3-9 WAAS Custom Data Sources Table**

| WAAS Devices                                                 |                |                                                                                                                            |                                                                                                                                                                  |                                                           |
|--------------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| <input type="checkbox"/> All                                 | Device         | Information                                                                                                                | Status                                                                                                                                                           | DataSource                                                |
| <input type="checkbox"/>                                     | 172.20.107.117 | nam-edge-wae (00:16:9d:38:b6:d1) Cisco WAAS 4.0.13-b23 [NM-WAE]<br>Last collection: Thu Aug 14 20:25:49 2008 (32272 bytes) | Active                                                                                                                                                           | WAE-172.20.107.117-Client<br>WAE-172.20.107.117-ClientWAN |
| <input type="checkbox"/>                                     | 172.20.107.118 | nam-core-wae (00:16:9d:38:b6:cf) Cisco WAAS 4.0.13-b23 [NM-WAE]<br>Last collection: Thu Aug 14 20:25:22 2008 (64952 bytes) | Active                                                                                                                                                           | WAE-172.20.107.118-SvrWAN<br>WAE-172.20.107.118-Server    |
| <input type="text"/> Select a device then take an action --> |                |                                                                                                                            | <input type="button" value="Add"/> <input type="button" value="Config"/> <input type="button" value="Enable Auto-Config"/> <input type="button" value="Delete"/> |                                                           |

**Step 3** Click **Add**.

The New Device dialog box displays. [Figure 3-10](#) shows an example of the Add New WAAS Device window.

**Figure 3-10 Add New WAAS Device**

The screenshot shows a 'New Device' configuration window. At the top, there's a title bar 'New Device'. Below it is a text input field labeled 'WAAS Device IP Addr:'. Underneath is a section titled 'Monitor WAAS segment(s):' which contains five checkboxes: 'Client', 'Client WAN', 'Server WAN', 'Server', and 'Export Passthru Response Time'. At the bottom of the window are three buttons: 'Submit', 'Reset', and 'Cancel'. A small vertical text '206584' is visible on the right side of the window.

**Step 4** Enter the device IP address in the Device field, and click to choose the type of WAAS data sources from this device to monitor.

See [Configuring WAAS Data Sources, page 3-38](#), for more information.

**Step 5** Click **Submit** to add the new WAAS custom data source.

## Configuring 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 ART metrics.

To configure a WAAS device's custom data source:

**Step 1** Click **Setup > Data Sources**.

**Step 2** From the contents menu, choose **WAAS -- Devices**.

The WAAS Device table displays.

**Step 3** Choose the WAAS device you want to modify, then click **Config**.

The Config Device dialog box displays the WAAS device IP address and the WAAS segments previously set to monitor. [Figure 3-11](#) shows an example of the Configure WAAS Device window.

**Figure 3-11**      **Configure WAAS Device**

**Config Device**

**WAAS Devices:** 172.20.107.118

**Monitor WAAS segments:**

☐ Client

☐ Client WAN

☒ Server WAN

☒ Server

☐ Export Passthru Response Time

**Submit** **Reset** **Cancel**

You can configure the WAAS data sources to monitor the following WAAS segments as shown in [Figure 3-8, 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.

[Table 3-18, 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 and NAM-2 blades. Scenario #2 is typical when using NM-NAM and NME-NAM devices.

**Table 3-18**      **WAAS Data Source Configurations**

|   | Deployment Scenario                                                                                                                                      | Edge WAE Data Source | Core WAE Data Source |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|----------------------|
| 1 | <ul style="list-style-type: none"> <li>• Clients in the edge (branch)</li> <li>• Servers in the core (data center)</li> <li>• NAM in the core</li> </ul> | Client               | Server<br>Server WAN |
| 2 | <ul style="list-style-type: none"> <li>• Clients in the edge (branch)</li> <li>• Servers in the core (data center)</li> <li>• NAM in the edge</li> </ul> | Client<br>Client WAN | Server               |
| 3 | <ul style="list-style-type: none"> <li>• Servers in the edge (branch)</li> <li>• Clients in the core (data center)</li> <li>• NAM in the core</li> </ul> | Server               | Client<br>Client WAN |
| 4 | <ul style="list-style-type: none"> <li>• Servers in the edge (branch)</li> <li>• Clients in the core (data center)</li> <li>• NAM in the edge</li> </ul> | Server<br>Server WAN | Client               |

**Table 3-18**      **WAAS Data Source Configurations**

|   | Deployment Scenario                                                                                                                            | Edge WAE Data Source                         | Core WAE Data Source                         |
|---|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|----------------------------------------------|
| 5 | <ul style="list-style-type: none"> <li>Clients and servers in the edge (branch) and the core (data center)</li> <li>NAM in the core</li> </ul> | Client<br>Server                             | Client<br>Server<br>Client WAN<br>Server WAN |
| 6 | <ul style="list-style-type: none"> <li>Clients and servers in the edge (branch) and the core (data center)</li> <li>NAM in the edge</li> </ul> | Client<br>Server<br>Client WAN<br>Server WAN | Client<br>Server                             |

SPAN data sources might take the place of the WAE Server data sources listed in [Table 3-18](#). For example, if you already configure SPAN to monitor the server LAN traffic, its 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 4** To export WAAS pass-through data to the External Response Time Reporting Console, click **Export Passthru to External Console**.

**Note**

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

See [Response Time Export, page 2-25](#), for more information.

## Deleting a WAAS Data Source

To delete a WAAS custom data source:

- Step 1** Click **Setup > Data Sources**.
- Step 2** From the contents menu, choose **WAAS > Devices**.  
The WAAS Custom Data Sources table displays.
- Step 3** Choose the WAAS custom data source you want to delete, then click **Delete**.  
A dialog box displays the device address and asks if you are sure you want to delete the device.

## Auto-Config New WAAS Devices

If you have numerous WAE devices, you can setup the NAM to configure newly discovered WAE devices using a pre-defined 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 auto-config:

**Step 1** Click **Setup > Data Sources**.

**Step 2** From the contents menu, choose **WAAS -- Devices**.

The WAAS Device table displays. [Figure 3-9](#) shows an example of the WAAS Custom Data Source table.

**Step 3** Click **Auto-Config**.

The Auto-Config Setting window displays. [Figure 3-12](#) shows an example of the WAAS Device Auto Config Setting window.

**Figure 3-12** WAAS Device Auto Config Setting Window

**Step 4** Click the Enable Auto Config check box and specify the configuration to be applied to newly discovered WAE devices. See [Configuring WAAS Data Sources, page 3-38](#), for more information.



### Note

After a WAAS device is auto configured, you can manually override its auto-configuration by selecting the device and click Config to reconfigure the device.

## Managing a WAAS Monitored Server

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 3-42](#)
- [Deleting a WAAS Monitored Server, page 3-43](#)

## Adding a WAAS Monitored Server

To add a WAAS monitored server:

**Step 1** Click **Setup > Data Sources**.

**Step 2** From the contents menu, choose **WAAS > Monitored Servers**.

The WAAS Monitored Servers table displays. [Figure 3-13](#) shows an example of the WAAS Monitored Servers table.

**Figure 3-13** WAAS Monitored Servers Table

| Monitored Server Filters                                                             |                                                                |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <input type="checkbox"/>                                                             | Filter Response Time for all Data Sources by Monitored Servers |
| <input type="checkbox"/>                                                             | Select All                                                     |
| <input type="checkbox"/>                                                             | 10.54.10.1                                                     |
| <input type="checkbox"/>                                                             | 10.54.10.2                                                     |
| <input type="checkbox"/>                                                             | 10.54.10.3                                                     |
| <input type="checkbox"/>                                                             | 10.54.10.4                                                     |
| <input type="checkbox"/>                                                             | 10.54.10.5                                                     |
| Select a server then take an action --> <button>Add</button> <button>Delete</button> |                                                                |

Click the Filter Response Time for all Data Sources by Monitored Servers checkbox 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 New Device dialog box displays.

**Step 4** Enter the server IP address in the Server Address field.



**Step 5** Click **Submit**.

---

## Deleting a WAAS Monitored Server

To delete a WAAS monitored server data source:

---

**Step 1** Click **Setup > Data Sources**.

**Step 2** From the contents menu, choose **WAAS > Monitored Servers**.

The WAAS Monitored Servers table displays any WAAS monitored servers.

**Step 3** 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 4** Click **OK** to delete the WAAS monitored server.

---

## Setting Up a WAAS Analysis Report

NAM provides WAAS custom reports to help users to analyze and evaluate the impact of WAAS optimization. These reports are helpful during WAAS Proof of Concept evaluation and WAAS deployment planning. This window sets up necessary data sources and data collections and custom reports for WAAS before-after analysis.

After setting up the WAAS analysis report, NAM 4.1 will do the following configurations as necessary:

- Configure branch WAE to export Client and Passthrough flows to the NAM.
- Configure core WAE to export Server flows to the NAM.
- Configure either branch WAE or Core WAE to export WAN flows to the NAM, depending on the NAM location.
- Configure branch and core WAEs to monitor the selected Server.
- Configure NAM data sources and associated response time collections for the WAE flows mentioned above
- Create Before-After Analysis custom reports for the selected client, server, and application.

Before attempting to set up the WAAS analysis report, ensure that the NAM GUI lists the WAE devices in your network and that you have configured the list of monitored servers (using **Setup > Data Sources > WAAS -- Monitored Servers** window).

To set up a WAAS analysis report:

**Step 1** Click **Setup > Data Sources**.

**Step 2** From the contents menu, click **WAAS -- Analysis**.

The Setup WAAS Analysis Report window displays as shown in [Figure 3-14](#).

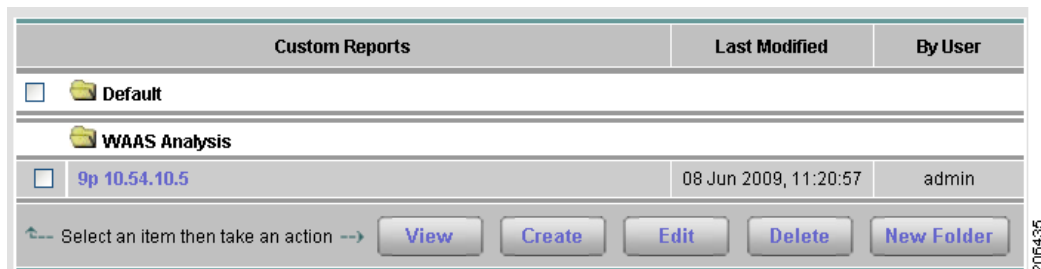
**Figure 3-14 Setup WAAS Analysis Window**

**Step 3** Choose a Branch WAE from the Select Branch WAE pull-down menu.

If no WAE devices listed, use WAE CLI command **flow monitor** to enable flow exports to the NAM.

- Step 4** Optionally, choose a Core (Data Center) WAE from the Select Core (Data Center) WAE pull-down menu.
- The NAM is Located Near field is enabled if you choose a Core WAE.
- Step 5** If you chose to enter a Core WAE, click a checkbox to indicate whether the NAM location is at the Branch WAE or the Core WAE.
- Step 6** Choose an application to analyze using the Application to Analyze field's pull-down menu.
- Step 7** Choose a server using the Specify Server pull-down menu.
- The servers listed are those monitored servers you should have configured using the **Setup > Data Sources > WAAS -- Monitored Servers** window.
- Step 8** Optionally, enter the IP address of a client.
- You will need to provide client IP address if you want to create a custom report like an Application-Server-Client report.
- Step 9** Click **Setup Analysis Report**.
- After you click **Setup Analysis Report**, the NAM creates the data sources required for these reports if the data sources have not already been configured. The NAM creates the reports and displays the Custom Reports window, as shown in [Figure 3-15](#). Under the **WAAS Analysis** folder, the NAM creates the following report types:
- Average Transaction Time of WAE-Client
  - Average Transaction Time of WAE-Passthrough data sources
  - Server Bytes on WAE-Passthrough
  - Server Bytes of WAE-Client
  - Server Bytes of WAE-ClientWAN or WAE-serverWAN
  - Server Bytes of WAE-Server data sources

**Figure 3-15 Custom Reports Window**



The custom reports window shows six reports created if a Core WAE was chosen. Under the **WAAS Analysis** folder, the NAM creates the following report types:

- Average Transaction Time of WAE-Client data sources
- Average Transaction Time of WAE-Passthrough data sources
- Server Bytes on WAE-Passthrough
- Server Bytes of WAE-Client
- Server Bytes of WAE-ClientWAN or WAE-serverWAN

If core WAE was chosen and the NAM location is branch, the WAE-clientWAN data source report is created among six reports. If core WAE was chosen and the NAM location is core, the WAE-serverWAN data source report is created among six reports.

- Server Bytes of WAE-Server data sources

If a Core WAE was not chosen, the Server Bytes of WAE-Server data sources report will not be created.

The NAM groups all the reports under one custom report of the type of either App-Server or App-Server-Client.

## MPLS Data Sources

When data packets containing MPLS labels are spanned to the NAM, the traffic can be monitored by the tag inside the data packets. This feature is especially useful in a network that deploys MPLS/VPN where traffic from each VPN can be uniquely identified by a combination of MPLS labels. When the NAM encounters stacked MPLS labels, only the relevant inner-most label (the bottom tag in the label stack) is used for monitoring.

To enable RMON monitoring for MPLS, you must first configure an MPLS data source. To enable MPLS traffic monitoring, you must create a form of virtual interface that can be tied to a particular MPLS tag. After setting up the custom MPLS data source, you can enable monitoring of the following:

- Applications per MPLS tag
- Hosts per MPLS tag
- Host conversation per MPLS tag

This section contains the following topics:

- [Automatic Discovery of MPLS VPN Labels, page 3-47](#)
- [Setting Up Layer 3 VRF Data Sources, page 3-48](#)
- [Setting Up Layer 2 Virtual Circuit Data Sources, page 3-49](#)
- [Setting Up MPLS Label Data Sources, page 3-50](#)
- [Creating a VRF/VC Configuration File, page 3-51](#)
- [Importing a VRF/VC Configuration File, page 3-51](#)
- [Exporting a VRF/VC Configuration File, page 3-52](#)
- [Importing Log, page 3-52](#)

### Automatic Discovery of MPLS VPN Labels

In an MPLS VPN environment, the NAM can monitor traffic using either VPN routing/forwarding (VRF) table name or virtual circuit (VC) ID configured at the switch. This higher level of abstraction hides the underlying label associations.

The VRF and VC information can only be obtained from the switch CLI. This requires you to provide the switch login credentials, username and password, and whether to access the switch CLI through **telnet** or **ssh**. Enable mode password is not required.

After the VRF, VC, and the associated labels are discovered, you can reference the VRF or VC using either the VRF name or VC ID directly without any knowledge of the underlying labels using the NAM monitoring functions.

The labels associated with each VRF or VC are allocated dynamically by the switch. As a result, the labels will not be persistent when the switch is rebooted or a supervisor switch-over occurred. The NAM will have to re-discover VRF and VC information from the switch under these situations. A manual refresh feature is also provided for on-demand refresh.

## Setting Up Layer 3 VRF Data Sources

To set up layer 3 VPN routing/forwarding (VRF) table (L3 VRF) data sources:

**Step 1** Click **Setup > Data Sources**.

The Active SPAN Sessions table displays.

**Step 2** In the contents, click **L3 VRF**.

The MPLS VRF Data Source Configuration window displays shown in [Figure 3-16](#).

**Figure 3-16 MPLS VRF Data Source Configuration Window**

|                       | VRF Name | Local Label | Egress Label     | Data Source   |
|-----------------------|----------|-------------|------------------|---------------|
| <input type="radio"/> | site1    | 344         | 34/549<br>23/18  | VRF:site1     |
| <input type="radio"/> | site10   | 353         | 34/534<br>23/27  | VRF:site10    |
| <input type="radio"/> | site100  | 443         | 34/584<br>34/640 | Not monitored |
| <input type="radio"/> | site101  | 444         | 34/585<br>34/641 | Not monitored |
| <input type="radio"/> | site102  | 445         | 34/586<br>34/642 | Not monitored |
| <input type="radio"/> | site103  | 446         | 34/587<br>34/643 | Not monitored |
| <input type="radio"/> | site104  | 447         | 34/588<br>34/644 | Not monitored |
| <input type="radio"/> | site105  | 448         | 34/589<br>34/645 | Not monitored |

**Step 3** If VRF information is not displayed or if some VRF information is missing, click **Import from Router** to refresh the list.

If the list is still empty after clicking **Import from Router**, the NAM failed to automatically import VRF configuration from the router. In this case, perform Step 4. If the VRF information is available, proceed to Step 5.

If the NAM failed to automatically import VRF configuration from the router, click **Import Log**. The MPLS Import log contains information that might help you diagnose the problem in the connection. See [Importing Log, page 3-52](#), for more information about the Import Log.

**Step 4** If necessary, create a text file containing the VRF information and click **Import from File**.

After clicking **Import from File**, the Import VRF/VC Configuration window displays enabling you to specify the location from which to import the VRF/VC configuration file. The VRF/VC configuration file might be on your local machine or at a remote URL.

See [Creating a VRF/VC Configuration File, page 3-51](#), for information about how to create the text VRF/VC configuration file.

**Step 5** Choose any VRF data source, then click **Create DataSrc**.

Creating or deleting a NAM data source does not affect the switch configuration.

## Setting Up Layer 2 Virtual Circuit Data Sources

To set up layer 2 (L2) virtual circuit data sources:

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

The Active SPAN Sessions table displays.

**Step 2** In the contents, click **L2 Virtual Circuit**.

The MPLS Virtual Circuit Data Source Configuration window displays shown in [Figure 3-17](#).

**Figure 3-17 MPLS Virtual Circuit Data Source Configuration Window**

|                       | VC ID | Local Label | Egress Label | Data Source   |
|-----------------------|-------|-------------|--------------|---------------|
| <input type="radio"/> | 30    | 318         | 0            | Not monitored |
| <input type="radio"/> | 2000  | 317         | 34/23        | Not monitored |
| <input type="radio"/> | 2001  | 17          | 34/24        | Not monitored |
| <input type="radio"/> | 2002  | 18          | 34/25        | Not monitored |
| <input type="radio"/> | 2003  | 19          | 34/26        | Not monitored |
| <input type="radio"/> | 2004  | 20          | 34/27        | Not monitored |
| <input type="radio"/> | 2005  | 21          | 34/28        | Not monitored |
| <input type="radio"/> | 2006  | 22          | 34/29        | Not monitored |

**Step 3** If VC information is not displayed or if some VC information is missing, click **Import from Router** to refresh the list.

If the list is still empty after clicking **Import from Router**, the NAM failed to automatically import VC configuration from the router. In this case, perform Step 4. If the VRF information is available, proceed to Step 5.

If the NAM failed to automatically import VC configuration from the router, click **Import Log**. The MPLS Import log contains information that might help you diagnose the problem in the connection. See [Importing Log, page 3-52](#), for more information about the Import Log.

**Step 4** If necessary, create a text file containing the VC information and click **Import from File**.

After clicking **Import from File**, the Import VRF/VC Configuration window displays enabling you to specify the location from which to import the VRF/VC configuration file. The VRF/VC configuration file might be on your local machine or at a remote URL.

See [Creating a VRF/VC Configuration File, page 3-51](#), for information about how to create the text VRF/VC configuration file.

**Step 5** Choose any VC data source, then click **Create DataSrc**.

Creating or deleting a NAM data source does not affect the switch configuration.

## Setting Up MPLS Label Data Sources

To set up MPLS Label data sources:

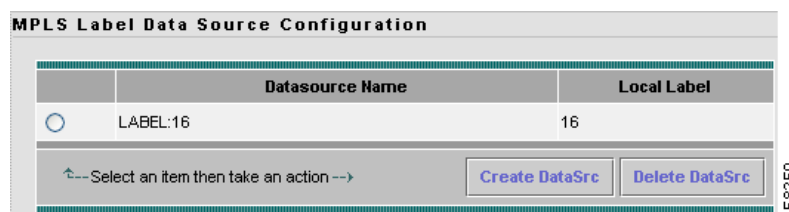
**Step 1** Choose **Setup > Data Sources**.

The Active SPAN Sessions table displays.

**Step 2** In the contents, click **Label**.

The MPLS Label Data Source Configuration window displays shown in [Figure 3-18](#).

**Figure 3-18 MPLS Label Data Source Configuration Window**



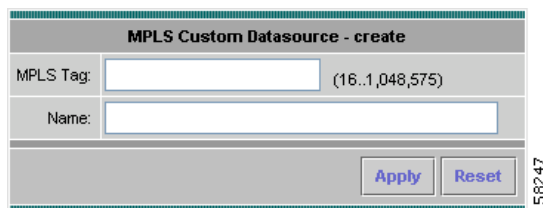
**Step 3** Click **Create DataSrc**.

A dialog box asks you to select a VRF or VC first.

**Step 4** Click **OK**.

The Create MPLS Custom Datasource window displays as shown in [Figure 3-19](#).

**Figure 3-19 Create MPLS Custom Datasource Window**



**Step 5** Enter an MPLS tag number in the **MPLS Tag** field.

The tag number must match the value in the packets, as only those will be represented in the data-source. You need to know the tag number from the router configuration. The NAM will assign a name based on the MPLS tag number you provide.

**Step 6** Accept the name the NAM assigns based on the MPLS tag number, or enter a name you prefer in the Name field.

You can use the name field to identify the MPLS tag value, the VRF tunnel name, or something else (such as VPN-San\_Jose-RTP).

**Step 7** Click **Apply**.



## Creating a VRF/VC Configuration File

The VRF/VC configuration file contains text information about the VRFs and VCs configured at the router. Each configuration line contains four fields separated by a space. [Table 3-19](#) describes the format of a configuration line.

**Table 3-19** VRF/VC Configuration Lines

| Field        | Description                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comment line | Begins with the # character                                                                                                                                                              |
| Type         | VRF or VC                                                                                                                                                                                |
| Name         | Name of the VRF or VC ID                                                                                                                                                                 |
| Local label  | The local label for the VRF or VC                                                                                                                                                        |
| Egress label | The out going label stack with the format outer label/inner label. If there is more than one label, each label stack is separated by a comma with <i>no spaces</i> between stack labels. |

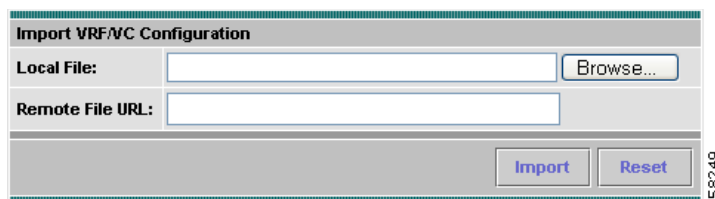
The following is an example of the VRF/VC configuration file:

```
MPLS configuration file
Autogenerated at 2006-04-26 19:43
VRF customer_A 114 0
VRF customer_B 600 204/500,204/308
VC 201 111 204/309
VC 202 120 204/310
VC 203 121 204/311
VC 204 122 204/312
VC 205 123 204/313
VC 206 124 204/314
VC 207 125 204/315
VC 208 126 204/319
VC 209 127 204/317
VC 210 128 204/318
```

## Importing a VRF/VC Configuration File

If you have a text file that contains the known VRF/VC configuration, you can import the configuration by clicking **Import from File**. You might have created this file by using the **Export to File** button. [Figure 3-20](#) shows the Importing VRF/VC Configuration File window.

Click **Browse** to locate the configuration file you want to import, or enter the URL of a remote file, then click **Import**.

**Figure 3-20 Importing VRF/VC Configuration File Window**

## Exporting a VRF/VC Configuration File

After you have the desired MPLS configuration on the NAM, you can export the configuration to a file to serve as a backup. Creating a backup file enables you reload the configuration if the configuration is lost or if you want to revert to an earlier configuration. Click **Export to File** to export your MPLS VRF/VC datasource configuration.

## Importing Log

After you import the VRF/VC data source configuration from the router or VRF/VC datasource configuration file, you can view the log of the MPLS import by clicking **Import Log**. The MPLS Import log contains a listing of occurrences in the connection and can be useful in troubleshooting. The log might show an invalid user name or password, no connection to the switch, command-line parsing errors, or other problems that might have occurred. An MPLS import log should contain the message: *VRF/VC update successful*.

## 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.

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

- [Sending ERSPAN Data to Layer 3 Interface, page 3-52](#)
- [Sending ERSPAN Data Directly to the NAM Management Interface, page 3-53](#)

## 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

Because this method does not affect NAM performance or accessibility, Cisco recommends this method.

### Sample Configuration of ERSPAN Source

```
monitor session 1 type erspan-source
no shut
```

```

source interface Fa 3/47
destination
 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, the ERSPAN data source should appear on the NAM GUI and can then be selected to analyze the ERSPAN traffic.



#### Note

This method affects NAM performance and accessibility.

#### 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

# Monitoring

Before you can monitor data, you must set up the data collections in the Monitor option of the Setup tab. For information on data collections, see the [“Overview of Data Collection and Data Sources” section on page 4-2](#). There are options to set up the following:

- [Monitoring Core Data, page 3-54](#)
- [Monitoring Voice Data, page 3-57](#)
- [Monitoring RTP Stream Traffic, page 3-58](#)
- [Monitoring Response Time Data, page 3-60](#)
- [Monitoring DiffServ Data, page 3-64](#)
- [Setting Up the DiffServ Profile, page 3-65](#)
- [Monitoring URL Collection Data, page 3-67](#)

## Monitoring Core Data

You can enable or disable individual core data collections on each available data source. The following core collections are available:

- Application Statistics—Enables the monitoring of application protocols observed on the data source.
- Host Statistics (Network and Application layers)—Enables the monitoring of network-layer host activity.
- Host Statistics (MAC layer)—Enables the monitoring of MAC-layer hosts activity. Also enables monitoring of broadcast and multicast counts for host detail windows.
- Conversation Statistics (Network and Application layers)—Enables the monitoring of pairs of network-layer hosts that are exchanging packets.
- Conversation Statistics (MAC layer)—Enables the monitoring of pairs of MAC-layer hosts that are exchanging packets.
- VLAN Traffic Statistics—Enables the monitoring of traffic distribution on different VLANs for the data source.
- VLAN Priority (CoS) Statistics—Enables the monitoring of traffic distribution using different values of the 802.1p priority field.
- Network-to-MAC Address Correlation—Enables the monitoring of MAC-level statistics which are shown in host detail windows. Without this collection, a MAC station cannot be associated with a particular network host.
- TCP/UDP Port Table—Enables the monitoring of server ports on a particular data source such as a VLAN, a physical port on the NAM, or a set of NDE flow records sent to the NAM.
- Switch engine module (Supervisor) records received by the NAM. You can select any combination of Port statistics, VLAN statistics, and NBAR statistics.
- Router engine module records (Router) received by the NAM. You can select any combination of Interface statistics and NBAR statistics.

**Note**

---

MAC and VLAN collections are not available on NME-NAM devices.

---

**Note**

For better overall system performance, enable only the collections you want to monitor.

**Note**

You must disable all reports for the collections you want to turn off. If you turn off collections that have reports running on them, the collections will automatically be turned on except for voice reports. For more information on disabling reports, see the [“Disabling Reports”](#) section on page 5-25.

To set up core monitoring functions:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions Dialog Box ([Figure 3-21](#)) displays.

**Figure 3-21 Core Monitoring Functions Dialog Box**

| Monitoring Function                                                                        | Max Entries    |
|--------------------------------------------------------------------------------------------|----------------|
| <input checked="" type="checkbox"/> Application Statistics                                 | Not applicable |
| <input checked="" type="checkbox"/> Host Statistics (Network & Application layers)         | 100            |
| <input checked="" type="checkbox"/> Host Statistics (MAC layer)                            | Not applicable |
| <input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers) | 500            |
| <input checked="" type="checkbox"/> Conversation Statistics (MAC layer)                    | Not applicable |
| <input checked="" type="checkbox"/> VLAN Traffic Statistics                                | Not applicable |
| <input checked="" type="checkbox"/> VLAN Priority (CoS) Statistics                         | Not applicable |
| <input checked="" type="checkbox"/> Network-to-MAC Address Correlation                     | Not applicable |
| <input checked="" type="checkbox"/> TCP/UDP Port Table                                     | Not applicable |

↑--- Check desired functions then Apply ---> Apply Reset

**Step 2** Select the collection data source from the Data Source drop-down menu.

To turn on core monitoring for the router, select Router from the Data Source drop-down menu. For routers, the following Data Sources are available:

- Internal
- External
- NETFLOW
- Router

To turn on core monitoring data for the switch or managed device, choose Supervisor from the drop-down menu. For switches and appliances, the following Data Sources are available:

- ALL SPAN
- VLANs
- NETFLOW
- NDE
- Supervisor

You can enter a partial name of a data source and click **Filter** to find data sources that match. Click **Clear** to return to the entire list of data sources.

**Step 3** Select the check boxes to enable any combination of the following specific core monitoring functions:

- Application Statistics
- Host Statistics (Network and Application layers)
- Host Statistics (MAC layer)
- Conversation Statistics ((Network and Application layers)
- Conversation Statistics (MAC layer)
- VLAN Traffic Statistics
- VLAN Priority (CoS) Statistics
- Network-to-MAC Address Correlation
- TCP/UDP Port Table

**Step 4** Select the maximum number of entries from the Max Entries lists.

**Step 5** Click **Apply** to save your changes, or click **Reset** to cancel.

## Enabling Mini-RMON Collection



### Note

This section does not apply to NME-NAM devices.

Enabling Mini-RMON on the switch Supervisor allows you to monitor port statistics data from each switch port. You must enable Mini-RMON in privileged mode from the CLI. To enable Mini-RMON, do one of the following:

#### For Switches Running Catalyst OS

Enter the **set snmp rmon enable** command.

#### For Switches Running Cisco IOS Software

You must enable Mini-RMON on each individual interface.

Enter the following commands:

```
Supervisor name(config) # interface interface-name
Supervisor name(config-if) # rmon collection stats collection-control-index owner monitor
Supervisor name(config-if) # end
```

where:

- The interface-name is the name of the interface on which you are enabling Mini-RMON.
- The collection-control-index is any arbitrary number that has not yet been used.

## Monitoring Voice Data

After you setup the NAM to monitor voice data, use the Monitor tab to view the collected voice data. For more information on viewing the voice data, see [Viewing Voice and Video Data](#), page 4-23.


**Note**

Voice monitoring features are supported with Cisco IP telephony devices only.

To set up voice monitoring:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

**Step 2** In the contents, click **Voice Monitoring**.

The [Voice Monitor Setup Window](#) (Table 3-20) displays. [Figure 3-22](#) shows an example of the [Voice Monitoring Setup Window](#).

**Figure 3-22 Voice Monitoring Setup Window**

**Step 3** Check the Enabled check box.

**Step 4** Accept the default MOS Score value range or modify the values as you prefer.

**Table 3-20 Voice Monitor Setup Window**

| Field                   | Description                                                                                                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Voice Monitoring</b> |                                                                                                                                       |
| Enabled                 | Enables voice monitoring                                                                                                              |
| Max Active Calls        | Maximum number of active calls to monitor                                                                                             |
| Max Known Phones        | Maximum number of phones to monitor                                                                                                   |
| Max Worst Call          | Maximum number of worst calls to monitor. Up to 40; this is due to the number of alarm threshold crossed and the alarms they generate |
| Max History Calls       | Maximum number of calls to store in the call archive                                                                                  |

**Table 3-20 Voice Monitor Setup Window**

| Field             | Description                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>MOS Values</b> |                                                                                                                    |
| Excellent         | Highest quality MOS score (5.0 being highest). The default value is 5.00.                                          |
| Good              | Quality less than excellent; MOS score ranges from this setting to less than excellent. The default value is 4.33. |
| Fair              | Quality less than good; MOS score ranges from this setting to less than good. The default value is 4.02.           |
| Poor              | Quality less than excellent; MOS score ranges from this setting to less than fair. The default value is 3.59.      |

Table 3-21, [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 3-21 Maximum and Default Voice/Video and RTP Stream Parameters per Platform**

| Field            | 2220 Appliance  | 2204 Appliance | NAM-2(x)      | NAM-1(x)      | NME-NAM   |
|------------------|-----------------|----------------|---------------|---------------|-----------|
| RTP Streams      | 4,000 (2000)    | 1,500 (750)    | 800 (400)     | 400 (200)     | 100 (50)  |
| Max Active Calls | 2,000 (1,000)   | 750 (375)      | 400 (200)     | 200 (100)     | 50 (25)   |
| Known Phones     | 10,000 (5,000)  | 3,500 (1,750)  | 2,000 (1,000) | 1,000 (500)   | 250 (125) |
| Phone History    | 25,000 (12,500) | 7,000 (3,500)  | 5,000 (2,500) | 2,500 (1,250) | 600 (300) |

**Note**

To report jitter and packet loss for the SCCP protocol, you must enable CDR on Cisco Unified CallManager. For more information on Cisco Unified CallManager, see the Cisco Unified CallManager documentation.

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)

**Step 5** Click **Apply** to save your changes, or click **Reset** to cancel and revert to the previous settings.

## Monitoring RTP Stream Traffic

The NAM enables you to identify and monitor all RTP stream traffic among all SPANed traffic without having to know the signalling traffic used in negotiating the RTP channels. When RTP Stream Monitoring is enabled, the NAM:

- Identifies all RTP streams among the SPANed traffic
- Monitors the identified RTP traffic
- Sends **syslog** alarm messages for RTP streams that violate the packet loss thresholds



By default, the NAM can monitor up to 30 concurrent RTP streams, but you can set up the NAM to monitor from 1 to 4,000 streams. See [Setting Up Voice/Video Stream Thresholds, page 3-88](#) for more information about how to set up NAM RTP Stream packet loss thresholds for the following:

- Number of Consecutive Packets Loss threshold

The valid threshold value is 1 to 10 inclusive. 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 ( $10^{-6}$ ) threshold

This value is accumulative per-million packet loss rate from 1 to 100 inclusive. Every time NAM detects a packet loss (sequence gap) event, the NAM calculates the per-million packet loss rate. If the computed per-million packet loss rate crosses this threshold, the NAM raises an alarm condition.

You can set up these thresholds at **Setup > Alarms > NAM RTP Stream 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. For example, a filter to set up the NAM to monitor RTP streams from the subnet 209.165.201.0 to host 1.1.1.1 would be:

```
source = 209.165.201.0
source mask = 255.255.255.0
destination = 1.1.1.1
destination mask = 255.255.255.255
```

To set up RTP Stream monitoring:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

**Step 2** In the contents, click **RTP Stream Monitoring**.

The RTP Stream Setup window displays with two distinct areas. [Figure 3-23](#) shows an example of the RTP Stream Monitoring Setup window.

**Figure 3-23 RTP Stream Monitoring Setup Window**

**RTP Stream Monitor Setup**

Enabled: ☒

Max RTP Streams: (1-4000): 4000

Report Interval: 60 seconds

Apply Reset

**Filter Table**

| Src Address           | Src Mask | Dst Address | Dst Mask |
|-----------------------|----------|-------------|----------|
| No filters configured |          |             |          |

Check desired functions then Apply Create Edit Delete

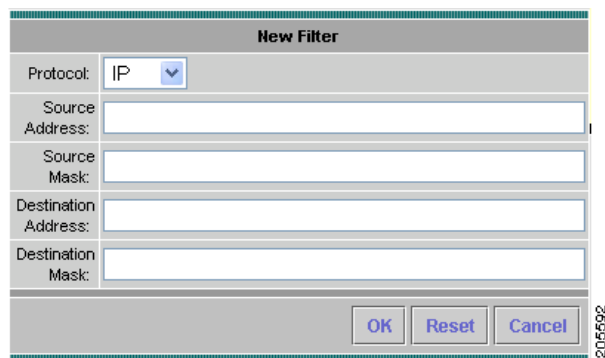
**Step 3** Click the Enabled check box to enable RTP stream monitoring.

**Step 4** Enter the maximum number of RTP streams to monitor (up to 4,000).

**Step 5** In the Filter Table area, click **Create** to enter filtering data.

The New Filter window (Figure 3-24) appears with fields for you to enter both the source and destination IP address and address mask for the RTP streams to monitor.

**Figure 3-24 Setup RTP Stream Monitoring New Filter Window**



**Step 6** Choose the protocol to monitor from the pull-down menu, IP or IPv6.

**Step 7** Enter the source and destination address information and click **OK**, or click **Cancel** to abort.  
Click **Reset** to clear all fields of the New Filter dialog box.

**Step 8** Click **Apply** to begin monitoring.

Click **Reset** to clear the values you might have modified to their previous set values.

## Monitoring Response Time Data

You can monitor response time to collect the response time between a client and a server. You can enable or disable response time monitoring on individual collection data sources. When you enable response time monitoring, the application supplies the default collection parameters.

The response time monitoring option is on by default; however to monitor response time data, you must enable response time monitoring in the NAM Traffic Analyzer application.

These topics help you set up and manage response time monitoring:

- [Setting Up Response Time Configuration, page 3-61](#)
- [Setting Up Response Time Data Monitoring, page 3-62](#)
- [Creating a Response Time Monitoring Collection, page 3-63](#)
- [Editing a Response Time Monitoring Collection, page 3-63](#)
- [Deleting Response Time Data Collections, page 3-64](#)

## Setting Up Response Time Configuration

To configure the timing parameters (or *buckets*) for response time data collections:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

**Step 2** In the contents, click **Response Time - Configuration**.

The Response Time Monitoring Setup, Collection Configuration window displays. See [Figure 3-25, Response Time Configuration Window](#). The settings you make on this window comprise the time distribution in milliseconds for the detailed Server Application Response Time data collection.

[Table 3-22](#) lists the time settings for the Response Time Configuration window.



**Note** These settings apply globally for all ART collections, including those you create using SNMP. The method you use last overrides previous settings. So if you change the settings using the GUI, those settings will override the settings made using SNMP, and vice versa.

**Figure 3-25 Response Time Configuration Window**

**Table 3-22 Response Time Configuration Window**

| Field                 | Description                                     | Usage Notes                                         |
|-----------------------|-------------------------------------------------|-----------------------------------------------------|
| Report Interval (sec) | Number of seconds between reports               | Enter a number in seconds. The default is 300.      |
| RspTime1 (msec)       | Upper response time limit for the first bucket  | Enter a number in milliseconds. The default is 5.   |
| RspTime2 (msec)       | Upper response time limit for the second bucket | Enter a number in milliseconds. The default is 10.  |
| RspTime3 (msec)       | Upper response time limit for the third bucket  | Enter a number in milliseconds. The default is 50.  |
| RspTime4 (msec)       | Upper response time limit for the fourth bucket | Enter a number in milliseconds. The default is 100. |

**Table 3-22**      *Response Time Configuration Window (continued)*

| Field             | Description                                                                       | Usage Notes                                          |
|-------------------|-----------------------------------------------------------------------------------|------------------------------------------------------|
| RspTime5 (msec)   | Upper response time limit for the fifth bucket                                    | Enter a number in milliseconds. The default is 200.  |
| RspTime6 (msec)   | Upper response time limit for the sixth bucket                                    | Enter a number in milliseconds. The default is 500.  |
| RspTimeMax (msec) | The maximum interval that the NAM waits for a server response to a client request | Enter a number in milliseconds. The default is 1000. |

- Step 3

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.

### Setting Up Response Time Data Monitoring

To configure response time monitoring:

- Step 1

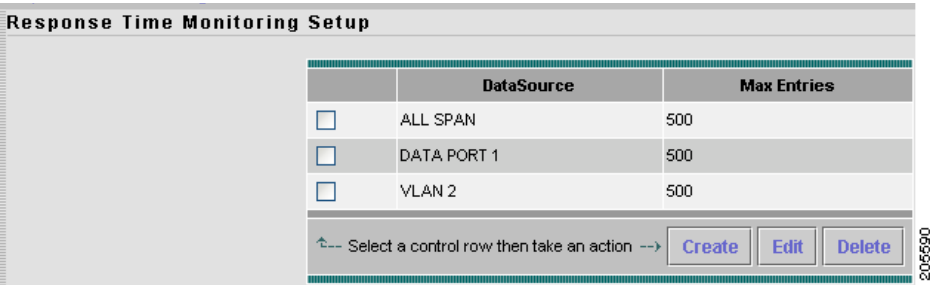
Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.
- Step 2

In the contents, click **Response Time - Monitoring**.

The Response Time Monitoring Setup table displays any data sources you might have already set up for response time monitoring as shown in [Figure 3-26, Response Time Monitoring Setup](#).

**Figure 3-26**      *Response Time Monitoring Setup*



Click **Create** to add another data source for which you want to monitor response time data. Check a data source and click **Edit** to modify the data source. Check a data source and click **Delete** to remove the data source.

## Creating a Response Time Monitoring Collection

To create a response time monitoring collection:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

**Step 2** In the contents, click **Response Time - Monitoring**.

The Response Time Monitoring Setup table displays any data sources you might have already set up for response time monitoring as shown in [Figure 3-26, Response Time Monitoring Setup](#).

**Step 3** Click **Create**.

The Response Time Monitoring Setup, Collection Configuration window displays as shown in [Figure 3-27](#).

**Figure 3-27** *Response Time Monitoring Setup, Collection Configuration*

**Step 4** Choose a data source from the drop-down menu, or enter a partial name in the empty field and click **Filter** to locate a specific data source from its partial name.

NAM 4.1 will build a table of response time data based on the number of entries you specify in Max. Table Entries and the timings you configured in [Setting Up Response Time Configuration, page 3-61](#).

**Step 5** Modify the number of table entries, or accept the default of 500 table entries and click **Submit**.

The new data source is listed as a Data Source when the Response Time Monitoring Setup window displays.

## Editing a Response Time Monitoring Collection

To edit a response time monitoring collection:

**Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

**Step 2** In the contents, click **Response Time - Monitoring**.

The Response Time Monitoring Setup table displays any data sources you might have already set up for response time monitoring as shown in [Figure 3-26, Response Time Monitoring Setup](#).

**Step 3** Check the data source you want to modify and click **Edit**.

The Response Time Monitoring Setup, Collection Configuration window displays as shown in [Figure 3-27](#).

- Step 4** Make the changes you want to the data source collection, then click **Submit**.

The modified data source displays as a Data Source when the Response Time Monitoring Setup window displays.

## Deleting Response Time Data Collections

To delete one or more response time data collections:

- Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

- Step 2** In the contents, click **Response Time - Monitoring**.

The Response Time Monitoring Setup table displays any data sources you might have already set up for response time monitoring.

- Step 3** Check one or more of the data source collections listed, then click **Delete**.

## Monitoring DiffServ Data

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

To monitor DiffServ data, 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 the [“Creating a DiffServ Profile” section on page 3-65](#).

To set up monitoring of differentiated services:

- Step 1** Choose **Setup > Monitor**.

The Core Monitoring Functions table displays.

- Step 2** In the contents under DiffServ, click **Monitoring**.

The DiffServ Monitor Setup Dialog Box ([Table 3-23](#)) displays.

You can enter a partial name of a data source and click **Filter** to find data sources that match. Click **Clear** to return to the entire list of data sources.

- Step 3** Select the appropriate information.

**Table 3-23** *DiffServ Monitor Setup Dialog Box*

| Element               | Description                                         | Usage Notes                                             |
|-----------------------|-----------------------------------------------------|---------------------------------------------------------|
| Data Source List      | Lists the data sources available.                   | Select the data source from the list.                   |
| DiffServ Profile List | Lists the user defined DiffServ profiles available. | Select the user-defined DiffServ profile from the list. |
| Traffic Statistics    | Shows basic DSCP traffic distribution.              | Select to enable or deselect to disable.                |

**Table 3-23** DiffServ Monitor Setup Dialog Box (continued)

| Element                | Description                                              | Usage Notes                                                                                              |
|------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Application Statistics | Shows DSCP traffic distribution by application protocol. | Select to enable or deselect to disable. Select the maximum number of entries from the Max Entries list. |
| IP Host Statistics     | Shows DSCP traffic distribution by host.                 | Select to enable or deselect to disable. Select the maximum number of entries from the Max Entries list. |

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

## Setting Up the DiffServ Profile

A DiffServ profile is a set of aggregation groups that can be monitored as a whole. After you create the proper profile(s), you can enable DiffServ collection. For more information on setting up DiffServ collections, see the “[Monitoring DiffServ Data](#)” section on page 3-64.

These topics help you set up and manage the DiffServ profile:

- [Creating a DiffServ Profile, page 3-65](#)
- [Editing a DiffServ Profile, page 3-66](#)
- [Deleting a DiffServ Profile, page 3-66](#)

## Creating a DiffServ Profile

To create a DiffServ profile:

- 
- Step 1** Choose **Setup > Monitor**.
- The Core Monitoring Functions table displays.
- Step 2** In the contents under DiffServ, click **Profile**.
- The DiffServ Monitor Profile Dialog Box displays.
- Step 3** Click **Create**.
- The DiffServ Profile Setup Dialog Box ([Table 3-24](#)) displays.
- Step 4** Select the appropriate information.

**Table 3-24** DiffServ Profile Setup Dialog Box

| Element               | Description                                               | Usage Notes                                                                     |
|-----------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------|
| Template List         | Templates for creating a differentiated services profile. | Select the template from the list. Select NONE if you are not using a template. |
| Profile Name text box | Name of the profile.                                      | Enter the name of the profile you are creating. The maximum is 64 characters.   |

Table 3-24 DiffServ Profile Setup Dialog Box (continued)

| Element                      | Description                                        | Usage Notes                                                                                |
|------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------|
| DSCP Value column            | DSCP numbers from 0 to 63.                         | —                                                                                          |
| Group Description text boxes | Name of the aggregation group for each DSCP value. | Enter the name of the aggregation group for each DSCP value. The maximum is 64 characters. |

Step 5 Click **Submit** to save your changes, or click **Reset** to cancel.

Editing a DiffServ Profile

To edit a DiffServ profile:

- Step 1 Choose **Setup > Monitor**.  
The Core Monitoring Functions table displays.
- Step 2 In the contents under DiffServ, click **Profile**.  
The DiffServ Monitor Profile Table displays.
- Step 3 Select the profile to edit, then click **Edit**.  
The DiffServ Profile Setup Dialog Box (Table 3-24) displays.
- Step 4 Make the necessary changes, then click **Submit** to save your changes, or click **Reset** to cancel.

Deleting a DiffServ Profile

To delete one or more DiffServ profiles, simply select the profiles from the DiffServ Monitor Profile table, then click **Delete**.



## Monitoring URL Collection Data

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. See [Creating a New Protocol, page 3-70](#), for more information about configuring a new protocol to use a specific port. 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 be configured to collect only some of the parts and ignore others.

This section contains the following sections:

- [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 > Monitor**.
- The Core Monitoring Functions table displays.
- Step 2** Click **URL Collection**.
- The URL Collection Configuration Dialog Box ([Figure 3-28](#)) displays.

**Figure 3-28 URL Collection Configuration Dialog Box**

- Step 3** Click the Enable check box to initiate URL Collection.
- The collection will not begin until you click **Apply**.
- Step 4** Provide the information described in the URL Collection Configuration Dialog Box ([Table 3-25](#)).

You can enter a partial name of a data source and click **Filter** to find data sources that match. Click **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.

**Table 3-25 URL Collection Configuration Dialog Box**

| Element     | Description                                               | Usage Notes                                                                                                                                        |
|-------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Datasource  | Identifies type of traffic incoming from the application. | Select one of the options from the drop down box.                                                                                                  |
| Max Entries | Maximum number of URLs to collect.                        | Select one of the following options from the drop down box: <ul style="list-style-type: none"> <li>• 100</li> <li>• 500</li> <li>• 1000</li> </ul> |
| Match only  | The application URL to match.                             | Optional parameter to limit collection of URLs that match the regular expression of this field.                                                    |

**Step 5** Click the Recycle Entries check box to recycle entries.

**Step 6** Click 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 7** Click **Apply** to save your changes, or click **Reset** to cancel.

## Changing a URL Collection

To change a URL collection:

**Step 1** Choose **Setup > Monitor**.

**Step 2** Select **URL Collection**.

The URL Collection Configuration Dialog Box ([Figure 3-29](#)) displays.

**Figure 3-29 URL Collection Configuration Dialog Box**

**Step 3** Change the information as described in the URL Collection Configuration Dialog Box ([Table 3-25](#)).

**Note**

Changing any parameters and applying the changes flushes the collected URLs and restarts the collection process.

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

## Disabling a URL Collection

To disable a URL collection:

- Step 1** Choose **Setup > Monitor**.
- Step 2** Click **URL Collection**.
- Step 3** Uncheck the Enabled check box.
- Step 4** Click **Apply**.

## Protocol Directory

The NAM contains a default set of protocols to be monitored. You can edit and delete protocols from the RMON2 protocol directory table on the NAM.

These topics enable you to manage the protocol directory:

- [Individual Applications, page 3-70](#)
- [Setting Up Application Groups, page 3-75](#)
- [Setting Up Autolearned Protocols, page 3-76](#)
- [Setting Up URL-Based Applications, page 3-77](#)

# Individual Applications

The Individual Applications window (Figure 3-30) lists protocols that have been set up for this NAM. To view the Individual Applications window, click **Setup > Protocol Directory > Individual Applications**. Use this window to view, add proprietary protocols, and to edit the settings for well-known protocols.

Figure 3-30 Protocol Directory Table

Individual Applications

Protocol Family: IP

Protocol

Filter

Clear

Showing 1-15 of 42 records

| #   | Protocol  | Master Port/Protocol | Port/Protocol | Port Range | AddrMap Stats | Host Stats | Conn Stats | RTT Stats |
|-----|-----------|----------------------|---------------|------------|---------------|------------|------------|-----------|
| 1.  | ah        | 51                   | 51            | 1          | n/a           | ✓          | ✓          | n/a       |
| 2.  | ax-25     | 93                   | 93            | 1          | n/a           | ✓          | ✓          | n/a       |
| 3.  | chaos     | 16                   | 16            | 1          | n/a           | ✓          | ✓          | n/a       |
| 4.  | egp       | 8                    | 8             | 1          | n/a           | ✓          | ✓          | n/a       |
| 5.  | gre       | 47                   | 47            | 1          | n/a           | ✓          | ✓          | n/a       |
| 6.  | icmp      | 1                    | 1             | 1          | n/a           | ✓          | ✓          | n/a       |
| 7.  | idpr      | 35                   | 35            | 1          | n/a           | ✓          | ✓          | n/a       |
| 8.  | idpr-cmtp | 38                   | 38            | 1          | n/a           | ✓          | ✓          | n/a       |
| 9.  | idrp      | 45                   | 45            | 1          | n/a           | ✓          | ✓          | n/a       |
| 10. | igmp      | 2                    | 2             | 1          | n/a           | ✓          | ✓          | n/a       |
| 11. | igrp      | 88                   | 88            | 1          | n/a           | ✓          | ✓          | n/a       |
| 12. | ipcomp    | 108                  | 108           | 1          | n/a           | ✓          | ✓          | n/a       |
| 13. | ipesp     | 50                   | 50            | 1          | n/a           | ✓          | ✓          | n/a       |
| 14. | ipip      | 94                   | 94            | 1          | n/a           | ✓          | ✓          | n/a       |
| 15. | ipip4     | 4                    | 4             | 1          | ✓             | ✓          | ✓          | n/a       |

Rows per page: 15

Go to page: 1 of 3

Go

Select a protocol then take an action

Create

Edit

Delete

This section provides the following sections:

- [Creating a New Protocol, page 3-70](#)
- [Editing a Protocol, page 3-72](#)
- [Deleting a Protocol, page 3-73](#)

## Creating a New Protocol

You can create additional protocol ports to enable the NAM to handle additional protocol traffic for standard protocols.

To create a new protocol:

- Step 1
- Choose **Setup > Protocol Directory**.
- The Protocol Directory Table (Figure 3-30) displays.

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

The New Protocol Parameters window (Figure 3-31) displays.

**Figure 3-31** New Protocol Parameters Window

Table 3-26 describes the fields of the New Protocol Parameters Dialog.

**Table 3-26** New Protocol Parameters Dialog

| Field                | Description                                                                                                                                                                                                                                                                                                              |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol Family      | Use the pull-down menu to choose a protocol: <ul style="list-style-type: none"> <li>IP</li> <li>TCP</li> <li>UDP</li> <li>STCP</li> </ul>                                                                                                                                                                                |
| Description          | Description of the protocol you create                                                                                                                                                                                                                                                                                   |
| Master Port/Protocol | Standard protocol port depending on the protocol family you choose                                                                                                                                                                                                                                                       |
| Port/Protocol        | Arbitrary port 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. <ul style="list-style-type: none"> <li>The range is 1-255 for IP</li> <li>The range is 1-65535 for TCP, UDP, and SCTP.</li> </ul> |
| Port Range           | Range of ports for the protocol you create                                                                                                                                                                                                                                                                               |
| Affected Stats       | <ul style="list-style-type: none"> <li>Address Map</li> <li>Host</li> <li>Conversations</li> <li>ART</li> </ul> <p><b>Note</b> You must choose a type of Affected Stats for the traffic type you want to monitor.</p>                                                                                                    |

- Step 3** Use the pull-down menu to choose a Protocol Family.  
Choose the protocol for the type of traffic you want to create the additional protocol to handle.
- Step 4** Enter a description of the protocol you create.
- Step 5** Use the pull-down menu to choose the master port for the type of traffic you want the new protocol to handle.  
  
If you select a Master Port/Protocol, this extends the master protocol to cover the port/protocol you assign as well. Traffic on the port/protocol you create is treated as though it were traffic on the Master Port/Protocol. In this case, you cannot edit the Description or Affected Stats.  
  
If you do not choose a Master Port/Protocol (None), the protocol you create is an independent protocol. You must still provide values for the Description and Affected Stats.
- Step 6** 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 7** Enter the number of ports you want to create to assign to the protocol you create.  
  
If you assign the new protocol to port 239, for example, and enter a range of four (4), the protocol you create will use ports 239, 240, 241, and 242 to handle traffic for the new protocol.
- Step 8** For Affected Stats, check the type of statistics for the traffic you want to monitor.
- Step 9** 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.

**Tip**

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

## Editing a Protocol

We recommend that you do not change any settings in the NAM protocol directory. Changing the default settings might cause unexpected behavior in SNMP-based management applications. However, advanced users might want to monitor proprietary protocols or alter the normal settings for well-known protocols.

To edit a protocol:

- Step 1** Choose **Setup > Protocol Directory**.  
The Protocol Directory table displays.
- Step 2** Select the protocol to edit, then click **Edit**.  
The [Edit Protocol Dialog Box](#) (Table 3-27) displays.
- Step 3** Make the necessary changes.

**Table 3-27 Edit Protocol Dialog Box**

| Field                  | Description                                                                                                                                                                | Usage Notes                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Name                   | The name of the protocol.                                                                                                                                                  |                                                                    |
| Currently displayed as | Protocol name as it appears in the Protocol Directory table.                                                                                                               |                                                                    |
| Port Range             | Port Range for this protocol                                                                                                                                               |                                                                    |
| Encapsulation          | Protocol encapsulation type.                                                                                                                                               |                                                                    |
| Affected Stats         | The statistics that can be collected for the protocol: <ul style="list-style-type: none"><li>• Address Map</li><li>• Hosts</li><li>• Conversations</li><li>• ART</li></ul> | A statistic is grayed out if it is not available for the protocol. |

**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**.

**Tip**

- You can display the Edit Protocol dialog box for a specific protocol by clicking on the protocol name in the Protocol Directory table.
- To view the full protocol name, move the cursor over the protocol name in the Protocol column of the Protocol Directory table.

## Deleting a Protocol

To delete a protocol, simply select it from the Protocol Directory table, then click **Delete**.

**Tip**

You can also delete a protocol from the Edit Protocol Directory dialog box. Select the protocol, then click **Delete**.

## Setting Up Encapsulation

Using Encapsulation Configuration gives you increased flexibility when trying to monitor (such as counting or grouping) different types of application traffic. Encapsulation Configuration enables you to configure how you want the NAM to handle IP tunnel encapsulations.

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

When set to IGNORE, the default mode, the NAM uses *application-based* counting. The encapsulation type is ignored, and the NAM counts all application traffic but ignores tunneled traffic. When you turn on Encapsulation Configuration for one or more protocols, you enable the NAM to count separately for *tunnel-based* counting in addition to application-based counting. When you turn off Encapsulation Configuration for one or more protocols, the NAM uses *tunnel-based* counting, and all traffic over the specified protocol is counted as the tunnel protocol. [Figure 3-32](#) shows the Encapsulation Configuration dialog box.

To configure encapsulation:

---

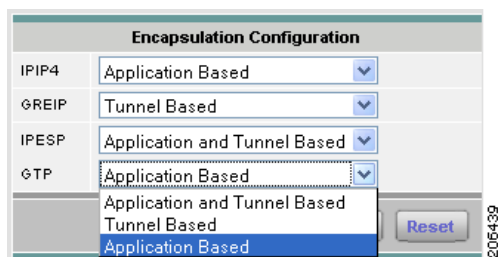
**Step 1** Choose **Setup > Protocol Directory**.

The Protocol Directory table appears.

**Step 2** Select **Encapsulations** from the Content menu.

The Individual Applications Encapsulation Configuration window displays.

**Figure 3-32** Encapsulation Configuration



**Step 3** Use the pull-down menu to choose the type of Encapsulation Configuration you want for each protocol.

- Application Based
- Tunnel Based
- Application and Tunnel Based

**Step 4** Click **Submit** to change the Encapsulation Configuration.

---

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



## Setting Up Application Groups

An application group is a set of application protocols that can be monitored as a whole. The following topics help you set up and manage the application group:

- [Creating an Application Group, page 3-75](#)
- [Editing an Application Group, page 3-75](#)
- [Deleting an Application Group, page 3-76](#)

### Creating an Application Group

To create an application group:

- 
- Step 1** Choose **Setup > Protocol Directory**.  
The Protocol Directory table displays.
- Step 2** Select **Application Groups** from the Content menu.
- Step 3** Click **Create**.  
The New Application Group Dialog Box ([Table 3-28](#)) displays.
- Step 4** Enter the *application group name*.
- Step 5** Select the appropriate information.

**Table 3-28**      **New Application Group Dialog Box**

| Element                | Description                       | Usage Notes                                                                                           |
|------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------|
| Application Group Name | Group Name                        | Enter the group name.                                                                                 |
| Encapsulation          | Encapsulation of the application. | Select the encapsulation from the drop down box.                                                      |
| Application Filter     | Options to filter or clear.       | Enter the name of the protocol you are filtering. The maximum is 64 characters.                       |
| Application            | List of applications              | Select an application and click <b>Add</b> .<br>Applications appear in the Selected Applications box. |

- 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 > Protocol Directory**.  
The Individual Applications window displays.

- Step 2

Select Application Groups from the Content menu.  
The Application Groups window displays.
- Step 3

Select the application group to edit, then click **Edit**.  
The Application Groups Edit window displays.
- Step 4

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

Deleting an Application Group

To delete one or more application groups, simply select the profiles from the Application Groups table, then click **Delete**.

Setting Up Autolearned Protocols

The Autolearned Protocols Preferences window allows you to configure the NAM to automatically learn application information. You can set the following preferences:

- Number of protocols to be learned (100 - 500)
- Number of TCP ports to be learned (0 - 65535)
- Number of UDP ports to be learned (0 - 65535)
- Range of TCP ports NOT to be learned (1 - 65535)
- Range of UDP ports NOT to be learned (1 - 65535)

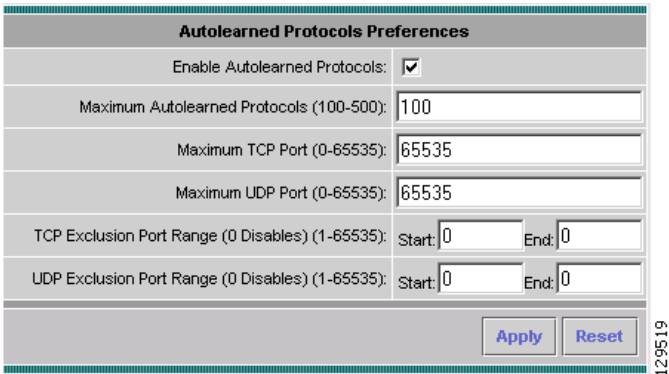
To set up Autolearned Protocol preferences:

- Step 1

Choose **Setup > Protocol Directory**.
- Step 2

Click **Autolearned Applications**.  
The Autolearned Protocols Preferences Dialog Box (Figure 3-33) displays.

Figure 3-33      Autolearned Protocols Preferences Dialog Box



- Step 3

Enter or change the information described in the Autolearned Protocols Preferences Dialog Box (Table 3-29).

**Table 3-29**      **Autolearned Protocols Preferences Dialog Box**

| Field                         | Description                                              | Usage Notes                                         |
|-------------------------------|----------------------------------------------------------|-----------------------------------------------------|
| Enable Autolearned Protocols  | Enables the Autolearned Protocols feature.               | Click checkbox to enable.                           |
| Maximum Autolearned Protocols | The maximum number of protocols that can be autolearned. | Enter a number from 100 to 500. The default is 100. |
| Maximum TCP Port              | The maximum number of TCP ports that can be autolearned. | Enter a number from 0 to 65535.                     |
| Maximum UDP Port              | The maximum number of UDP ports that can be autolearned. | Enter a number from 0 to 65535.                     |
| TCP Exclusion Port Range      | Specifies range of TCP ports to be excluded.             | Enter a number from 0 to 65535. (0 Disables)        |
| Start                         | Specifies start of TCP ports to be excluded.             |                                                     |
| End                           | Specifies end of TCP ports to be excluded.               |                                                     |
| UDP Exclusion Port Range:     | Specifies range of UDP ports to be excluded.             | Enter a number from 0 to 65535. (0 Disables)        |
| Start                         | Specifies start of UDP ports to be excluded.             |                                                     |
| End                           | Specifies start of UDP ports to be excluded.             |                                                     |

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

## Setting Up URL-Based Applications

URL-based applications are extensions to the protocol directory. When the URL in an HTTP request (a URL on TCP port 80) matches the criteria of a URL-based application, the traffic is classified as that protocol.

A URL-based application can be used the same way as any other protocol in the protocol directory. 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.

This section contains the following sections:

- [Creating a URL-Based Application](#)
- [Editing a URL-Based Application](#)
- [Deleting a URL-based Application](#)

## Creating a URL-Based Application

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.



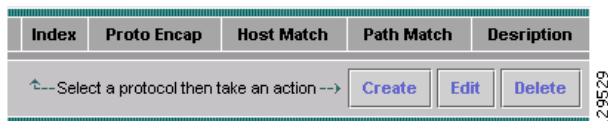
### Note

A maximum of 64 URL-based applications can be defined.

To set up URL-based applications:

- Step 1** Choose **Setup > Protocol Directory**.
- Step 2** Click **URL-Based Applications** in the TOC.  
The URL Matches Dialog Box ([Figure 3-34](#)) displays.

**Figure 3-34 URL Matches Dialog Box**



- Step 3** Click **Create**.  
The Create URL Match Entry Dialog Box ([Figure 3-35](#)) displays.

**Figure 3-35 Create URL Match Entry Dialog Box**

**Step 4** Enter the information described in the URL Match Entry Dialog Box (Table 3-30).

RFC 2895 specifies rules for creating a protocol name. In accordance with these rules, only the following characters are allowed:

- A through Z
- a through z
- 0 through 9
- dash (-)
- underbar (\_)
- asterisk (\*)
- plus (+)

**Note**

All other characters are changed to a dash (-).

**Table 3-30 URL Match Entry Dialog Box**

| Field                  | Description                                                                          | Usage Notes                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Index                  | URL Matches are executed in order of the Index                                       | Enter a number from 1 to 64. To change an index, the entry needs to be deleted and recreated with the new index value. |
| Encapsulation Protocol | The protocol that encapsulates the URL                                               | Select IPv4 or IPv6 from the drop down box.                                                                            |
| URL Host Part Match    | POSIX regular expression that the host part is matched against                       | For example: <b>domain.com</b> .                                                                                       |
| URL Path Part Match    | POSIX regular expression that the path and argument part of a URL is matched against | For example: <b>/intro?id</b> .                                                                                        |

**Table 3-30      URL Match Entry Dialog Box (continued)**

| Field                | Description                                                                                    | Usage Notes                                                    |
|----------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Content Type Match   | Content-Type in HTTP headers that identify the data type the message; also known as MIME types | For example: application/octet-stream, text/html, or image/gif |
| Protocol Description | Name of the URL based application                                                              | For example: <b>url-match-domain-com.</b>                      |

**Step 5**      Click **Apply** to save your changes, or click **Reset** to cancel.

Editing a URL-Based Application

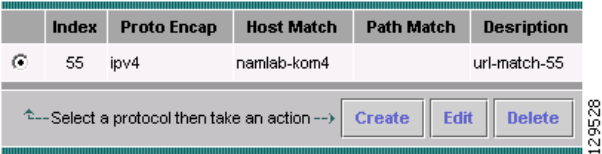
To edit URL-based applications:

- Step 1**      Choose **Setup > Protocol Directory**.

**Step 2**      Click **URL-Based Applications** in the TOC.

              The URL Matches Dialog Box ([Figure 3-36](#)) displays.

**Figure 3-36      URL Matches Dialog Box**



- Step 3**      Select a URL and click **Edit**.

              The Edit URL Match Entry Dialog Box ([Figure 3-37](#)) displays.



**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.

**Figure 3-37** Edit URL Match Entry Dialog Box

**Edit HTTP URL Match Entry**

Index: 55

Encapsulation Protocol:

URL Host Part Match:

URL Path Part Match:

Protocol Description:

Fill in values then Apply -->

Change the information as described in the URL Match Entry Dialog Box (Table 3-30).

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

## Deleting a URL-based Application

To delete a URL-based application:

**Step 1** Choose **Setup > Protocol Directory**.

**Step 2** Click **URL-Based Applications** in the TOC.

The URL Matches Dialog Box (Figure 3-38) displays.

**Figure 3-38** URL Matches Dialog Box

|                                  | Index | Proto Encap | Host Match | Path Match | Description          |
|----------------------------------|-------|-------------|------------|------------|----------------------|
| <input checked="" type="radio"/> | 55    | ipv4        | domain.com | /intro?id  | url-match-domain.com |

↑---Select a protocol then take an action-->

**Step 3** Choose a URL and click **Delete**.

## Setting Up Alarm Events and Thresholds

You can set up alarm thresholds by defining threshold conditions for the following monitored variables on the NAM:

- Response times
- Server-client response times
- DiffServ host statistics
- DiffServ traffic statistics

- DiffServ application statistics
- Voice protocols
- Mini-RMON MIB on the switch
- Network layer statistics
- MAC layer statistics
- Application statistics

**Note**

MAC layer and Mini-RMON statistics do not apply on NME-NAM devices.

These topics help you set up and manage alarm threshold settings:

- [Setting Up Alarm Events, page 3-82](#)
- [Setting Alarm Thresholds, page 3-84](#)
- [Setting Up Voice/Video Stream Thresholds, page 3-88](#)
- [Setting Up the NAM Syslog, page 3-90](#)
- [Setting Chassis or Managed Device Thresholds, page 3-90](#)
- [Setting NAM Trap Destinations, page 3-93](#)
- [Setting NAM Alarm Mail, page 3-94](#)

## Setting Up Alarm Events

Use this window to set up the alarm events, then use these events to set up the alarms you want to use. These events are also used for the Capture Trigger events. After creating events, go to the **Setup > Alarm Events** to see a list of the events you created. There you select which event you wish to be associated with that alarm. See [Setting Alarm Thresholds, page 3-84](#).

You do not need to set up logs and traps before you set up Alarm Event. Logs and traps are part of the event parameters and specify what the NAM should do after an alarm is triggered.

To create an alarm event:

---

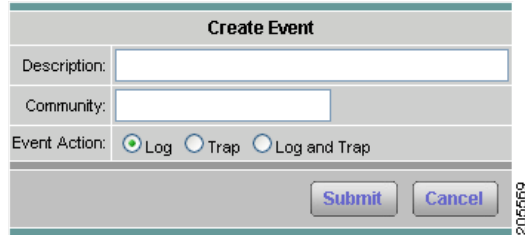
**Step 1** Choose **Setup > Alarms**.

The Alarm Events table displays any configured Alarm Events. An alarm event is listed by its Description, Community, and Type. The type can be one of Log, Trap, or Log and Trap. Each alarm event also contains a Last Sent and Status field. The Last Sent field is a timestamp indicating the date and time the last event occurred. The Status field indicates the current status of the event.

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

The Create Alarm Events Dialog displays, as shown in [Figure 3-39](#).



**Figure 3-39 Create Alarm Events Dialog**


The dialog box is titled "Create Event". It contains three input fields: "Description:" with a text box, "Community:" with a text box, and "Event Action:" with three radio buttons labeled "Log", "Trap", and "Log and Trap". The "Log" radio button is selected. At the bottom right are "Submit" and "Cancel" buttons. A small vertical text "205569" is visible on the right side of the dialog box.

- Step 3** Enter a description of the Alarm Event.  
Enter up to 128 characters that describe this Alarm Event. This description displays on automatic captures you might configure.
- Step 4** In the Community field, enter the community string for the SNMP community to which traps are sent. This community string must match a trap community string set in the NAM traps.
- Step 5** Choose an event action.  
Choose **Log** to log the event and display it in the Alarms tab. Choose **Trap** to send the event to traps processing. Choose **Log and Trap** to log the event and send it to trap processing.
- Step 6** Click **Submit**.  
The Alarm Events table displays the newly configured Alarm Event in its list.

## Editing Alarm Events

To edit an alarm event:

- Step 1** Choose **Setup > Alarms**.  
The Alarm Events table displays any configured Alarm Events.
- Step 2** Choose the alarm event you want to modify, and click **Edit**.

## Deleting Alarm Events

To delete an alarm event:

- Step 1** Choose **Setup > Alarms**.  
The Alarm Events table displays any configured Alarm Events.
- Step 2** Choose the alarm event you want to remove, and click **Delete**.

## Setting Alarm Thresholds

You use the NAM GUI to set up alarm thresholds for MIB variables with values that trigger alarms. To view currently set alarm thresholds:

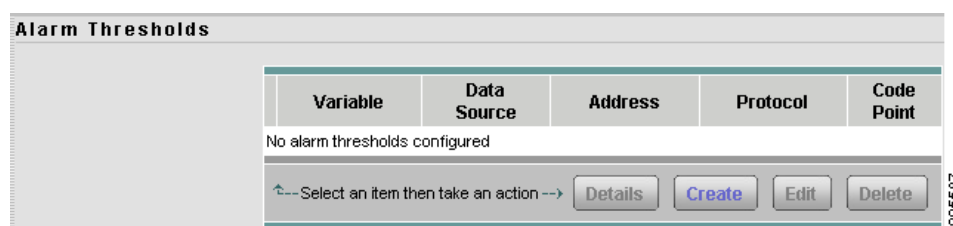
**Step 1** Click **Setup > Alarms**.

The Alarm Events table displays any configured Alarm Events.

**Step 2** In the content menu, click **Alarm Thresholds**.

The Alarm Thresholds table displays any currently setup alarm thresholds. [Figure 3-40](#) shows an example of the Alarm Thresholds table.

**Figure 3-40 Alarm Thresholds**



| Variable                                 | Data Source | Address | Protocol | Code Point |
|------------------------------------------|-------------|---------|----------|------------|
| No alarm thresholds configured           |             |         |          |            |
| ←--Select an item then take an action--> |             |         |          |            |
| <div>Details Create Edit Delete</div>    |             |         |          |            |

**Step 3** Click **Create** to set up an alarm threshold.

### Alarm Thresholds - Selecting a Variable

After you click Create on the Alarm Thresholds window, you must set up alarm threshold variable properties. To set up an alarm threshold variable:

**Step 1** Click **Setup > Alarms**.

The Alarm Events table displays any configured Alarm Events.

**Step 2** In the content menu, click **Alarm Thresholds**.

The Alarm Thresholds table displays any currently setup alarm thresholds. [Figure 3-40](#) shows an example of the Alarm Thresholds table.

**Step 3** Click **Create**.

The Alarm Thresholds - Create - Select a Variable window displays. [Figure 3-41](#) shows an example of the Alarm Thresholds - Create - Select a Variable window.

**Figure 3-41 Alarm Thresholds - Create - Select a Variable**

**Step 4** From the Variable pull-down list, choose one of the following variables:

You can choose from among the following:

- Network Layer Host
- Network Layer Conversations
- MAC Layer Hosts
- MAC Layer Conversations
- Application Statistics
- Server Response Times
- Server-Client Response Times
- DiffServ Traffic Stats
- DiffServ Host Stats
- DiffServ Application Stats

**Step 5** From the pull-down menu, choose the type of packets or bytes:

You can choose from among the following:

- In Packets
- Out Packets
- In Bytes
- Out Bytes

**Step 6** For Network Protocol, use the pull-down menu to choose IPv4 (default) or IPv6.

**Step 7** Click **Next**.

## Alarm Thresholds - Selecting Parameters

After you click **Next** in the Alarm Thresholds - Create - Select a Variable window, you must set up the parameters for the alarm threshold variable.

To set up an alarm threshold variable parameters:

**Step 1** From the Alarm Thresholds - Create - Select a Variable window, click **Next**.

[Figure 3-40](#) shows an example of the Alarm Thresholds table. The Alarm Thresholds - Create - Select Parameters window displays. [Figure 3-42](#) shows an example of the Alarm Thresholds - Create - Select Parameters window.

**Figure 3-42 Alarm Thresholds - Create - Select Parameters**

**Alarm Thresholds - Create - Select parameters**

**Select Parameters**

Data Source: ALL SPAN ▼

Network Protocol: IPv4

Variable: Network Layer Host InPkts

Network Address: 255.255.255.255

Polling Interval (seconds): 60

Sample Type: ☒ Absolute ☐ Delta

Rising Threshold (# of Pkts):

Falling Threshold (# of Pkts): 0

Rising Event: None ▼

Falling Event: None ▼

Table 3-31 lists and describes the parameters for Alarm Thresholds - Create - Select Parameters window.

**Table 3-31 Alarm Thresholds - Create - Select Parameters**

| Field             | Description                                                                                            | Usage Notes                                                                                                                                                                                                                           |
|-------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Source       | Available data sources on the NAM.                                                                     | Select the data source from the list.                                                                                                                                                                                                 |
| Network Protocol  | Selected protocol to be monitored.                                                                     | This is the network protocol you chose in Step 5.                                                                                                                                                                                     |
| Variable          | Selected variable to be monitored.                                                                     | This is the variable you chose in Step 3.                                                                                                                                                                                             |
| Network Address   | Network address of host.                                                                               | For network-layer host variables only.                                                                                                                                                                                                |
| Polling Interval  | Interval in seconds for the sampling period.                                                           | Enter the number of seconds for the polling interval duration.                                                                                                                                                                        |
| Sample Type       | Type of sampling to be done.                                                                           | <ul style="list-style-type: none"> <li>Click <b>Absolute</b> for an alarm to be triggered by an absolute value that is reached.</li> <li>Click the <b>Delta</b> for an alarm to be triggered by a change in the data rate.</li> </ul> |
| Rising Threshold  | Number of packets that triggers the alarm. For response time alarms, it is the number of milliseconds. | Enter a whole number (an integer)                                                                                                                                                                                                     |
| Falling Threshold | Number of packets that triggers the alarm. For response time alarms, it is the number of milliseconds. | Enter a whole number (an integer)                                                                                                                                                                                                     |
| Rising Event      | Alarm threshold as defined in the RMON1 MIB.                                                           | Use the pull-down menu to select a rising threshold event.                                                                                                                                                                            |
| Falling Event     |                                                                                                        | Use the pull-down menu to select a falling threshold event.                                                                                                                                                                           |

**Step 2** Enter the desired parameters for the alarm threshold you are creating.

**Step 3** Click **Finish** to accept your changes, or click **Cancel** to cancel.

## Viewing Alarm Details from the NAM MIB Thresholds Table

To view details of a specific alarm from the NAM MIB Thresholds table, select the radio button, then click **Details**. The Alarms Details Table (Table 3-32) displays.

**Table 3-32 Alarm Details Table**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variable           | Monitored variable.                                                                                                                                                                                                                                                                                                                                         |
| Data Source        | Data source being monitored.                                                                                                                                                                                                                                                                                                                                |
| Address            | Destination and source address of the hose.                                                                                                                                                                                                                                                                                                                 |
| Interval (seconds) | Interval of the sampling period.                                                                                                                                                                                                                                                                                                                            |
| Sample Type        | Sample type of the alarm—absolute or delta.                                                                                                                                                                                                                                                                                                                 |
| Rising Threshold   | The number of rising packets or octets that triggers the alarm.                                                                                                                                                                                                                                                                                             |
| Falling Threshold  | The number of falling packets or octets that triggers the alarm.                                                                                                                                                                                                                                                                                            |
| Alarm Action       | Action to be taken when the alarm is triggered.                                                                                                                                                                                                                                                                                                             |
| Community          | SNMP community where traps are sent.                                                                                                                                                                                                                                                                                                                        |
| Trigger Set        | None, Start or Stop. Start indicates a capture process would start when this alarm is triggered. Stop means a capture process would stop when this alarm is triggered. None means no capture trigger is set for this alarm.<br><br>See <a href="#">Using Alarm-Triggered Captures</a> for information about how to use the alarm-triggered capture feature. |

## Editing an Alarm Threshold

To edit an alarm threshold:

- 
- Step 1** Choose **Setup > Alarms**.  
The Thresholds table displays.
  - Step 2** Select the alarm to edit, then click **Edit**.  
The Edit Event dialog box displays.
  - Step 3** Make the necessary changes.
  - Step 4** Click **Finish** to save your changes, or click **Cancel** to cancel the edit.
- 

## Deleting a NAM MIB Threshold

To delete a NAM MIB threshold, simply select it from the Alarms table, then click **Delete**.

- Step 5** Click **Apply** to save your changes, or click **Reset** to leave the configuration unchanged.
-

## Setting Up Voice/Video Stream Thresholds

You can set up the NAM to monitor voice and video streams to display packet loss statistics based on the RTP sequence number. When you set up the RTP stream thresholds and enable alarms, an EMail alarm message is sent to those configured under **Admin > System > EMail Configuration**. See [E-Mail Configuration, page 2-18](#) for information about how to configure EMail.

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

The Alarm Events table displays.

**Step 2** In the content menu, click **Voice/Video Stream Thresholds**.

The Voice/Video Stream Thresholds window displays as shown in [Figure 3-43](#).



**Note**

The values in the Voice/Video Thresholds, even if unchecked, are the thresholds used when you view the different menu options of the **Monitor > Voice/Video** windows.

**Figure 3-43 Setup Voice/Video Stream Thresholds Window**

| Voice/Video Stream Thresholds Per Minute |                                       |            |
|------------------------------------------|---------------------------------------|------------|
| Enable Alarm Thresholds                  | Codec                                 | Thresholds |
| <input type="checkbox"/>                 | G711 (1-4.4):                         | 4.1        |
|                                          | G722 64k (1-4.5):                     | 3.3        |
|                                          | G722 56k (1-3.3):                     | 3.3        |
|                                          | G722 48k (1-4.5):                     | 3.3        |
|                                          | G723.1 (1-3.9):                       | 3.4        |
|                                          | MOS:                                  |            |
|                                          | G728 (1-4.0):                         | 3.6        |
|                                          | G729 (1-4.11):                        | 3.9        |
|                                          | GSM (1-4.3):                          | 3.5        |
|                                          | G726 32k (1-4.2):                     | 3.6        |
|                                          | G726 24k (1-4.2):                     | 3.3        |
|                                          | G726 16k (1-4.2):                     | 3.1        |
| <input type="checkbox"/>                 | Adjusted Packet Loss %(1-100):        | 3.0        |
| <input type="checkbox"/>                 | Actual Packet Loss %(1-100):          | 3.0        |
| <input type="checkbox"/>                 | Actual Packet Loss (1-10000):         | 100        |
| <input type="checkbox"/>                 | Jitter (1-10000 ms):                  | 5          |
| <input type="checkbox"/>                 | Seconds of Severe Concealment (1-60): | 2          |
| <input type="checkbox"/>                 | Seconds of Concealment (1-60):        | 6          |

206509

[Table 3-33](#) describes the fields of the Voice/Video Stream Thresholds window. To enable alarms for the thresholds listed, you must click at least one checkbox under Enable Alarm Thresholds on the left side of the Voice/Video Stream Thresholds Per Minute window.

**Table 3-33 Voice/Video Stream Thresholds**

| Field                                | Description                                                                                                                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MOS                                  | Click the MOS (Mean Opinion Scores) check box to enable an alarm when the NAM detects MOS quality above the thresholds for each codec listed.                                             |
| Adjusted Packet Loss %(1-100)        | Click the Adjusted Packet Loss % check box to enable an alarm when the NAM detects Adjusted Packet Loss percentage to be more than the value set here.                                    |
| Actual Packet Loss %(1-100)          | Click the Actual Packet Loss % check box to enable an alarm when the NAM detects Actual Packet Loss percentage to be more than the value set here.                                        |
| Actual Packet Loss (1-10000)         | Click the Actual Packet Loss (number of packets) check box to enable an alarm when the NAM detects the actual number of packets lost in an RTP stream to be more than the value set here. |
| Jitter                               | Click the Jitter check box to enable an alarm when the NAM detects SoC to be more than the value set here.                                                                                |
| Seconds of Severe Concealment (1-60) | Click the Seconds of Severe Concealment check box to enable alarms when the NAM detects Seconds of Severe Concealment to be more than the value set here.                                 |
| Seconds of Concealment (1-60)        | Click the Seconds of Concealment check box to enable alarms when the NAM detects Seconds of Concealment to be more than the value set here.                                               |

**Step 3** Choose the type or types of threshold for which you want to enable an alarm.

**Step 4** Click **Apply** to set the voice/video stream thresholds, click **Defaults** to reset the thresholds to their default value, or click **Reset** to remove any changes you might have made.

## Setting Up the NAM Syslog

NAM syslogs are created for alarm threshold events, voice threshold events, or system alerts. The NAM maintains two syslog files, one for logging RMON threshold events (for MIB and voice threshold events) and one for logging local NAM 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 Traffic Analyzer to view the local NAM syslogs.

For information on viewing the **syslog**, see [Chapter 7, “Viewing Alarms.”](#) You can use a standard text editor to view **syslog** on remote hosts.

To set up the NAM syslog:

- 
- Step 1** Choose **Setup > Alarms**.  
The Alarm Events table displays.
- Step 2** In the content menu, click **NAM Syslog**.  
The [NAM Alarms Syslog Dialog Box](#) ([Table 3-34](#)) displays.
- Step 3** Make the necessary changes.

**Table 3-34** *NAM Alarms Syslog Dialog Box*

| Field                         | Usage Notes                                                                                                                                                                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Thresholds              | <ul style="list-style-type: none"><li>• Select <b>Local</b> to log messages on your local system.</li><li>• Select <b>Remote</b> to log messages on a remote system.</li></ul>                                                                                                                 |
| Voice/Video Stream Thresholds | <ul style="list-style-type: none"><li>• Select <b>Local</b> to log voice/video threshold syslogs on your local system.</li><li>• Select <b>Remote</b> to log voice/video threshold syslogs on a remote system.</li></ul>                                                                       |
| RTP Stream                    | <ul style="list-style-type: none"><li>• Select <b>Local</b> to log RTP Stream threshold syslogs on your local system.</li><li>• Select <b>Remote</b> to log RTP Stream threshold syslogs on a remote system.</li></ul>                                                                         |
| System                        | <ul style="list-style-type: none"><li>• Select <b>Local</b> to log system alert syslogs on your local system.</li><li>• Select <b>Remote</b> to log system alert syslogs on a remote system.</li><li>• Select <b>Debug</b> to log debug messages from the application to the syslog.</li></ul> |
| Remote Server Names           | Enter the IP address or DNS name of up to 5 remote systems where syslog messages are logged. Each address you enter receives syslog messages from all three alarms (Alarm Thresholds, Voice/Video Stream Thresholds, and System).                                                              |

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

## Setting Chassis or Managed Device Thresholds

**Note**

This section does not apply to NME-NAM devices.

---



You can configure RMON thresholds in the switch Mini-RMON MIB. You can specify only variables from the etherStatsTable in the Mini-RMON MIB to monitor for threshold-crossing conditions.

These topics help you set up and manage switch thresholds:

- [Creating Chassis or Managed Device Thresholds, page 3-91](#)
- [Editing Chassis or Managed Device Thresholds, page 3-92](#)
- [Deleting Chassis or Managed Device Thresholds, page 3-93](#)

## Creating Chassis or Managed Device Thresholds

To create chassis or managed device thresholds:

- 
- Step 1** Choose **Setup > Alarms**.  
The Thresholds table displays.
- Step 2** In the contents, click **Chassis Thresholds** or **Managed Device Thresholds**.  
The Chassis Threshold table displays.
- Step 3** Click **Create**.  
The New Chassis Thresholds ([Table 3-35](#)) displays.

**Table 3-35**      **New Chassis Alarm Dialog Box**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Usage Notes |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Data Source List | Data source from the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | —           |
| Variable         | <p>The following variables are available:</p> <ul style="list-style-type: none"> <li>• Broadcast Pkts</li> <li>• Collisions</li> <li>• CRC Align Errors</li> <li>• Drop Events</li> <li>• Fragments</li> <li>• Jabbers</li> <li>• Multicast Pkts</li> <li>• Bytes</li> <li>• Oversize Pkts</li> <li>• Packets</li> <li>• Pkts size 64 Bytes</li> <li>• Pkts 65 to 127 Bytes</li> <li>• Pkts 128 to 255 Bytes</li> <li>• Pkts 256 to 511 Bytes</li> <li>• Pkts 512 to 1023 Bytes</li> <li>• Pkts 1024 to 1518 Bytes</li> <li>• Undersize Pkts</li> </ul> | —           |

**Table 3-35**      **New Chassis Alarm Dialog Box (continued)**

| Field              | Description                                                  | Usage Notes                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interval (seconds) | Length of time, in seconds, for the sampling period to last. | Enter a decimal number.                                                                                                                                                                                                                                |
| Sample Type        | Type of sampling to be done.                                 | <ul style="list-style-type: none"> <li>Click <b>Absolute</b> for an alarm to be triggered by an absolute value that is reached.</li> <li>Click <b>Delta</b> for an alarm to be triggered by a change in the data rate.</li> </ul>                      |
| Rising Threshold   | Number of packets/octets that trigger the alarm.             | Enter a number (an integer)                                                                                                                                                                                                                            |
| Falling Threshold  | Number of packets/octets that trigger the alarm.             | Enter a number (an integer)                                                                                                                                                                                                                            |
| Alarm Description  | Description of the alarm.                                    | Must not exceed 128 characters.                                                                                                                                                                                                                        |
| Alarm Action       | Action to be taken when the alarm is triggered.              | <ul style="list-style-type: none"> <li>Click <b>Log</b> to log the event and display it in the Alarms tab.</li> <li>Click <b>Trap</b> to send the event to traps.</li> <li>Click <b>Log and Trap</b> to log the event and send it to traps.</li> </ul> |
| Community          | SNMP community where traps are sent.                         | This community string must match the traps community string set on the switch.                                                                                                                                                                         |

**Step 4** Click **Submit** to save your changes, or click **Reset** to reset any entries you might have made.



**Note** If the switch is running a Catalyst operating system image, the switch alarm configuration is automatically stored. If the switch is running a Cisco IOS image, you can save the alarm configuration to NVRAM.

## Editing Chassis or Managed Device Thresholds



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

To edit chassis thresholds or managed device thresholds:

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

The Thresholds table displays.

**Step 2** In the content menu, click **Chassis Thresholds** or **Chassis Thresholds**.

- The Switch Threshold Alarms dialog box displays.
- Step 3** Select the alarm to edit, then click **Edit**.
- The Edit Alarm dialog box displays.
- Step 4** Make the necessary changes, then click **Submit** to save your changes, or click **Reset** to cancel and leave the configuration unchanged.
- 

## Deleting Chassis or Managed Device Thresholds

**Note**

This section does not apply to NME-NAM devices.

To delete an existing chassis threshold or managed device threshold, select it from the Chassis Threshold Alarms table, then click **Delete**.

## Setting NAM Trap Destinations

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.

These topics help you set up and manage NAM traps:

- [Creating a NAM Trap Destination, page 3-93](#)
- [Editing a NAM Trap Destination, page 3-94](#)
- [Deleting a NAM Trap Destination, page 3-94](#)

## Creating a NAM Trap Destination

To create a NAM trap destination:

- Step 1** Choose **Setup > Alarms**.
- The NAM MIB Thresholds table displays.
- Step 2** In the content, click **NAM Trap Destinations**.
- The Traps dialog box displays.
- Step 3** Click **Create**.
- The Create Trap Dialog Box ([Table 3-36](#)) displays.
- Step 4** Enter the appropriate information.

**Table 3-36** Create Trap Dialog Box

| Field      | Description                                                                              |
|------------|------------------------------------------------------------------------------------------|
| Community  | The community string of the <i>alarm</i> community string set in the NAM MIB Thresholds. |
| IP Address | The IP address to which the trap is sent if the alarm and trap community strings match.  |
| UDP Port   | The UDP port number.                                                                     |

- Step 5** 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 **Setup > Alarms**.  
The Thresholds table displays
- Step 2** In the contents, click **NAM Traps**.  
The Traps dialog box displays.
- Step 3** Select the trap to edit, then click **Edit**.  
The Edit Trap dialog box displays.
- Step 4** Make the necessary changes.
- Step 5** 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**.

## Setting NAM Alarm Mail



### Note

NAM alarm mail is sent as a result of NAM alarms, not router or switch alarms.

---

You can configure the NAM to send Email to one or more addresses in the case of a NAM alarm. To configure Email alarms:

- 
- Step 1** Choose **Setup > Alarms**.
- Step 2** From the content menu, click **NAM Alarm Mail**.  
The Alarm Mail Configuration dialog box displays.
- Step 3** In the **Mail Alarm to** field, enter one or more Email addresses to receive the NAM alarm mail.  
Use an Email address such as *jdoe@cisco.com*. Use a space to separate multiple Email addresses.
- 

## Setting Global Preferences

Global preferences settings apply to all users of the NAM and determine how data displays are formatted. To set up global preferences.

- Step 1** Choose **Setup > Preferences**.  
The Preferences Dialog Box (Figure 3-44) displays.

**Figure 3-44** Preferences Dialog Box

- Step 2** Enter or change the information described in the Preferences Dialog Box (Table 3-37).

**Table 3-37** Preferences Dialog Box

| Field                           | Description                                                                                                        | Usage Notes                                                                                                                                                                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entries Per Screen              | The number of rows to display in tabular screens.                                                                  | Enter a number from 1 to 100. The default is 15.                                                                                                                                  |
| Refresh Interval                | The number of seconds between monitor display refreshes.                                                           | Enter a number from 15 to 3600. The default is 60.                                                                                                                                |
| Number Graph Bars               | The number of graph bars to display in TopN displays and charts.                                                   | Enter a number from 1 to 15. The default is 10.                                                                                                                                   |
| Perform IP Host Name Resolution | Display DNS names, if available.                                                                                   | Select to enable or deselect to disable. Enabled by default.<br><b>Note</b> Enabling IP host name resolution without configuring nameservers might result in slow response times. |
| Data Displayed in               | Option to display data in bits or bytes.                                                                           | Select Bytes or Bits. Default is bytes.                                                                                                                                           |
| Format Large Numbers            | Display large integer values in appropriate units with prefixes such as Kilo (K), Mega (M), Giga (G) and Tera (T.) | Check box to format large numbers. If this box is unchecked, large numbers are not formatted. The default is unchecked.                                                           |

**Table 3-37**      **Preferences Dialog Box (continued)**

| Field                        | Description                                                                                                                              | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| International Notation       | You have the option to print numbers in the following format:<br><br>1,025.72<br>1.025,72<br>1 025,72                                    | Default is 1,025.72                                                                                                                                                                                                                                                                                                                                                                                            |
| CSV Export Monitor Entries   | Provides the option to CSVexport all entries in a particular monitor table or just the current entries displayed on a particular window. | Default is Current Window Only.                                                                                                                                                                                                                                                                                                                                                                                |
| Audit Trail                  | Check box to enable or disable the audit trail.                                                                                          | Enables the recording of critical user activities to an internal log file. By default, the audit trail is enabled.<br><br>See also:<br><ul style="list-style-type: none"> <li>• <a href="#">Viewing the Audit Trail, page 2-26</a>, for information about audit trail entries</li> <li>• <a href="#">Setting Up the NAM Syslog, page 3-90</a>, for information about setting up remote file storage</li> </ul> |
| ESP-Null Heuristic           | Enables NAM to detect ESP-null encryption and parse content as described in Internet RFC 2410.                                           | Enabling ESP-Null Heuristic forces the NAM to check all packets with an ESP header to see if it could be using Null encryption. The ESP-Null Heuristic feature adds processing overhead, so it is disabled by default.                                                                                                                                                                                         |
| Capture File Download Format | Check ENC or PCAP.                                                                                                                       | <to be supplied>                                                                                                                                                                                                                                                                                                                                                                                               |

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



## CHAPTER 4

# Monitoring Data

---

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

- [Overview of Data Collection and Data Sources, page 4-2](#)
- [Viewing the Monitor Overview Charts, page 4-6](#)
- [Viewing Application Groups, page 4-14](#)
- [Viewing Individual Applications Data, page 4-9](#)
- [Viewing Collected URLs, page 4-18](#)
- [Viewing Voice and Video Data, page 4-23](#)
- [Monitoring Hosts, page 4-34](#)
- [Viewing Conversations Data, page 4-42](#)
- [Viewing VLAN Data, page 4-51](#)
- [Viewing DiffServ Data, page 4-57](#)
- [Monitoring Response Time Data, page 4-69](#)
- [Viewing Port/Interface Statistics Data, page 4-93](#)
- [Viewing System Health, page 4-103](#)
- [Viewing NBAR, page 4-111](#)
- [Viewing MPLS Traffic Statistics, page 4-115](#)



### Note

NAM 4.1 supports IPv6 for all monitoring functionality except monitoring response time and RTP stream analysis.

# Overview of Data Collection and Data Sources

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

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

**Table 4-1**      **Collection Definitions**

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

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



## Note

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

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

- The number of potential simultaneous collections is limited only by CPU and memory resources.
- The collection data sources are limited by the SPAN sources. For more information on SPAN sources, see the [“Data Sources” section on page 3-10](#).
- NAM 4.1 can support a maximum of at least 1,500 data sources.

## Configuring Multiple Collections

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



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

- All packets in the SPAN/VACL traffic stream regardless of the port/VLAN or origin (ALL SPAN).
- All packets in the SPAN/VACL traffic stream on a specific VLAN (VLAN x).
- All packets in the SPAN/VACL traffic stream that were configured to arrive on a specific NAM data port (DATA PORT 1 or DATA PORT 2).
- NetFlow Data Export (NDE) records received by the NAM from either the local Supervisor engine module or other remote NDE sources such as remote routers. (Available only on NAM-1 and NAM-2.)
- Switch engine module (Supervisor) records received by the NAM. You can select any combination of Port statistics, VLAN statistics, and NBAR statistics. (Available only on NAM-1 and -NAM-2.)
- Router engine module records (Router) received by the NAM. You can select any combination of Interface statistics and NBAR statistics. (Available only on the NME-NAM.)

**Note**

Data sources persist across all Monitor windows. For example, if you select VLAN2 as a data source, then go to another Monitor window, VLAN2 will be displayed there if it is configured for that collection. If the previously selected data source is not configured for collection on the new Monitor window, the NAM displays the default data source for that window.

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

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

**Scenario**

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

You must specify a collection data source for this collection. The data source could be VLAN 1, VLAN 2, or VLAN 3.

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

**Note**

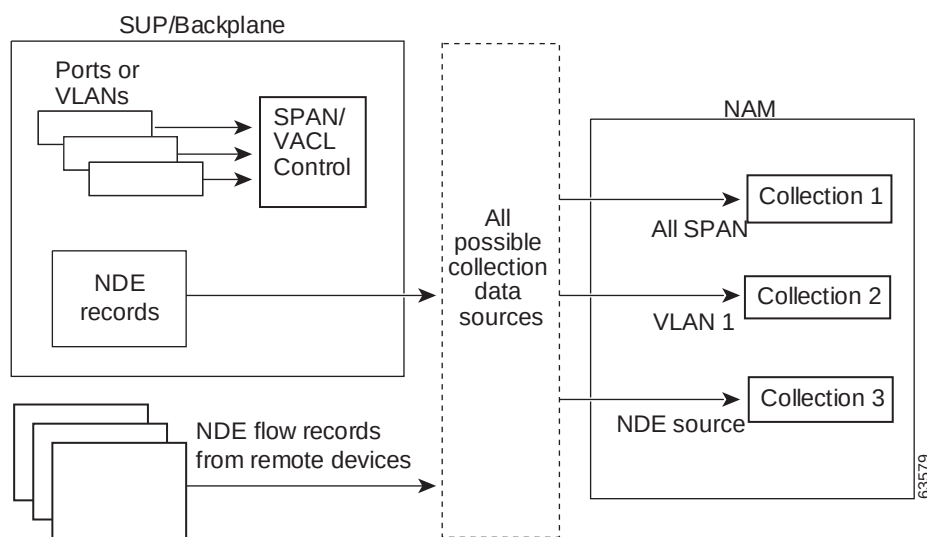
The SPAN/VACL traffic stream represents the aggregate sum of all traffic being sent to the NAM for monitoring as a result of SPAN or VACL configuration on the local Supervisor engine module. In addition to the SPAN/VACL traffic stream, one or more NDE traffic streams might be received from the local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

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

**Table 4-2 Data Collection Sources**

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

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

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

You can view real-time data from collections that were configured on the NAM. For more information on setting up collections on the NAM, see the [“Configuring Capture Settings”](#) section on page 6-3.

## Protocol Auto Discovery

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

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

**Table 4-3 Auto-Discovered Protocol Types**

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

**Note**

The automatically discovered protocols are not saved in NVRAM and are lost when the NAM is rebooted. To save an auto-discovered protocol, you can enter it manually into the Protocol Directory. For more information, see the [“Creating a New Protocol” section on page 3-70](#). You can also clear the auto-discovered protocols without rebooting by entering the command `no monitor protocol auto-learned` in the NAM CLI.

## NDE Flow Masks and V8 Aggregation Caches

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

**Table 4-4 Flow Mask and Aggregation Window Conditions**

| Flow Mask or Aggregation Cache | Window Conditions                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full flow mask                 | Supported in all windows.                                                                                                                                                                                                                                                                                                                                                            |
| Destination only flow mask     | <ul style="list-style-type: none"> <li><b>Monitor &gt; Apps</b> displays “Others” only, and the detail pop-up window does not have data.</li> <li><b>Monitor &gt; Hosts</b> displays 0.0.0.0 and the detail pop-up window does not have data.</li> <li><b>Monitor &gt; Conversations</b> displays 0.0.0.0 for some hosts and the detail pop-up window does not have data.</li> </ul> |
| Destination-Source flow mask   | <ul style="list-style-type: none"> <li><b>Monitor &gt; Apps</b> displays “Others” only, and the detail pop-up window does not have data.</li> <li><b>Monitor &gt; Hosts</b> has data, but the detail pop-up window does not.</li> <li><b>Monitor &gt; Conversations</b> has data, but the detail pop-up window does not.</li> </ul>                                                  |

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

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

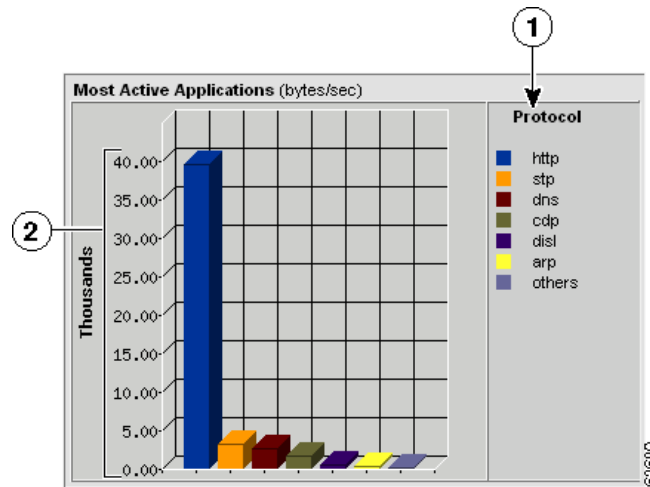
## Viewing the Monitor Overview Charts

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

The following charts are displayed:

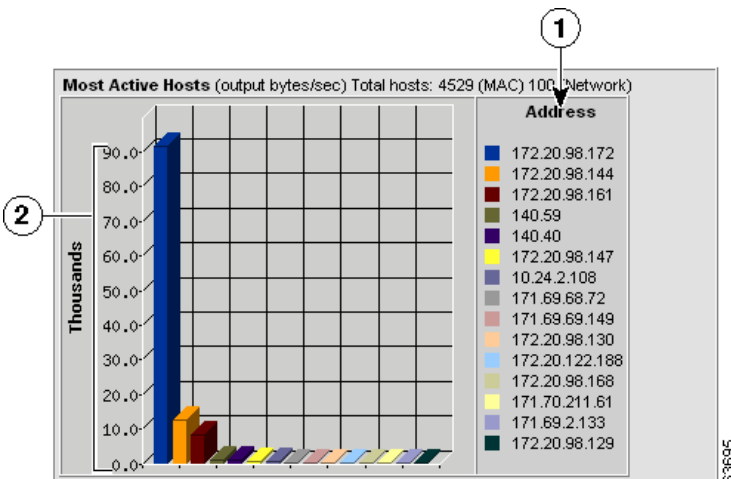
- [Most Active Applications Chart](#) (Figure 4-2)
- [Most Active Hosts Chart](#) (Figure 4-3)
- [Server Response Times Chart](#) (Figure 4-4)
- [Protocol Suites Chart](#) (Figure 4-5)

**Figure 4-2 Most Active Applications Chart**

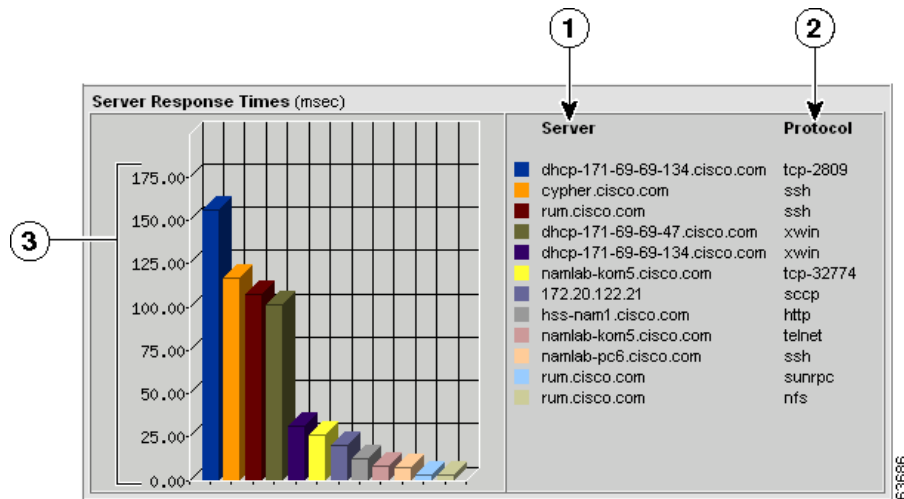


|   |                                  |   |                                                         |
|---|----------------------------------|---|---------------------------------------------------------|
| 1 | Top N protocols sorted by color. | 2 | Number of bytes collected per second for each protocol.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

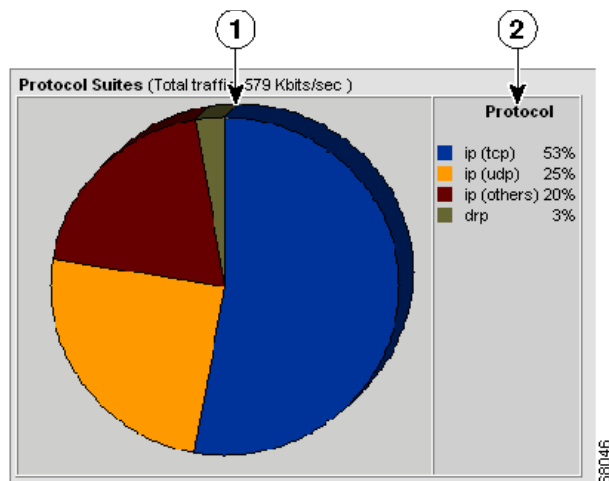
**Figure 4-3 Most Active Hosts Chart**



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

**Figure 4-4 Server Response Times Chart**

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

**Figure 4-5 Protocol Suites Chart**

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

## Data Source Persistence

When you view a monitor window with drop down data source lists, the NAM saves the selected data source. When you next view a monitor window with a drop down data source list, the NAM displays the previously saved data source. If no data source has been previously viewed and saved, the NAM displays the default data source. If you go to a different monitor window, and no collection has been configured with the saved data source, the default data source displays.

## Viewing Individual Applications Data

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

You can select a radio button for:

- [Viewing the Application Groups Current Rates Table, page 4-14](#)
- [Viewing the Top N Application Group Chart, page 4-16](#)
- [Viewing the Application Groups Cumulative Data Table, page 4-17](#)

## Viewing the Applications

The Applications Current Rates table enables you to view the number of packets and bytes collected for each application protocol. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the “[Setting Global Preferences](#)” section on page 3-94.

**Note**

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

To view the Applications Current Rates table:

- Step 1** Click the Current Rates table radio button.  
The [Applications Current Rates Table](#) (Table 4-5) displays.

**Table 4-5**      **Applications Current Rates Table**

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

- Step 2** Choose the data source to monitor from the Data Source list.
- Step 3** To view data for a specific protocol, enter the protocol name in the Protocol text box, then click **Filter**. Any matching protocols are displayed.

Click to select a protocol from those listed, then:

- Click **Save** to save the protocol to the database.
- Click **Details** to view more details about the protocol.
- Click **Capture** to begin a capture of data flow of the chosen protocol.
- Click **Real-Time** to view a real-time graph of the protocol's traffic.
- Click **Report** to generate a report of the chosen protocol.



**Tip**

- To view the full protocol name, move the cursor over the protocol name in the Protocol column of the Protocol Directory table.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Displaying Details from the Applications Table

To view details for a specific application protocol, select the protocol and click Details, or click on the protocol name in the Protocol column. The Application Group Window ([Figure 4-10](#)) displays, showing all network hosts using this protocol. The displayed data is specific to the selected data source.

**Figure 4-6 Application Protocol Detail Window**

| Host                         | In Pkts | Out Pkts | In Bytes | Out Bytes |
|------------------------------|---------|----------|----------|-----------|
| static-10-24-2-108.cisco.com | 158060  | 315964   | 23055636 | 21507392  |
| 172.20.98.134                | 315968  | 158062   | 21507664 | 23055928  |

The Applications Protocol Detail Window displays the following information.

**Table 4-6 Application Protocol Detail Table**

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



## Capturing Application Protocol Data from the Application Table

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

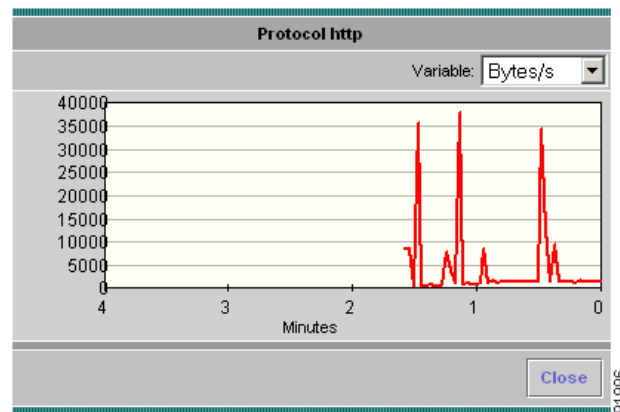
Choose the protocol from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information”](#) section on page 6-14.

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

## Viewing Real-Time Data from the Application Table

You can view real-time data in a graphical format for a specific application protocol. Choose the protocol from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-7](#)) displays.

**Figure 4-7** Real-Time Graph



## Viewing Reports from the Applications Table

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

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

## Viewing the Top N Applications Chart

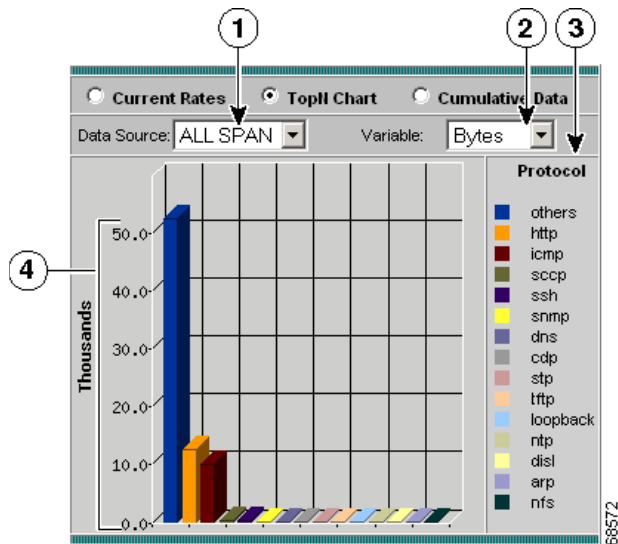
The TopN Applications Chart enables you to view the number of packets and bytes collected for the Top N application protocols in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the TopN Applications chart:

- 
- Step 1** Click the TopN Chart radio button.

The TopN Application Group Chart (Figure 4-8) displays.

**Figure 4-8** *TopN Applications Chart*



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

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

**Step 3** Choose one of the following from the Variable list:

- Packets—Displays the number of packets per second monitored.
- Bytes—Displays the number of bytes per second monitored.



**Tip**

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

## Viewing the Applications Cumulative Data Table

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

To view the Applications Cumulative Data table:

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

The [Application Group Cumulative Data Table](#) (Table 4-11) displays.

**Table 4-7 Applications Cumulative Data Table**

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

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

**Step 3** To refresh the table, click **Refresh**.

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



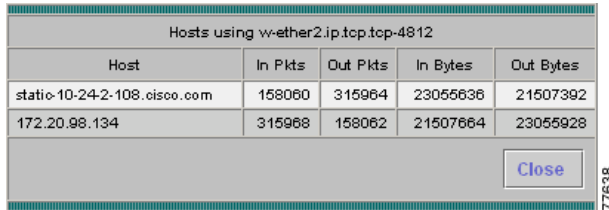
**Tip**

- To view the full encapsulated protocol name, move the cursor over the protocol name in the Protocol column of the Protocol Directory table.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Displaying Details from the Applications Table

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

**Figure 4-9 Protocol Detail Window**



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

The Protocol Detail Window displays the following information:

**Table 4-8 Protocol Detail Table**

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

## Viewing Application Groups

To view the distribution of packets and bytes based on the application group, click the Monitor tab, then click **Apps** and select **Application Groups** from the Contents Menu. The Applications Group table displays with three radio buttons on top.

You can select a radio button for:

- [Viewing the Application Groups Current Rates Table, page 4-14](#)
- [Viewing the Top N Application Group Chart, page 4-16](#)
- [Viewing the Application Groups Cumulative Data Table, page 4-17](#)

## Viewing the Application Groups Current Rates Table

The Application Groups Current Rates table enables you to view the number of packets and bytes collected for each application group. The data displayed is the number of packets and bytes or bits collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Application Groups Current Rates table:

- Step 1** Click the Current Rates table radio button.  
The [Application Groups Current Rates Table](#) (Table 4-9) displays.

**Table 4-9 Application Groups Current Rates Table**

| Field              | Description                             |
|--------------------|-----------------------------------------|
| Application Groups | Name of the application group.          |
| Packets/s          | Number of packets collected per second. |
| Bytes/s            | Number of bytes collected per second.   |
| Bits/s             | Number of bits collected per second.    |

- Step 2** Choose the data source to monitor from the Data Source list.  
**Step 3** To view data for a specific protocol group, enter the group name in the text box, then click **Filter**.  
Any matching groups are displayed.



**Tip**

- To view the application list for a particular protocol group, click the + sign in front of the group name.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Displaying Details from the Application Group Table

To view details for a specific application group, select the application group and click Details. The Application Group Window ([Figure 4-10](#)) displays, showing all applications in this group and the network hosts using those particular applications. The displayed data is specific to the selected data source.

**Figure 4-10 Application Group Window**

| Application Group Web                           |         |          |          |           |
|-------------------------------------------------|---------|----------|----------|-----------|
| Hosts using w-ether2.ip.tcp.http                |         |          |          |           |
| Description: Hypertext Transfer Protocol (HTTP) |         |          |          |           |
| Host                                            | In Pkts | Out Pkts | In Bytes | Out Bytes |
| 171.69.65.192                                   | 401     | 318      | 357603   | 58479     |
| 171.69.125.53                                   | 265     | 197      | 300024   | 23005     |
| 171.69.125.85                                   | 219     | 196      | 160757   | 50420     |
| 172.20.98.136                                   | 73      | 73       | 21970    | 5430      |
| 172.20.104.90                                   | 784     | 958      | 137334   | 840354    |
|                                                 |         |          |          | Close     |

12/6/18

The Applications Group Detail Window displays the information listed in [Table 4-10](#).

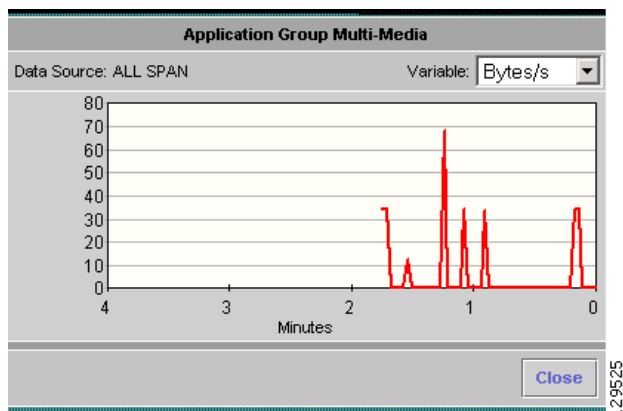
**Table 4-10**      **Application Group Detail Window Fields**

| Field       | Description                                                     |
|-------------|-----------------------------------------------------------------|
| Description | Full name and description of each application in that group.    |
| Host        | The hostname of the computer using the application group.       |
| In Pkts     | Number of packets the host received for the specified group.    |
| Out Pkts    | Number of packets the host transmitted for the specified group. |
| In Bytes    | Number of bytes the host received for the specified group.      |
| Out Bytes   | Number of bytes the host transmitted for the specified group.   |

## Viewing Real-Time Data from the Application Group Table

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

Choose the protocol from the table, then click **Real-Time**. The Real-Time Graph([Figure 4-11](#)) displays.

**Figure 4-11**      **Real-Time Graph**

## Viewing Reports from the Application Group Table

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

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

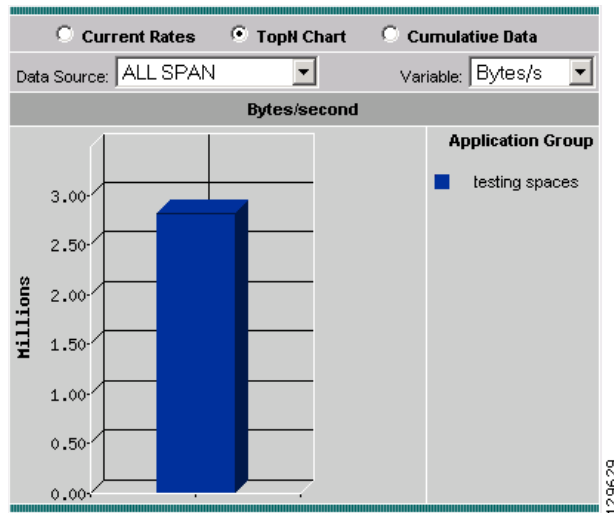
## Viewing the Top N Application Group Chart

The TopN Applications Chart enables you to view the number of packets and bytes collected for the Top N application protocols in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the TopN Applications chart:

- Step 1** Click the TopN Chart radio button.  
The TopN Application Group Chart (Figure 4-12) displays.

**Figure 4-12 TopN Application Group Chart**



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



**Tip**

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

## Viewing the Application Groups Cumulative Data Table

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

To view the Applications Groups Cumulative Data table:

- Step 1** Click the Cumulative Data radio button.  
The [Application Group Cumulative Data Table](#) (Table 4-11) displays.

**Table 4-11 Application Group Cumulative Data Table**

| Field      | Description                                                    |
|------------|----------------------------------------------------------------|
| Group Name | Name of the monitored group.                                   |
| Packets    | Total number of packets collected over the last time interval. |
| Bytes      | Total number of bytes collected over the last time interval.   |

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

**Step 3** To refresh the table, click **Refresh**.

**Step 4** To view data for a specific group, enter the group name in the Group text box, then click **Filter**.  
Any matching groups are displayed.

**Tip**

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

## Viewing Collected URLs

This section contains the following sections:

- [Viewing Collected URLs](#)
- [Filtering a URL Collection List](#)
- [Creating a URL-based Application from a Collected URL](#)

## Viewing Collected URLs

To view collected URLs:

**Step 1** Click **Monitor > Apps**.

**Step 2** Click **URLs** in the TOC.

The [URLs Window](#) ([Figure 4-13](#)) displays with the collected URLs.



**Figure 4-13** URLs Window

| #  | URL                                                         | Hits |
|----|-------------------------------------------------------------|------|
| 16 | http://hamlab-kom4.cisco.com/help/mappingfiles/divva_map.js | 7    |
| 17 | http://hamlab-kom4.cisco.com/images/abr_btn_hlt_bg_08.gif   | 1    |
| 18 | http://hamlab-kom4.cisco.com/images/abr_btn_hlt_rt_08.gif   | 8    |
| 19 | http://hamlab-kom4.cisco.com/images/abr_btn_nrm_lt_08.gif   | 1    |
| 20 | http://hamlab-kom4.cisco.com/images/abr_btn_nrm_rt_08.gif   | 4    |
| 21 | http://hamlab-kom4.cisco.com/images/abr_left_08.gif         | 10   |
| 22 | http://hamlab-kom4.cisco.com/images/abr_right_08.gif        | 4    |
| 23 | http://hamlab-kom4.cisco.com/images/arrow_pt_right.gif      | 6    |
| 24 | http://hamlab-kom4.cisco.com/images/btn_bg_1.gif            | 4    |
| 25 | http://hamlab-kom4.cisco.com/images/btn_rt_1.gif            | 9    |
| 26 | http://hamlab-kom4.cisco.com/images/export_list_16.gif      | 2    |
| 27 | http://hamlab-kom4.cisco.com/images/first16.gif             | 8    |
| 28 | http://hamlab-kom4.cisco.com/images/last16.gif              | 2    |
| 29 | http://hamlab-kom4.cisco.com/images/hext16.gif              | 4    |
| 30 | http://hamlab-kom4.cisco.com/images/plus.gif                | 9    |

**Table 4-12** URLs Table

| Field | Description    |
|-------|----------------|
| Index | URL index      |
| URL   | Name of URL    |
| Hits  | Number of hits |

**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](#) (Figure 4-13), select 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**.

## Creating a URL-based Application from a Collected URL

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

**Step 1** From the list of URLs shown in the Create URL-based Application window, click a radio button to select a row in the URL list.

**Step 2** Click **Create URL-based Application**.

The Create URL-based Application window ([Figure 4-14](#)) displays.

**Figure 4-14** Create URL-based Application

**Step 3** Enter a value in the fields for Index and Protocol Description.

For information about appropriate values for the Index and Protocol Description fields, see [Creating a URL-Based Application, page 3-78](#).

**Step 4** Click **Apply**.

## Viewing the TCP/UDP Port Table

The TCP/UDP Port Table displays with three radio buttons; one for current rates (the default view), one for TopN Chart, and one for Cumulative Data.

You can select a radio button for:

- [Viewing the TCP/UDP Port Table Current Rates, page 4-21](#)
- [Viewing the TCP/UDP Port Table TopN Chart, page 4-21](#)
- [Viewing the TCP/UDP Port Table Cumulative Data, page 4-22](#)

## Viewing the TCP/UDP Port Table Current Rates

To view the TCP/UDP Port Table current rates, click **Monitor > Apps > TCP/UDP Port Table**.

The TCP/UDP Port Table Current Rates table enables you to view the current rates of data transfer for the various TCP and UDP server ports. [Table 4-13](#) lists the statistics shown in the TCP/UDP Port Table Current Rates table.

**Table 4-13** TCP/UDP Port Table Current Rates

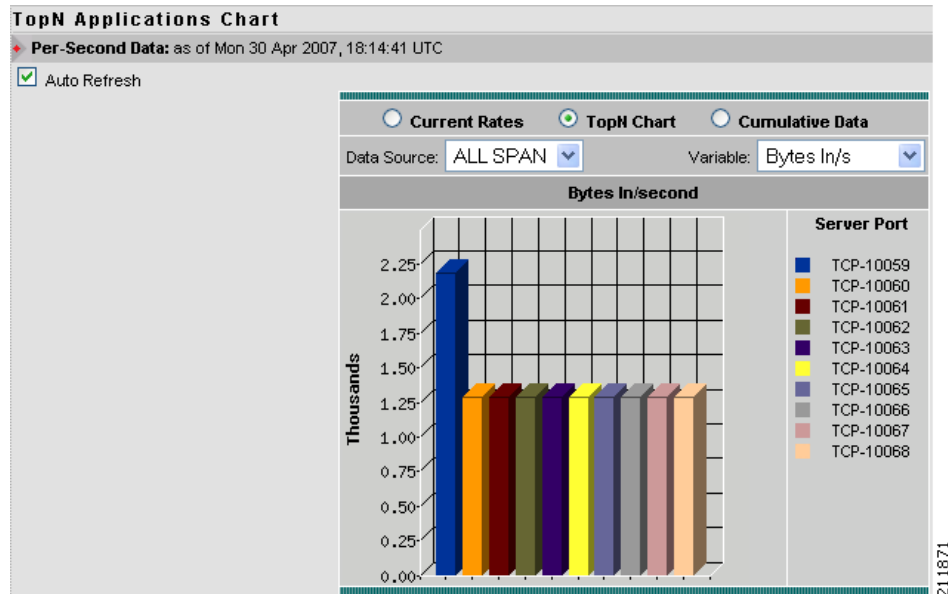
| Field         | Description                                                                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Port   | All server ports currently in use.                                                                                                                                                                                                                                                                                                                                        |
| Application   | Application in use on each port.<br><br><b>Note</b> In some cases, the Application field might be blank. This usually happens with TCP/UDP ports that are used dynamically rather than static or well-known ports. When the NAM determines that the same port was used for more than one application, from that point on the NAM displays the Application field as blank. |
| Packets In/s  | Packets in per second                                                                                                                                                                                                                                                                                                                                                     |
| Packets Out/s | Packets out per second                                                                                                                                                                                                                                                                                                                                                    |
| Bytes In/s    | Bytes in per second                                                                                                                                                                                                                                                                                                                                                       |
| Bytes Out/s   | Bytes out per second                                                                                                                                                                                                                                                                                                                                                      |

## Viewing the TCP/UDP Port Table TopN Chart

To view the TCP/UDP Port Table TopN Chart, click **Monitor > Applications > TCP/UDP Port Table**, then click the TopN button. The TCP/UDP Port Table TopN Chart shows a graphical chart of the most active TCP and UDP ports currently being used.

You can select to show the chart based on different Data Sources or to select a different variable such as packets or bytes in or out per second.

[Figure 4-15](#) shows an example of the TCP/UDP Port Table TopN Chart.

**Figure 4-15 TCP/UDP Port Table TopN Chart**

## Viewing the TCP/UDP Port Table Cumulative Data

The TCP/UDP Port Table Cumulative Data table enables you to view the number of packets and bytes collected for each server port. The data displayed is the total number of packets and bytes collected since the collection was created or since the NAM was restarted.

To view the TCP/UDP Port Table Cumulative Data table:

- Step 1** Click the Cumulative Data radio button.  
 The [TCP/UDP Table Cumulative Data Table](#) (Table 4-14) displays.

**Table 4-14 TCP/UDP Table Cumulative Data Table**

| Field       | Description                       |
|-------------|-----------------------------------|
| Server Port | All server ports currently in use |
| Application | Application in use on each port   |
| Packets In  | Total number of packets received  |
| Packets Out | Total number of packets sent      |
| Bytes In    | Total number of bytes received    |
| Bytes Out   | Total number of bytes sent        |

- Step 2** Choose the data source to be monitored from the Data Source list.  
**Step 3** To refresh the table, click **Refresh**.  
**Step 4** To view data for a specific group, enter the group name in the Group text box, then click **Filter**.  
 The GUI displays any matching groups.

**Tip**

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

## Viewing Voice and Video Data

You can use the NAM Traffic Analyzer to view data collected from any enabled voice and video protocols on the NAM. This enables you to troubleshoot and identify potential problems within your voice and video network.

This section is organized to match the menu options of the **Monitor > Voice/Video** portion of the NAM GUI.

- [Active Calls, page 4-23](#)
  - [MOS Quality Chart, page 4-23](#)
  - [Alarm Threshold Chart, page 4-24](#)
  - [Active Calls Table, page 4-26](#)
- [Terminated Calls, page 4-28](#)
  - [Overview, page 4-28](#)
  - [Worst N Calls, page 4-29](#)
- [Viewing Known Phones, page 4-30](#)
- [Viewing RTP Stream Traffic, page 4-32](#)

## Active Calls

The Voice Quality menu options provide an overview of voice quality and the worst calls.

- [MOS Quality Chart, page 4-23](#)
- [Alarm Threshold Chart, page 4-24](#)
- [Active Calls Table, page 4-26](#)

## MOS Quality Chart

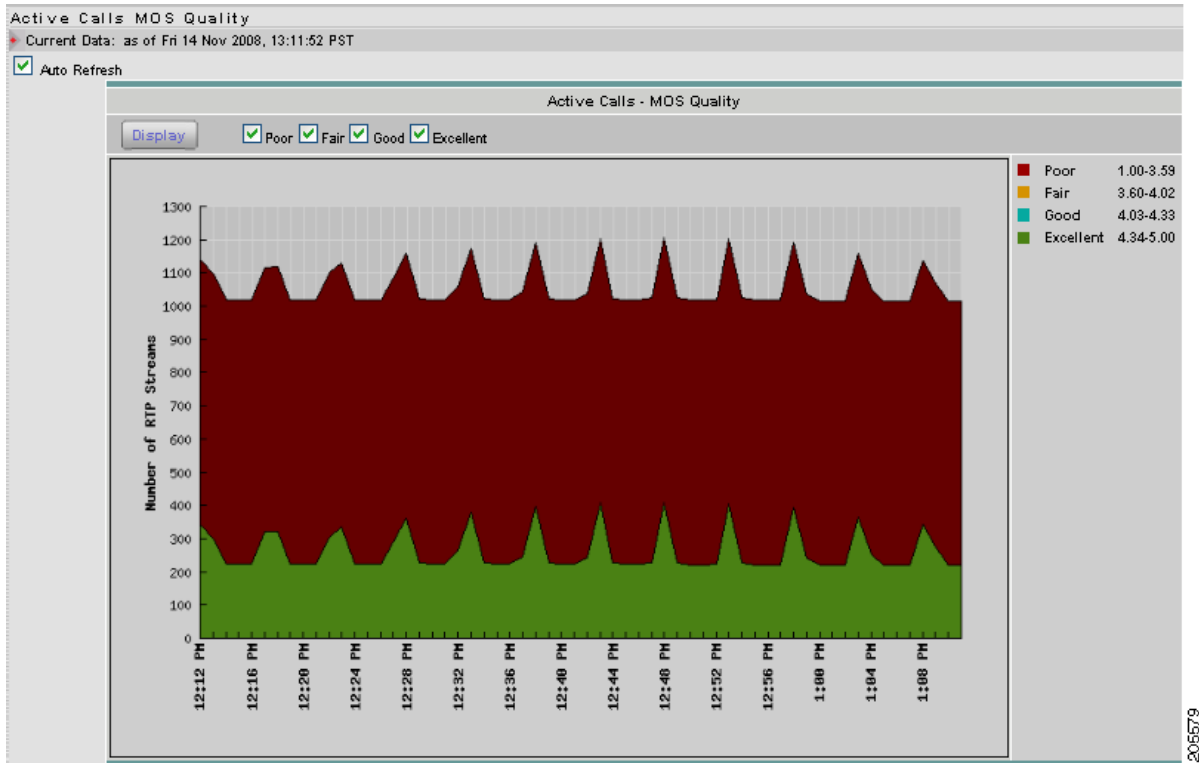
To view the Active Calls MOS Quality chart:

---

**Step 1** Choose **Monitor > Voice/Video**.

**Step 2** In the content menu under Active Calls, click **MOS Quality Chart**.

The Active Calls MOS Quality Chart displays. [Figure 4-16](#) shows an example of the Active Calls MOS Quality chart.

**Figure 4-16 Active Calls MOS Quality Chart**

The Active Calls MOS Quality Chart displays a graph that indicates the active calls and the time when they occurred. You can choose a specific quality (Poor, Fair, Good, or Excellent) of active call using the check boxes above the chart, then click **Display** to see one or more of that specific quality of active calls.

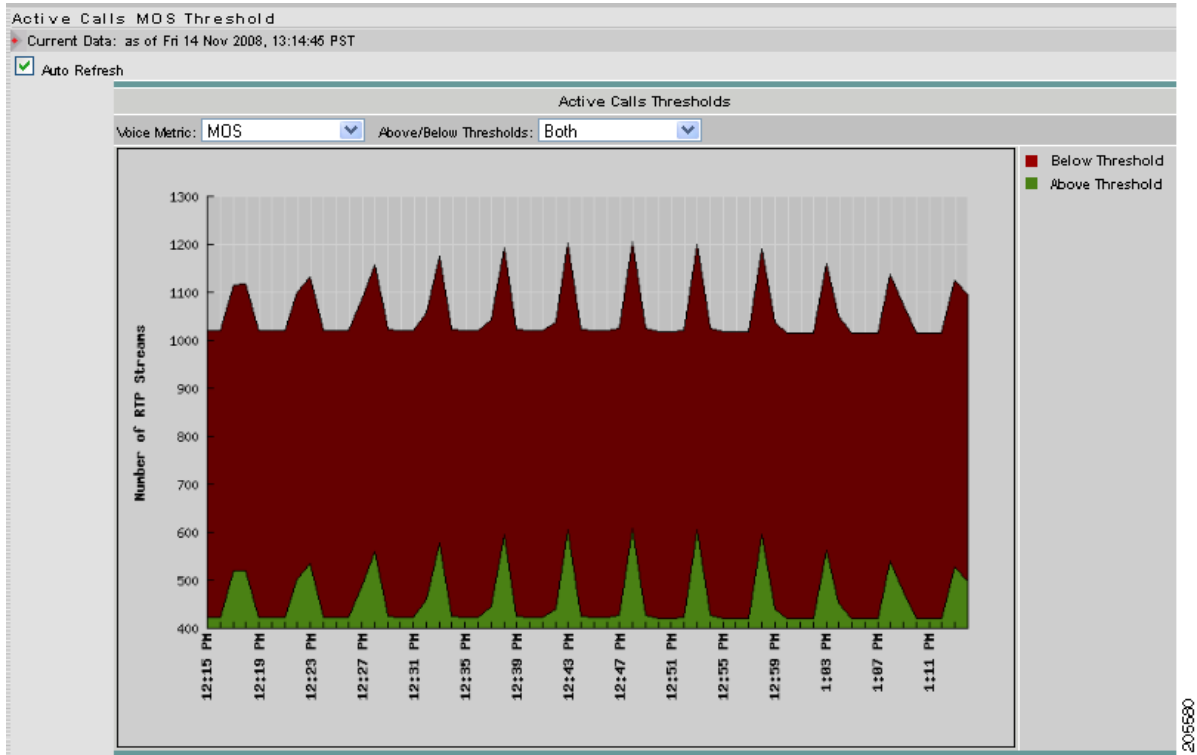
## Alarm Threshold Chart

To view the Active Calls Alarm Threshold chart:

- Step 1** Choose **Monitor > Voice/Video**.
- Step 2** In the content menu under Active Calls, click **Active Calls Thresholds Chart**.

The Active Calls MOS Quality Chart displays. [Figure 4-17](#) shows an example of the Active Calls Alarm Thresholds chart.

Use the Voice Metric pull-down menu to choose the voice quality metric to display. Use the Above/Below Thresholds pull-down metric to display calls above the threshold, below the threshold, or both above and below the threshold you set.

**Figure 4-17 Active Calls Alarm Thresholds Chart**

Active Calls Table

To view the Active Calls Table:

- Step 1 Choose **Monitor > Voice/Video**.
- Step 2 In the content menu under Active Calls, click **Table**.

The Active Calls Table displays. Figure 4-18 shows an example of the Active Calls table. The Active Calls Table (Figure 4-18) shows a list of all currently active calls.

Figure 4-18 Active Calls Table

Caller Number

Time Voice Enabled: 03-13-09 22:09:04 UTC Showing 1-1 of 1 records

| #  | Caller |               |       |                      | Called                |        |              |       | Worst Calculated     |                       |      |             |                  |                  | Start Time |           |                       |
|----|--------|---------------|-------|----------------------|-----------------------|--------|--------------|-------|----------------------|-----------------------|------|-------------|------------------|------------------|------------|-----------|-----------------------|
|    | Number | IP Address    | Alias | Reported Jitter (ms) | Reported Pkt Loss (%) | Number | IP Address   | Alias | Reported Jitter (ms) | Reported Pkt Loss (%) | MOS  | Jitter (ms) | Adj Pkt Loss (%) | Act Pkt Loss (%) |            | SSC (sec) | SOC (sec)             |
| 1. | 1003   | 172.20.104.28 | -     | 0                    | 3.03                  | 1004   | 172.20.104.8 | -     | 0                    | 3.57                  | 4.38 | 0.15        | 0                | 0                | 0          | 0         | 03-16-09 22:55:32 UTC |

Rows per page: 15  1 of 1

Select an item then take an action-->

Table 4-15 provides descriptions of the fields of the Active Calls Table.

  
**Note**

Some values in the Active 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 4-15, Active Calls Table](#), are based on a one-minute interval.

**Table 4-15 Active Calls Table**

| Field                    | Description                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------|
| <i>Caller</i>            |                                                                                                           |
| Number                   | Number of the phone placing the call.                                                                     |
| IP Address               | IP address of the phone placing the call.                                                                 |
| Alias                    | Alias name, MGCP endpoint ID, or SIP URI of the calling party phone.                                      |
| Reported Jitter (ms)     | Reported volume of jitter, an unwanted variation of one or more characteristics of voice traffic quality. |
| Reported Pkt Loss (%)    | Percentage of packet loss reported by the caller's phone.                                                 |
| <i>Called</i>            |                                                                                                           |
| Number                   | Number of the phone receiving the call.                                                                   |
| IP Address               | IP address of the phone receiving the call.                                                               |
| Alias                    | Alias name, MGCP endpoint ID, or SIP URI of the called party phone.                                       |
| Reported Jitter (ms)     | Jitter reported by the caller phone or called phone.                                                      |
| Reported Pkt Loss (%)    | Percentage of packet loss reported by the called phone.                                                   |
| <i>Worst Calculated</i>  |                                                                                                           |
| MOS                      | Worst calculated Mean Opinion of Score (MOS) for this call.                                               |
| Jitter                   | Worst calculated jitter value for this call.                                                              |
| Adjusted Packet Loss (%) | Worst calculated packet loss within a buffer emulation time (default is 45 ms) for this call.             |
| Actual Packet Loss (%)   | Worst calculated packet loss on the network for this call.                                                |
| SSC (sec)                | Worst calculated total number of seconds of severe concealment for this call.                             |
| SOC (sec)                | Worst calculated seconds of concealment for this call.                                                    |

## Terminated Calls

The Terminated Calls windows provide information about calls that have terminated. These windows provide a historical archive based on the parameters you choose on each window. You can view the following Terminated Calls windows:

- [Overview, page 4-28](#)
- [Worst N Calls, page 4-29](#)

### Overview

To view the Terminated Calls Overview window:

---

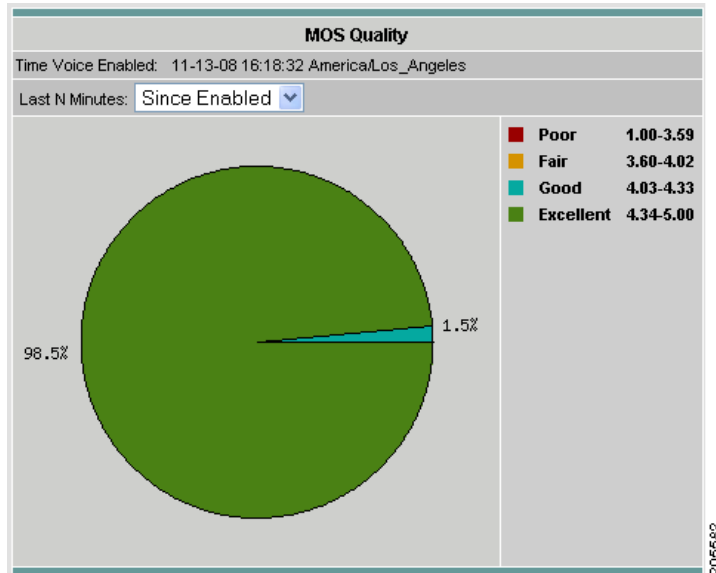
**Step 1** Choose **Monitor > Voice/Video**.

The Active Calls MOS Quality Chart displays.

**Step 2** In the Content Menu, click **Terminated Calls -- Overview**.

The Voice Quality Overview window displays. [Figure 4-19](#) shows an example of the Terminated Calls - Overview window. The Terminated Calls - Overview window is a pie chart that displays the various terminated call quality using colors for Poor, Fair, Good, and Excellent quality. Use the Last N Minutes pull-down menu to display the chart for the one of the following:

- 5 minutes
- 15 minutes
- 30 minutes
- 45 minute
- 60 minutes
- Since Enabled (Displays quality of calls since you enabled Voice monitoring.)

**Figure 4-19** Terminated Calls - Overview Window

## Worst N Calls

You can use the Worst N Calls window to view the poorest quality calls monitored by the NAM.

To view the worst quality calls:

**Step 1** Choose **Monitor > Voice/Video**.

The Voice Quality Overview window displays.

**Step 2** In the content menu, click **Worst N Calls**.

The Voice Worst N Calls window displays a list of the worst calls in tabular format. [Figure 4-20](#) shows an example of the Voice Worst N Calls window.

**Figure 4-20** Voice Worst N Calls Window

**Voice Worst N Calls**

★ **Current Data:** as of Thu 13 Nov 2008, 04:46:43 UTC

☒ Auto Refresh

**Worst Quality Calls by MOS**

Last N Minutes:  Metric:  Filter:

Time Voice Enabled: 11-13-08 00:02:58 UTC Showing 1-5 of 5 records

| #  | Caller                   |              |         | Called                   |              |         | Worst MOS | Start Time            | End Time              |
|----|--------------------------|--------------|---------|--------------------------|--------------|---------|-----------|-----------------------|-----------------------|
|    | Number                   | IP Address   | Alias   | Number                   | IP Address   | Alias   |           |                       |                       |
| 1. | sip:id00151@10.16.10.152 | 10.16.10.152 | id00151 | sip:id50151@10.15.10.152 | 10.15.10.152 | id50151 | 4.38      | 11-13-08 00:04:41 UTC | 11-13-08 00:09:41 UTC |
| 2. | sip:id00559@10.16.12.48  | 10.16.12.48  | id00559 | sip:id50559@10.15.12.48  | 10.15.12.48  | id50559 | 4.38      | 11-13-08 00:04:57 UTC | 11-13-08 00:09:57 UTC |
| 3. | sip:id00781@10.16.13.14  | 10.16.13.14  | id00781 | sip:id50781@10.15.13.14  | 10.15.13.14  | id50781 | 4.38      | 11-13-08 00:04:57 UTC | 11-13-08 00:09:57 UTC |
| 4. | sip:id00844@10.16.13.77  | 10.16.13.77  | id00844 | sip:id50844@10.15.13.77  | 10.15.13.77  | id50844 | 4.38      | 11-13-08 00:04:57 UTC | 11-13-08 00:09:57 UTC |
| 5. | sip:id00850@10.16.13.83  | 10.16.13.83  | id00850 | sip:id50850@10.15.13.83  | 10.15.13.83  | id50850 | 4.38      | 11-13-08 00:04:57 UTC | 11-13-08 00:09:57 UTC |

← Select an item then take an action →

205577

Table 4-16, [Worst N Calls Window](#), provides definitions of the calls that fall into the category based on the Last N Minutes, Metric, and the Filter you choose.

**Table 4-16** Worst N Calls Window

| Field         | Definition                                                                                           |
|---------------|------------------------------------------------------------------------------------------------------|
| <b>Caller</b> |                                                                                                      |
| Number        | Phone number of the caller                                                                           |
| IP Address    | IP Address of the callers phone                                                                      |
| Alias         | Name of Email Alias                                                                                  |
| <b>Called</b> |                                                                                                      |
| Number        | Phone number of the called phone.                                                                    |
| IP Address    | IP Address of the called phone                                                                       |
| Alias         | Name of Email Alias                                                                                  |
| Worst MOS     | Worst MOS of this call. This will be the metric you choose from the Display Metric pull-down window. |
| Start Time    | Start time of the call.                                                                              |
| End Time      | End time of the call.                                                                                |

## Viewing Known Phones

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

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

To view known phones:

**Step 1** Choose **Monitor > Voice/Video**.

The Voice Quality Overview window displays.

**Step 2** In the contents, click **Known Phones**.

The Phones Table displays. [Figure 4-21](#) shows an example of the Known Phones table.

**Figure 4-21 Known Phones Table**

**Phones**

Current Data: as of Thu 13 Nov 2008, 00:34:27 UTC

☒ Auto Refresh

Phone

Time Voice Enabled: 11-13-08 00:02:58 UTC Showing 1-15 of 848 records

| #   | Number                      | IP Address  | Alias   | Worst MOS | Worst Adj Pkt Loss (%) | Worst Act Pkt Loss (%) | Worst Jitter (ms) | Worst Severe Concealment (sec) | Worst Concealment (sec) |
|-----|-----------------------------|-------------|---------|-----------|------------------------|------------------------|-------------------|--------------------------------|-------------------------|
| 1.  | 1. sip:id00001@10.16.10.2   | 10.16.10.2  | id00001 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 2.  | 2. sip:id00021@10.16.10.22  | 10.16.10.22 | id00021 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 3.  | 3. sip:id00022@10.16.10.23  | 10.16.10.23 | id00022 | -         | -                      | -                      | -                 | -                              | -                       |
| 4.  | 4. sip:id00023@10.16.10.24  | 10.16.10.24 | id00023 | 4.38      | 0.00                   | 0.00                   | 0.02              | 0                              | 0                       |
| 5.  | 5. sip:id00024@10.16.10.25  | 10.16.10.25 | id00024 | -         | -                      | -                      | -                 | -                              | -                       |
| 6.  | 6. sip:id00025@10.16.10.26  | 10.16.10.26 | id00025 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 7.  | 7. sip:id00026@10.16.10.27  | 10.16.10.27 | id00026 | 4.38      | 0.00                   | 0.00                   | 0.03              | 0                              | 0                       |
| 8.  | 8. sip:id00027@10.16.10.28  | 10.16.10.28 | id00027 | -         | -                      | -                      | -                 | -                              | -                       |
| 9.  | 9. sip:id00028@10.16.10.29  | 10.16.10.29 | id00028 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 10. | 10. sip:id00029@10.16.10.30 | 10.16.10.30 | id00029 | -         | -                      | -                      | -                 | -                              | -                       |
| 11. | 11. sip:id00030@10.16.10.31 | 10.16.10.31 | id00030 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 12. | 12. sip:id00031@10.16.10.32 | 10.16.10.32 | id00031 | 4.38      | 0.00                   | 0.00                   | 0.02              | 0                              | 0                       |
| 13. | 13. sip:id00032@10.16.10.33 | 10.16.10.33 | id00032 | -         | -                      | -                      | -                 | -                              | -                       |
| 14. | 14. sip:id00033@10.16.10.34 | 10.16.10.34 | id00033 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |
| 15. | 15. sip:id00034@10.16.10.35 | 10.16.10.35 | id00034 | 4.38      | 0.00                   | 0.00                   | 0.06              | 0                              | 0                       |

Rows per page: 15  Go

Go to page: 1 of 57

Select an item then take an action -->

[Table 4-17](#) describes the fields of the Known [Phones Table](#).

**Table 4-17**      **Phones Table**

| Field                          | Description                                                    |
|--------------------------------|----------------------------------------------------------------|
| Number                         | Phone number or MGCP endpoint.                                 |
| IP Address                     | IP address of the phone.                                       |
| Alias                          | Alias name or MGCP endpoint ID of the phone.                   |
| Worst MOS                      | Worst MOS quality for this call.                               |
| Worst Adj Pkt Loss %           | Worst adjusted packets loss percentage on the phone.           |
| Worst Act Pkt Loss %           | Worst actual packets loss percentage on the phone.             |
| Worst Jitter                   | Worst jitter on the phone (in milliseconds) for selected call. |
| Worst Severe Concealment (sec) | Worst severe concealment for this call.                        |
| Worst Concealment (sec)        | Worst concealment for this call.                               |

**Tip**

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

## Viewing RTP Stream Traffic

To view RTP Stream Traffic, choose **Monitor > Voice/Video**, then choose **RTP Stream Traffic** in the content menu. The [RTP Stream Traffic Window](#) (Figure 4-22) displays.

**Note**

NAM 4.1 does not support IPv6 for RTP stream analysis.

**Figure 4-22 RTP Stream Traffic Window**

**RTP Stream Traffic**

Current Data: as of Wed 12 Nov 2008, 22:24:01 UTC

☒ Auto Refresh

Source Address

Showing 1-15 of 800 records

| #   | Source Addr : Port   | Dest Addr : Port     | Payload Type | SSRC   | Act Pkt Loss /million | Worst MOS | Adj Pkt Loss (%) | Jitter (ms) | Total SSC | Status   | Start Time            |
|-----|----------------------|----------------------|--------------|--------|-----------------------|-----------|------------------|-------------|-----------|----------|-----------------------|
| 1.  | 10.15.10.1 : 10236   | 10.16.10.1 : 10240   | G711Alaw_64k | 112363 | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:17:00 UTC |
| 2.  | 10.15.10.1 : 10244   | 10.16.10.1 : 10246   | G711Alaw_64k | 169225 | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:08:00 UTC |
| 3.  | 10.15.10.10 : 10192  | 10.16.10.10 : 10192  | G711Alaw_64k | 66316  | 0                     | 4.38      | 0.00             | 0.05        | 0         | Inactive | 11-12-08 19:19:00 UTC |
| 4.  | 10.15.10.10 : 10194  | 10.16.10.10 : 10194  | G711Alaw_64k | 148892 | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:06:17 UTC |
| 5.  | 10.15.10.100 : 10188 | 10.16.10.100 : 10188 | G711Alaw_64k | 127114 | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:17:00 UTC |
| 6.  | 10.15.10.100 : 10190 | 10.16.10.100 : 10190 | G711Alaw_64k | 1937   | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:06:17 UTC |
| 7.  | 10.15.10.101 : 10066 | 10.16.10.101 : 10066 | G711Alaw_64k | 17969  | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:06:08 UTC |
| 8.  | 10.15.10.101 : 10070 | 10.16.10.101 : 10064 | G711Alaw_64k | 34907  | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:16:14 UTC |
| 9.  | 10.15.10.102 : 10278 | 10.16.10.102 : 10280 | G711Alaw_64k | 147179 | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:16:27 UTC |
| 10. | 10.15.10.102 : 10286 | 10.16.10.102 : 10286 | G711Alaw_64k | 147049 | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:06:22 UTC |
| 11. | 10.15.10.103 : 10348 | 10.16.10.103 : 10350 | G711Alaw_64k | 33739  | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:17:00 UTC |
| 12. | 10.15.10.103 : 10352 | 10.16.10.103 : 10352 | G711Alaw_64k | 86231  | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:07:00 UTC |
| 13. | 10.15.10.104 : 10292 | 10.16.10.104 : 10294 | G711Alaw_64k | 95808  | 0                     | 4.38      | 0.00             | 0.02        | 0         | Inactive | 11-12-08 19:08:00 UTC |
| 14. | 10.15.10.104 : 10314 | 10.16.10.104 : 10318 | G711Alaw_64k | 92474  | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:16:30 UTC |
| 15. | 10.15.10.105 : 10270 | 10.16.10.105 : 10270 | G711Alaw_64k | 137107 | 0                     | 4.38      | 0.00             | 0.04        | 0         | Inactive | 11-12-08 19:16:26 UTC |

Rows per page: 15  1 of 54

Select an item then take an action -->

205576

Table 4-18 describes the fields of the RTP Stream Traffic window.

**Table 4-18 RTP Stream Traffic Window Fields**

| Field                     | Description                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Address: Port      | Source address and port of the RTP stream traffic                                                                                                |
| Destination Address: Port | Destination address and port of the RTP stream traffic                                                                                           |
| RTP Payload Type          | Payload type as seen in the RTP stream                                                                                                           |
| SSRC Value                | Synchronization Source of the RTP packet                                                                                                         |
| Act Pkt Loss/million      | Actual packet loss rate (divided by 1,000,000 for ease of viewing)                                                                               |
| Worst MOS                 | Worst (lowest) MOS score for this RTP stream                                                                                                     |
| Adjusted Packet Loss      | Adjusted packet loss percentage for this RTP stream                                                                                              |
| Jitter (ms)               | Average jitter value (ms) of this RTP stream                                                                                                     |
| Total SSC                 | Sum of all seconds of severe concealment value for this RTP stream                                                                               |
| Status                    | <ul style="list-style-type: none"> <li>Active indicates an active RTP stream</li> <li>Inactive indicates an RTP stream that has ended</li> </ul> |
| Start Time                | Start time for this RTP stream                                                                                                                   |

# Monitoring Hosts

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

To view hosts data:

**Step 1** Click **Monitor** > **Hosts**.

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

- [Viewing the Network Hosts Current Rates Table, page 4-34](#)
- [Viewing the Network Hosts Top N Chart, page 4-37](#)
- [Viewing the Network Hosts Cumulative Data Table, page 4-38](#)

**Step 2** To view the data based on the host MAC addresses, click **MAC Stations** in the contents.



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

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

- [Viewing the MAC Stations Current Rates Table, page 4-39](#)
- [Viewing the MAC Stations Top N Chart, page 4-40](#)
- [Viewing the MAC Stations Cumulative Data Table, page 4-41](#)

## Viewing the Network Hosts Current Rates Table

The Network Current Rates table enables you to view the various data collected for each host. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Network Current Rates table:

**Step 1** Click **Monitor** > **Hosts**.

The [Network Hosts Current Rates Table \(Table 4-19\)](#) displays by default.

**Table 4-19** *Network Hosts Current Rates Table*

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



- Step 2** Choose a data source to monitor from the Data Source list.
- Step 3** Enter an address to filter in the Address text box, then click **Filter**.  
The specified address displays.

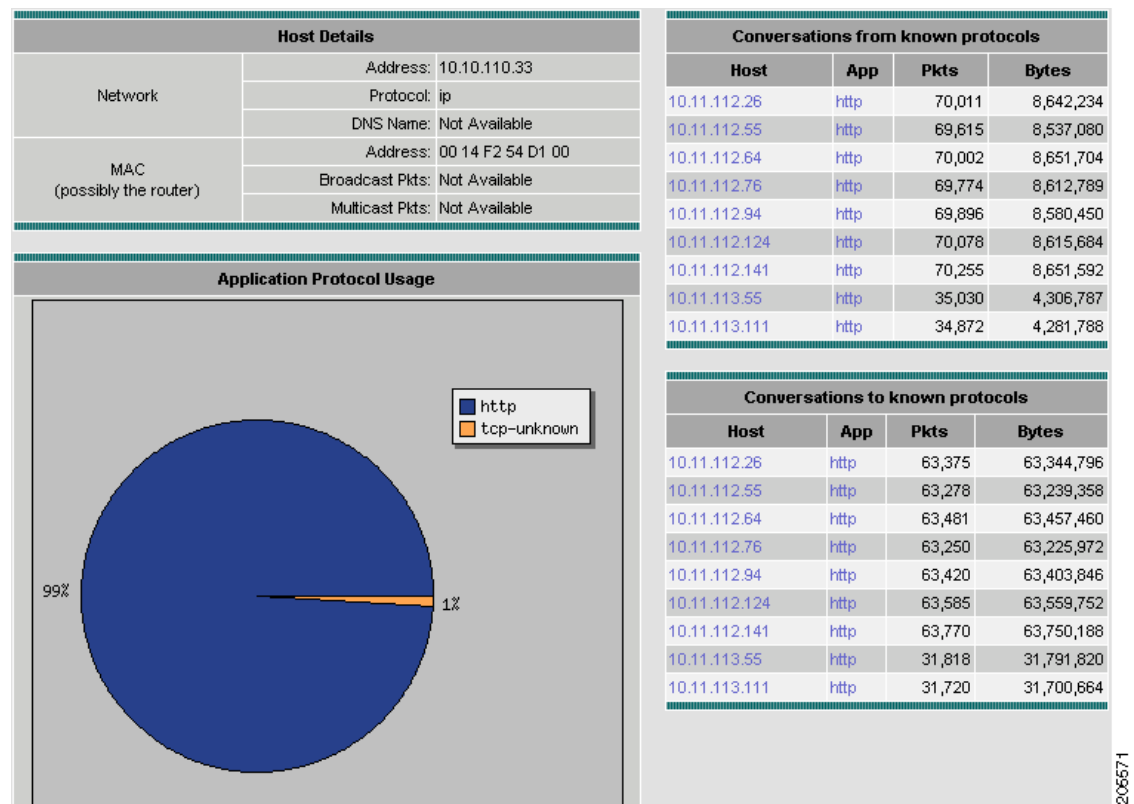
**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing Network Host Details

To view details for a specific host, click on the address in the Address column of the Network Hosts table, or click to select a specific host and click **Details**. The Network Hosts Detail Window displays, as shown in [Figure 4-23](#).

**Figure 4-23** Network Hosts Detail Window



- Host Details—Displays detailed information for the host.
- Application Protocol Usage Chart—Displays the application protocol usage for the host in graphical format.

- Conversations From Known Protocols—Displays known conversations and statistics *from* the specified host to other hosts on the network using known protocols.
- Conversations To Known Protocols—Displays known conversations and statistics *to* the specified host from other hosts on the network using known protocols.

**Note**

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

**Tips**

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

## Capturing Network Host Data from the Network Host Table

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

Choose the host from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

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

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).

**Note**

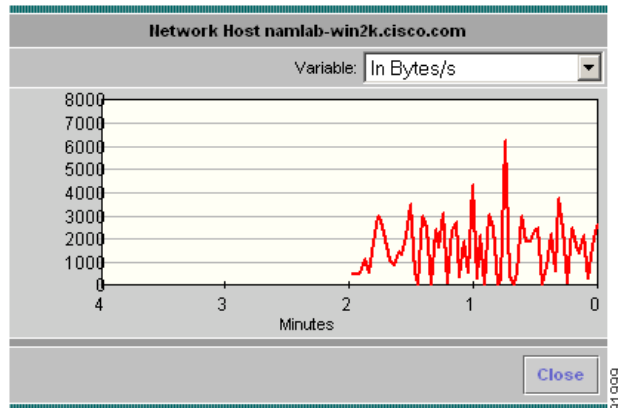
The Capture button is disabled for NetFlow-based data sources.

## Viewing Real-Time Traffic Statistics from the Hosts Table

You can view real-time traffic statistics in a graphical format for a specific host. Choose the host from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-24](#)) displays.

**Note**

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

**Figure 4-24 Real-Time Graph**

## Viewing Reports from the Network Hosts Table

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

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

## Viewing the Network Hosts Top N Chart

The Network Hosts Top N Chart enables you to view various data for the TopN hosts in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the Network Hosts Top N Chart:

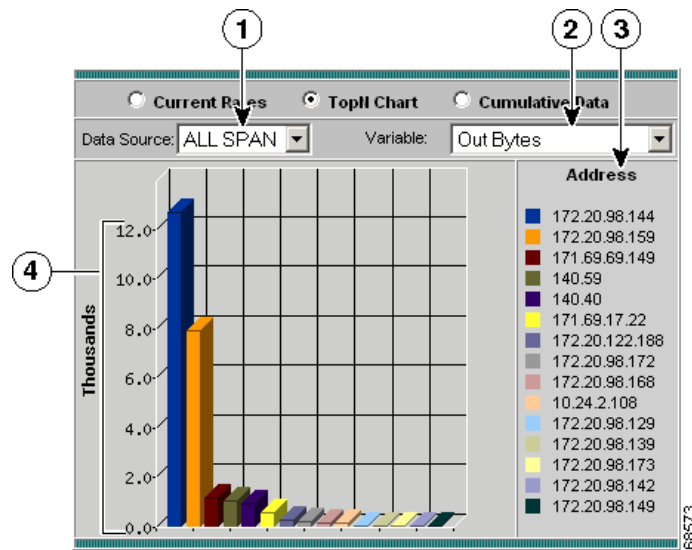
---

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

**Step 2** Click the TopN Chart radio button.

The [Top N Network Hosts Chart](#) (Figure 4-25) displays.

Figure 4-25 Top N Network Hosts Chart



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

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

**Step 4** Choose one of the following from the Sort Option list:

- In Pkts—Displays the number of input packets.
- Out Pkts—Displays the number of output packets.
- In Bytes—Displays the number of input bytes.
- Out Bytes—Displays the number of output bytes.
- Non Unicast Pkts—Displays the number of non-unicast packets.



**Tip**

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

## Viewing the Network Hosts Cumulative Data Table

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

To view the Network Hosts Cumulative Data Table:

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

**Step 2** Click the Cumulative Data radio button.

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

**Table 4-20 Network Hosts Cumulative Data Table**

| Field       | Description                                                           |
|-------------|-----------------------------------------------------------------------|
| Address     | Network address of the host.                                          |
| Via         | Protocol being monitored.                                             |
| In Pkts     | Total number of input packets over the last interval.                 |
| Out Pkts    | Total number of output packets over the last interval.                |
| In Bytes    | Total number of input bytes over the last interval.                   |
| Out Bytes   | Total number of output bytes over the last interval.                  |
| Non Unicast | Total number of non-unicast broadcast packets over the last interval. |

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

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



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing the MAC Stations Current Rates Table



**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The MAC Stations Current Rates table enables you to view the various data collected for each host. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the MAC Stations Current Rates table:

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

**Step 2** Click the Current Rates Table radio button.

The [MAC Stations Table](#) (Table 4-21) displays.

**Table 4-21 MAC Stations Table**

| Field        | Description                                        |
|--------------|----------------------------------------------------|
| Address      | MAC address of the host.                           |
| In Packets/s | Number of packets received by the host per second. |

**Table 4-21**      **MAC Stations Table (continued)**

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

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

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

The specified address displays.

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing the MAC Stations Top N Chart

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

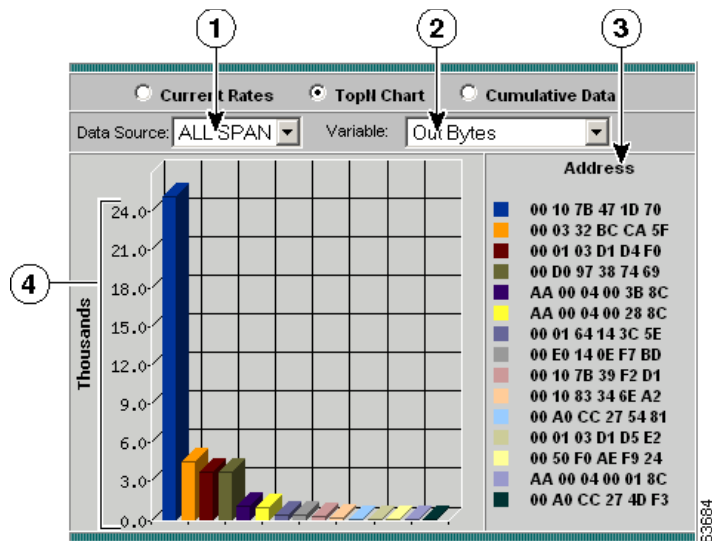
The MAC Stations Top N chart enables you to view the various data collected for each host in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the MAC Stations Top N chart:

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

**Step 2**      Click the TopN Chart radio button.

The [Top N MAC Stations Chart \(Figure 4-26\)](#) displays.

**Figure 4-26 Top N MAC Stations Chart**

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

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

**Step 4** Choose one of the following from the Sort Option list:

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

**Tip**

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

## Viewing the MAC Stations Cumulative Data Table

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

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

To view the MAC Stations Cumulative Data Table:

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

**Step 2** Click the Cumulative Data radio button.

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

**Table 4-22** *MAC Stations Cumulative Data Table*

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

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

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

The specified address displays.



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing Conversations Data

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

NAM provides three menu options for monitoring conversations:

- [Viewing Network Hosts, page 4-43](#)
- [Viewing the Application Hosts, page 4-47](#)
- [Viewing MAC Stations, page 4-48](#)



## Viewing Network Hosts

The Network Hosts Conversations table displays statistics between pairs of IP addresses *talking* to each other. The statistics pertain to all packets between the hosts, regardless of protocol or application. There are three options you can use to display the Network Hosts Conversations table:

- [Viewing the Network Host Conversations Current Rates Table, page 4-43](#)
- [Viewing the Network Host Conversations Top N Chart, page 4-45](#)
- [Viewing the Network Host Conversations Cumulative Data Table, page 4-46](#)

### Viewing the Network Host Conversations Current Rates Table

The Network Host Conversations Current Rates table enables you to view the number of packets and bytes collected for each host conversation. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Network Host Conversations Current Rates table:

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

**Table 4-23 Network Host Conversations Current Rates Table**

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

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



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing Network Host Conversation Details

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

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



### Note

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

## Capturing Network Host Conversation Data from the Network Host Conversations Table

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

Choose the conversation from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

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

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).



### Note

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

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

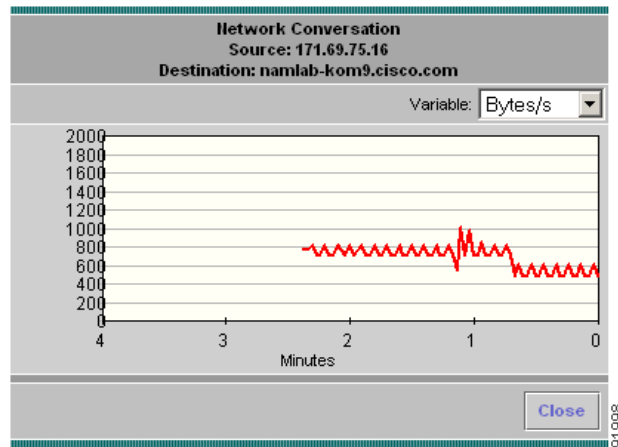
You can view real-time traffic statistics in a graphical format for a specific host conversation.

Choose the conversation from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-24](#)) displays.



### Note

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

**Figure 4-27 Real-Time Graph**

### Viewing Reports from the Network Host Conversations Table

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

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

### Viewing the Network Host Conversations Top N Chart

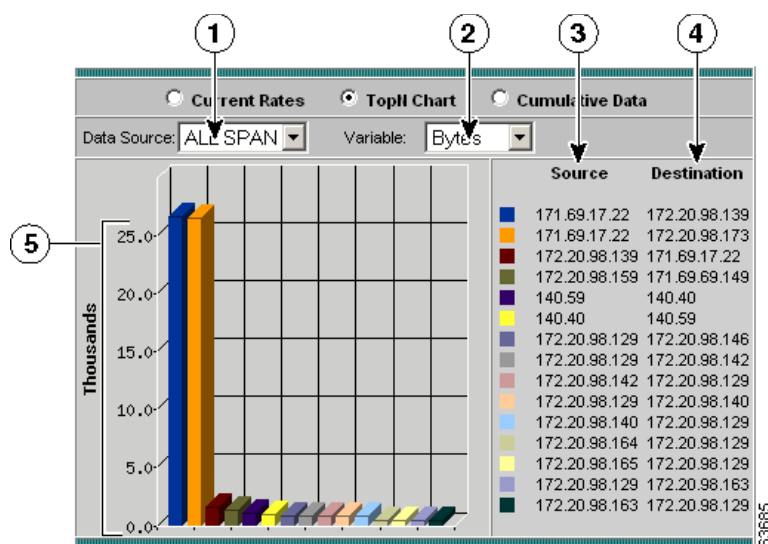
The Top N Network Host Conversations Chart enables you to view the number of packets and bytes collected for the Top N network host conversations in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the Top N Network Host Conversations chart:

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

**Step 2** Click the TopN Chart radio button.

The [Top N Network Host Conversations Chart](#) (Figure 4-28) displays.

**Figure 4-28 Top N Network Host Conversations Chart**

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

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

**Step 4** Choose one of the following from the Variable list:

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

## Viewing the Network Host Conversations Cumulative Data Table

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

To view the Network Host Conversations Cumulative Data table:

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

The Network Hosts Conversations Current Rates table displays.

**Step 2** Click the **Cumulative Data** radio button.

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

**Table 4-24 Network Host Conversations Cumulative Data Table**

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

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

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

The specified address displays.

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

**Tip**

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

## Viewing Network Host Conversation Details

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

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

## Viewing the Application Hosts

The Application Hosts table enables you to view the number of packets and bytes collected for each host conversation. You can use this data to identify application hosts conversations and port numbers that can help you design access control lists on switches and routers to allow or block certain ports between certain hosts. The data displayed is the number of packets and bytes collected per second over the last time interval.

To view the Application Hosts table, click **Monitor > Conversations > Application Hosts**. [Figure 4-29](#) shows an example of the Application Hosts table.

**Figure 4-29 Application Hosts Table**

**Application Hosts**  
 Current Data: as of Mon 30 Apr 2007, 20:44:03 UTC

Application Hosts

Data Source: ALL SPAN Server Filter Clear

\* denotes server

| Source   | Destination | Application | Port      | Packets | Bytes    |
|----------|-------------|-------------|-----------|---------|----------|
| 1.1.1.1  | 192.6.2.1*  | ndmp        | TCP-10000 | 108394  | 17559828 |
| 1.1.1.2  | 192.6.2.2*  | tcp-unknown | TCP-10001 | 108394  | 17559828 |
| 1.1.1.3  | 192.6.2.3*  | etheric     | TCP-10002 | 108395  | 17559990 |
| 1.1.1.4  | 192.6.2.4*  | tcp-10003   | TCP-10003 | 108396  | 17560152 |
| 1.1.1.5  | 192.6.2.5*  | tcp-10004   | TCP-10004 | 108396  | 17560152 |
| 1.1.1.6  | 192.6.2.6*  | tcp-10005   | TCP-10005 | 108396  | 17560152 |
| 1.1.1.7  | 192.6.2.7*  | tcp-10006   | TCP-10006 | 108396  | 17560152 |
| 1.1.1.8  | 192.6.2.8*  | tcp-10007   | TCP-10007 | 108394  | 17559828 |
| 1.1.1.9  | 192.6.2.9*  | tcp-10008   | TCP-10008 | 108394  | 17559828 |
| 1.1.1.10 | 192.6.2.10* | tcp-10009   | TCP-10009 | 108394  | 17559828 |
| 1.1.1.11 | 192.6.2.11* | tcp-10010   | TCP-10010 | 108394  | 17559828 |
| 1.1.1.12 | 192.6.2.12* | tcp-10011   | TCP-10011 | 108397  | 17560314 |
| 1.1.1.13 | 192.6.2.13* | tcp-10012   | TCP-10012 | 108395  | 17559990 |
| 1.1.1.14 | 192.6.2.14* | tcp-10013   | TCP-10013 | 108396  | 17560152 |
| 1.1.1.15 | 192.6.2.15* | tcp-10014   | TCP-10014 | 108396  | 17560152 |

Rows per page: 15 Units: Bytes Start Prev Next 211867

Table 4-25 lists the fields of the Application Hosts Conversations table.

**Table 4-25 Application Hosts Conversations**

| Field       | Description                                                                        |
|-------------|------------------------------------------------------------------------------------|
| Source      | Source address of the conversation                                                 |
| Destination | Destination address of the conversation                                            |
| Application | Application used in conversation                                                   |
| Port        | Port used for the conversation.                                                    |
| Packets     | Total number of packets collected over the last time interval for the conversation |
| Bytes       | Total number of bytes collected over the last time interval for the conversation   |

## Viewing MAC Stations

The Media Access Control (MAC) Stations Conversations table displays statistics of conversations between two MAC addresses instead of two IP addresses.

- [Viewing the MAC Station Conversations Current Rates Table, page 4-49](#)
- [Viewing the MAC Conversations Top N Chart, page 4-49](#)
- [Viewing the MAC Station Conversations Cumulative Data Table, page 4-51](#)

## Viewing the MAC Station Conversations Current Rates Table

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The MAC Station Conversations Current Rates table enables you to view the number of packets and bytes collected for each host conversation. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the MAC Station Conversations Current Rates table:

- Step 1** In the contents, click **Monitor > Conversations > MAC Stations**.  
The [MAC Station Conversations Current Rates Table \(Table 4-26\)](#) displays.

**Table 4-26** *MAC Station Conversations Current Rates Table*

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

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

- Step 3** To view data for a specific address, enter the full or partial MAC address in the Address text box, then click **Filter**.

Any matching addresses are displayed.

**Tip**

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

## Viewing the MAC Conversations Top N Chart

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The Top N MAC Station Conversations Chart enables you to view the number of packets and bytes collected for the Top N MAC station conversations in a graphical format. The data displayed is the number of packets and bytes collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

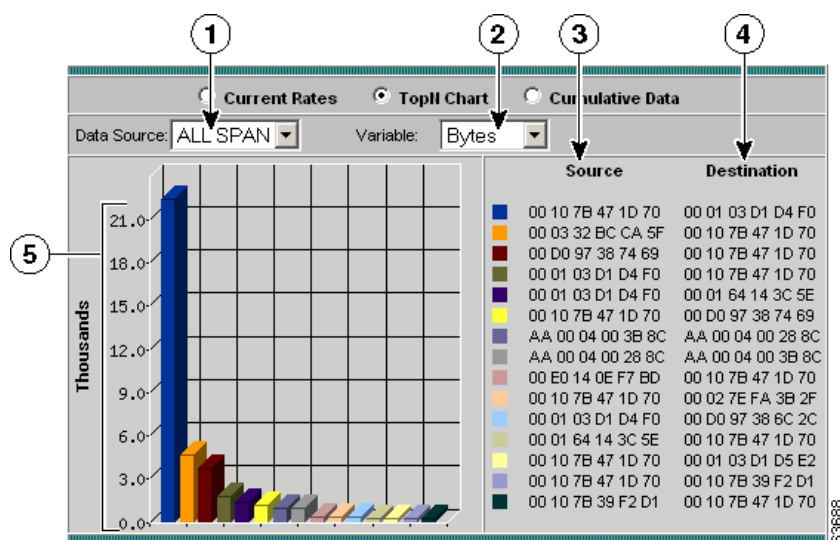
To view the Top N MAC Station Conversations chart:

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

**Step 2** Click the TopN Chart radio button.

The [Top N MAC Station Conversations Chart](#) (Figure 4-30) displays.

**Figure 4-30 Top N MAC Station Conversations Chart**



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

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

**Step 4** Choose one of the following from the Variable list:

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



**Tip**

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



## Viewing the MAC Station Conversations Cumulative Data Table


**Note**

This section does not apply to NM-NAM or NME-NAM devices.

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

To view the MAC Station Conversations Cumulative Data table:

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

**Step 2** Click the Cumulative Data radio button.

The [MAC Station Conversations Cumulative Data Table](#) (Table 4-27) displays.

**Table 4-27** *MAC Station Conversations Cumulative Data Table*

| Field       | Description                                                                         |
|-------------|-------------------------------------------------------------------------------------|
| Source      | Source MAC address of the conversation.                                             |
| Destination | Destination MAC address of the conversation.                                        |
| Pkts        | Total number of packets collected over the last time interval for the conversation. |
| Bytes       | Total number of bytes collected over the last time interval for the conversation.   |
| Errors      | Total number of errors collected over the last time interval for the conversation.  |

**Step 3** Choose the data source from the Data Source list.

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

The specified address displays.

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


**Tip**

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

## Viewing VLAN Data


**Note**

This section does not apply to NM-NAM or NME-NAM devices.

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

**Note**

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

To view VLAN data:

**Step 1** Click **Monitor** > **VLAN**.

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

- [Viewing the VLAN Traffic Statistics Current Rates Table, page 4-52.](#)
- [Viewing the VLAN Traffic Statistics Top N Chart, page 4-53.](#)
- [Viewing VLAN Traffic Statistics Cumulative Data Table, page 4-54.](#)

**Step 2** To view the VLAN data based on VLAN priority (COS) statistics, click **VLAN Priority (COS) Statistics** in the contents.

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

- [Viewing the VLAN Priority \(COS\) Statistics Current Rates Table, page 4-55.](#)
- [Viewing the VLAN Priority \(COS\) Statistics Top N Chart, page 4-56.](#)
- [Viewing the VLAN Priority \(COS\) Statistics Cumulative Data Table, page 4-57.](#)

## Viewing the VLAN Traffic Statistics Current Rates Table

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The VLAN Traffic Statistics Current Rates table enables you to view various data collected for each VLAN ID. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94.](#)

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

The [VLAN Traffic Statistics Table \(Table 4-28\)](#) displays.

**Table 4-28** *VLAN Traffic Statistics Table*

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

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing Reports from the VLAN Traffic Statistics Table

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

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

## Viewing the VLAN Traffic Statistics Top N Chart

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

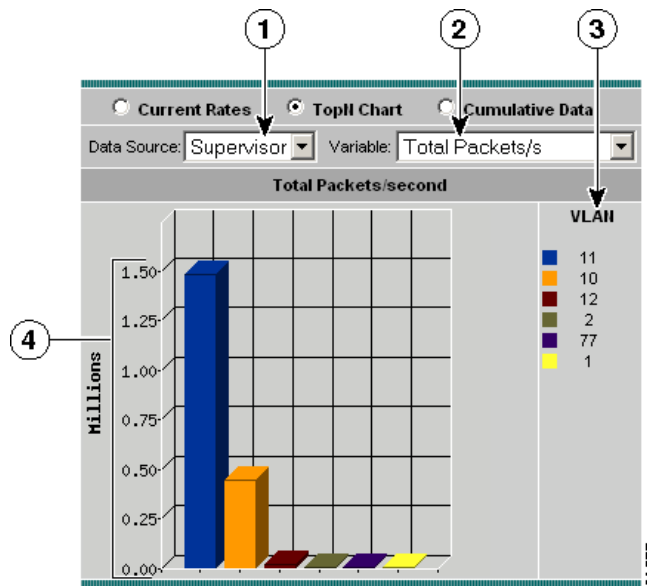
The Top N VLAN Traffic Statistics Chart enables you to view the various data collected for the top N VLAN IDs in a graphical format. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences”](#) section on page 3-94.

To view the Top N VLAN Traffic Statistics chart:

**Step 1** Click the TopN Chart radio button.

The [Top N VLAN Traffic Statistics Chart](#) (Figure 4-31) displays.

**Figure 4-31 Top N VLAN Traffic Statistics Chart**



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

**Step 2** Choose the data source from the Data Source list.

**Step 3** Choose one of the following from the Variable list:

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



**Tip**

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

## Viewing VLAN Traffic Statistics Cumulative Data Table



**Note**

This section does not apply to NM-NAM or NME-NAM devices.

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

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

The [VLAN Traffic Statistics Cumulative Data Table](#) (Table 4-29) displays.

**Table 4-29 VLAN Traffic Statistics Cumulative Data Table**

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

**Tip**

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

## Viewing the VLAN Priority (COS) Statistics Current Rates Table

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The VLAN Priority (COS) Statistics Current Rates table enables you to view user priority distributions per data source. The displayed information represents the data collected each second during the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the VLAN Priority (COS) Statistics Current Rates table:

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

The [VLAN Priority \(COS\) Statistics Current Rates Table](#) (Table 4-30) displays.

**Table 4-30 VLAN Priority (COS) Statistics Current Rates Table**

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

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

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

# Viewing the VLAN Priority (COS) Statistics Top N Chart



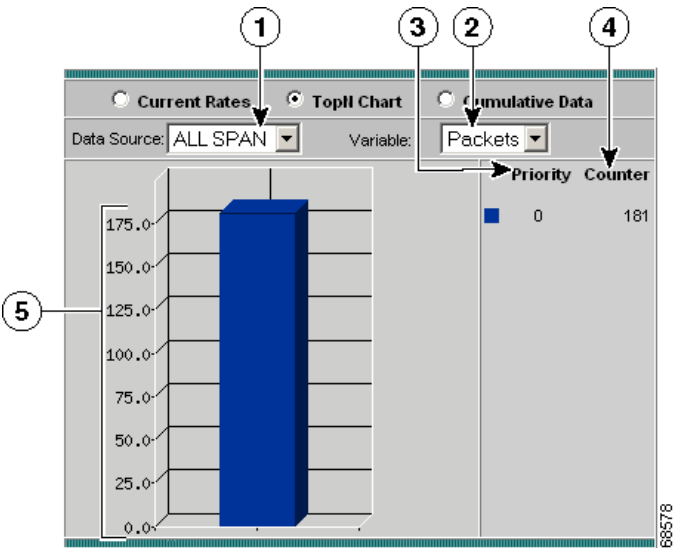
**Note** This section does not apply to NM-NAM or NME-NAM devices.

The Top N VLAN Priority (COS) Statistics Chart enables you to view user priority distributions per data source in a graphical format. The information displayed represents the data collected *per second* over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Top N VLAN Priority (COS) Statistics chart:

- Step 1** In the contents, click **Priority (COS) Statistics**.
- Step 2** Click the TopN Chart radio button.  
The [Top N VLAN Priorities \(COS\) Statistics Chart](#) (Figure 4-32) displays.

**Figure 4-32 Top N VLAN Priorities (COS) Statistics Chart**



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

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

**Tip**

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

## Viewing the VLAN Priority (COS) Statistics Cumulative Data Table

**Note**

This section does not apply to NM-NAM or NME-NAM devices.

The VLAN Priority (COS) Statistics Cumulative Data table enables you to view user priority distributions per data source. The information displayed represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the VLAN Priority (COS) Statistics Cumulative Data table:

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

**Step 2** Click the Cumulative Data radio button.

The [VLAN Priority \(COS\) Statistics Cumulative Data Table](#) (Table 4-31) displays.

**Table 4-31 VLAN Priority (COS) Statistics Cumulative Data Table**

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

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

**Tip**

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

## Viewing DiffServ Data

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

**Note**

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

To view DiffServ data:

**Step 1** Click **Monitor** > **DiffServ**.

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

- [Viewing the DiffServ Traffic Statistics Current Rates Table, page 4-58.](#)
- [Viewing the DiffServ Traffic Top N Chart, page 4-59.](#)
- [Viewing the DiffServ Traffic Statistics Cumulative Data Table, page 4-60.](#)

**Step 2** To view the DiffServ data based on the application statistics, click **Application Stats** in the contents.

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

- [Viewing the DiffServ Application Statistics Current Rates Table, page 4-61.](#)
- [Viewing the DiffServ Application Statistics Top N Chart.](#)
- [Viewing the DiffServ Application Statistics Cumulative Data Table, page 4-64.](#)

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

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

You can select a radio button for:

- [Viewing the DiffServ Host Statistics Current Rates Table, page 4-65.](#)
- [Viewing the DiffServ Host Statistics Top N Chart, page 4-67.](#)
- [Viewing the DiffServ Host Statistics Cumulative Data Table, page 4-68.](#)

## Viewing the DiffServ Traffic Statistics Current Rates Table

To view the DiffServ Traffic Statistics Current Rates table:

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

The DiffServ Traffic Statistics Current Rates Table ([Table 4-32](#)) displays.

**Table 4-32** *DiffServ Traffic Statistics Current Rates Table*

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

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

The specified aggregation group displays.



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

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

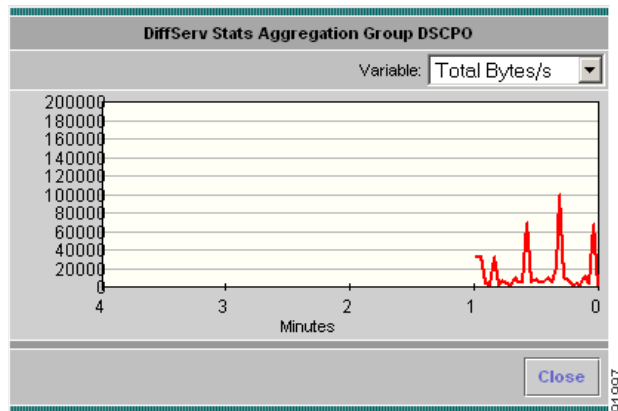
You can view real-time traffic statistics in a graphical format for a specific aggregation group in the DiffServ Traffic Statistics table.

Choose the aggregation group from the table, then click **Real-Time**. The Real-Time Graph (Figure 4-24) displays.

**Note**

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

**Figure 4-33 Real-Time Graph**



## Viewing Reports from the DiffServ Traffic Statistics Table

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

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

## Viewing the DiffServ Traffic Top N Chart

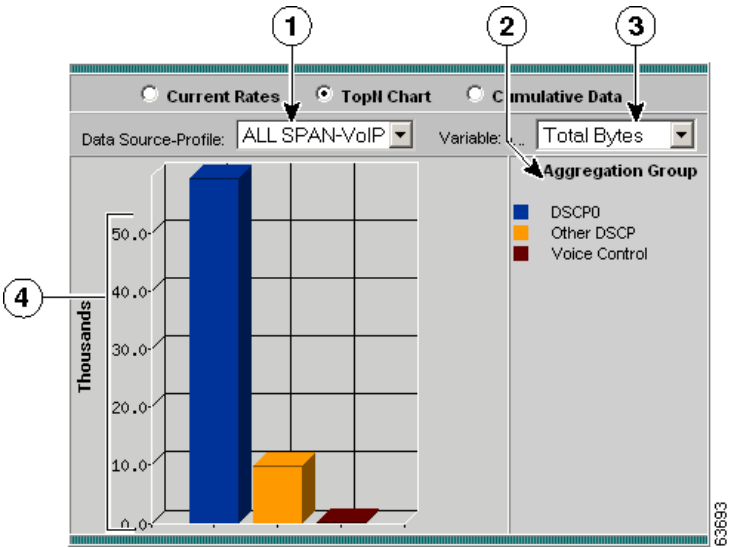
To view the DiffServ Traffic Top N chart:

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

**Step 2** Click the TopN Chart radio button.

The [Top N DiffServ Aggregation Group Chart](#) (Figure 4-34) displays.

Figure 4-34 Top N DiffServ Aggregation Group Chart



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

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



Tip

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

## Viewing the DiffServ Traffic Statistics Cumulative Data Table

To view the DiffServ Traffic Statistics Cumulative Data table:

- Step 1** In the contents, click **Traffic Stats**.
- Step 2** Click the Cumulative Data radio button.
- The [DiffServ Traffic Statistics Cumulative Data](#) (Table 4-33) displays.

**Table 4-33 DiffServ Traffic Statistics Cumulative Data**

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

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

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

**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing the DiffServ Application Statistics Current Rates Table

To view the DiffServ Application Statistics Current Rates table:

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

**Step 2** Click the Current Rates Table radio button.

The [DiffServ Application Statistics Current Rates](#) (Table 4-34) table displays.

**Table 4-34 DiffServ Application Statistics Current Rates**

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

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

**Step 4** Choose the aggregation group from the Aggregation list.

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

The specified protocol displays.

**Tip**

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

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

## Displaying Application Conversation Details From Application Statistics Table

To view the Application Conversations details table, click the protocol name in the Protocol Name column. The [Application Conversations Table](#) (Table 4-35) displays.

**Table 4-35**      *Application Conversations Table*

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



### Tip

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

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

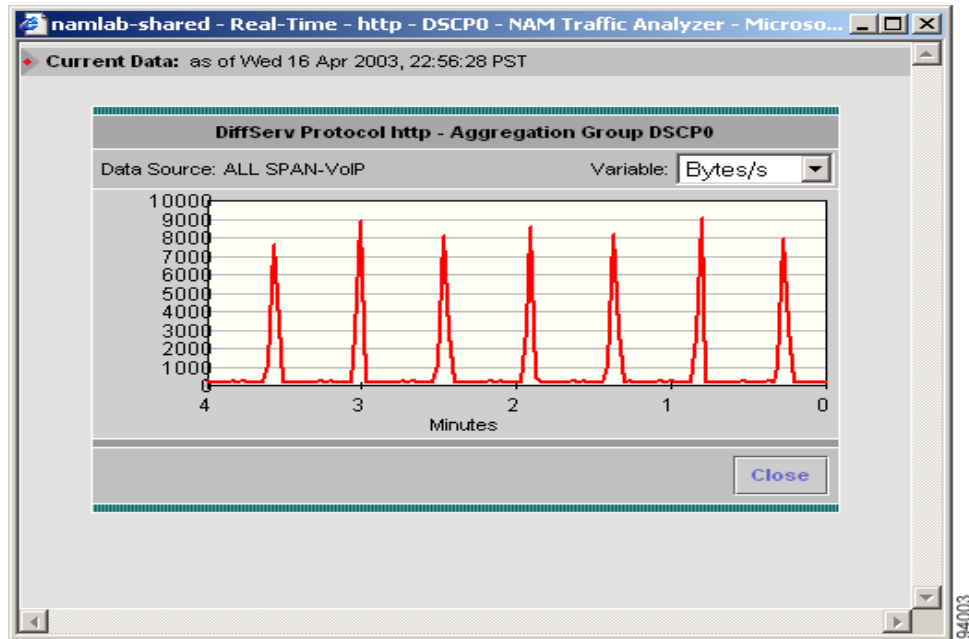
You can view real-time traffic statistics in a graphical format for a specific application protocol in the DiffServ Application Statistics table.

Choose the application protocol from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-24](#)) displays.



### Note

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

**Figure 4-35 Real-Time Graph**

## Viewing Reports from the DiffServ Application Statistics Table

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

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

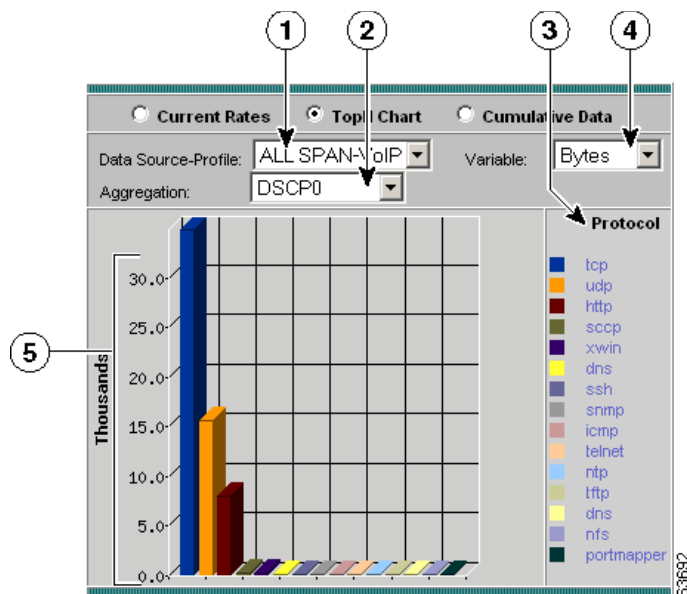
## Viewing the DiffServ Application Statistics Top N Chart

To view the Top N DiffServ Application Statistics chart:

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

**Step 2** Click the TopN Chart radio button.

The [Top N DiffServ Application Statistics Chart](#) (Figure 4-36) displays.

**Figure 4-36 Top N DiffServ Application Statistics Chart**

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

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

**Step 4** Choose the aggregation group from the Aggregation list.

**Step 5** Choose one of the following from the Variable list:

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

**Tip**

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

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

## Viewing the DiffServ Application Statistics Cumulative Data Table

To view the DiffServ Application Statistics Cumulative Data table:

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

**Step 2** Click the Cumulative Data radio button.

The [DiffServ Application Statistics Cumulative Data Table](#) (Table 4-36) displays.

**Table 4-36 DiffServ Application Statistics Cumulative Data Table**

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

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

**Step 4** Choose the aggregation group from the Aggregation list.

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

The specified protocol displays.

**Tip**

- To view the full protocol name, move the cursor over the protocol name.
- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Viewing the DiffServ Host Statistics Current Rates Table

To view the DiffServ Host Statistics Current Rates table:

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

**Step 2** Click the Current Rates radio button.

The [DiffServ Host Statistics Current Rates Table](#) (Table 4-37) displays.

**Table 4-37 DiffServ Host Statistics Current Rates Table**

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

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

**Step 4** Choose the aggregation group from the Aggregation list.

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

The specified address displays.



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Displaying Host Conversation Details From the DiffServ Host Statistics Table

To view the Host Conversations details table, click the address name in the Address column. The [Host Conversations Table](#) (Table 4-38) displays.

**Table 4-38**      *Host Conversations Table*

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



**Tip**

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

## Viewing Real-Time Data from the DiffServ Host Statistics Table

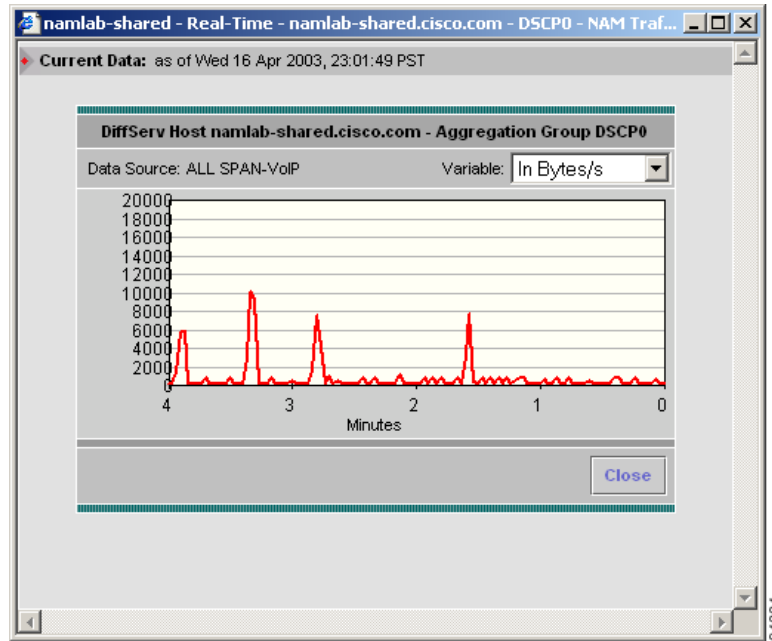
You can view real-time data in a graphical format for a specific host in the DiffServ Host Statistics table. Choose the host from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-24](#)) displays.



**Note**

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



**Figure 4-37 Real-Time Graph**

## Viewing Reports from the DiffServ Host Statistics Table

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

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

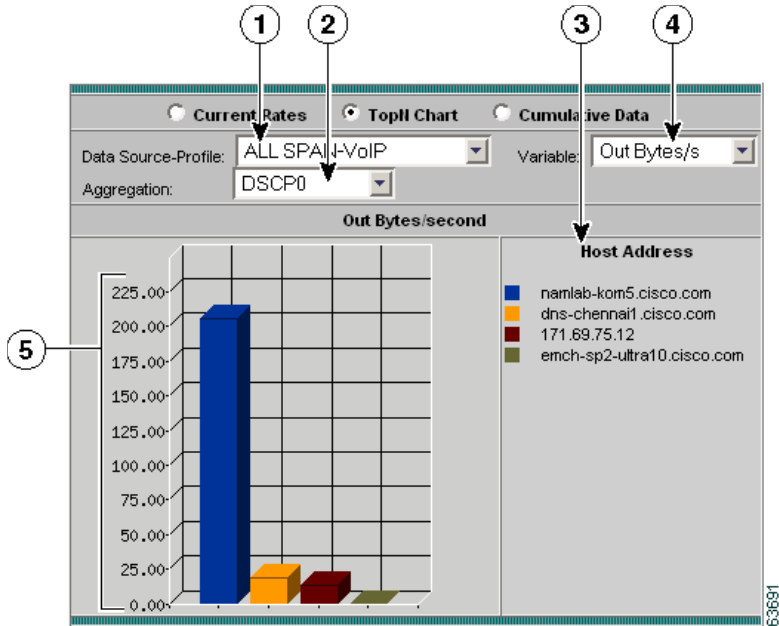
## Viewing the DiffServ Host Statistics Top N Chart

To view the DiffServ Top N Host Statistics chart:

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

The [DiffServ Top N Host Statistics Chart](#) (Figure 4-38) displays.

**Figure 4-38** *DiffServ Top N Host Statistics Chart*



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

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



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

# Viewing the DiffServ Host Statistics Cumulative Data Table

To view the DiffServ Host Statistics Cumulative Data table:

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

The [DiffServ Host Statistics Cumulative Data Table](#) (Table 4-39) displays.

**Table 4-39** *DiffServ Host Statistics Cumulative Data Table*

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

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

**Step 4** Choose the aggregation group from the Aggregation list.

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

The specified address displays.



**Tip**

- To turn off auto refresh, deselect the Auto Refresh check box.
- To sort a table variable by percentage of the total, click on the column header. The variable is listed in descending order according to the percentage of the total.

## Monitoring Response Time Data

NAM 4.1 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. NAM 4.1 response time monitoring provides end-to-end response times and to help you locate possible network and application delays.



**Note**

NAM 4.1 does not support IPv6 for response time monitoring.

You can set up the NAM to measure network round trip time (RTT), client response time, server response time, and total transaction time to improve application performance. [Figure 4-39](#) shows the various points in network packet flow where the NAM gathers data and the trip times you can monitor.

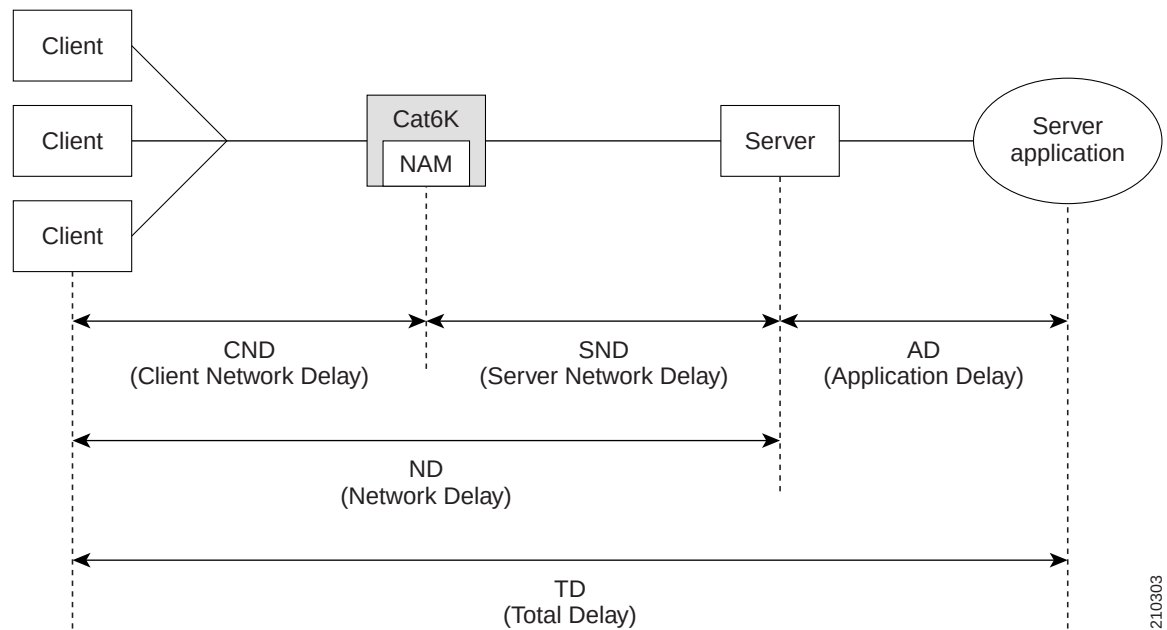
**Figure 4-39 NAM Application Response Time Measurements**

Figure 4-40 shows a representation of total transaction time as opposed to application response time.

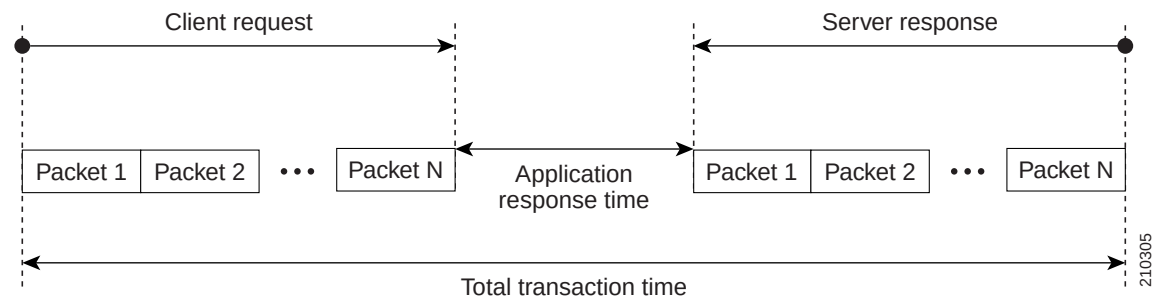
**Figure 4-40 Transaction Time versus Response Time Measurements**

Table 4-40 lists and describes the ART metrics measured by NAM 4.1.

**Table 4-40 Application Response Time Metrics**

| Metric                   | Description                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Response Time (average)  | Response Time is the amount of time it takes a server to send the initial response to a client request as seen by the NAM. This is the initial server <i>think time</i> . 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. |
| Response Time (minimum)  |                                                                                                                                                                                                                                                                                                                                                                       |
| Response Time (maximum)  |                                                                                                                                                                                                                                                                                                                                                                       |
| Number of responses      | Total number of responses observed during the monitoring interval                                                                                                                                                                                                                                                                                                     |
| Number of late responses | Total number of responses that exceed the Max Response Time; see <a href="#">Setting Up Response Time Configuration, page 3-61</a> .                                                                                                                                                                                                                                  |

**Table 4-40**      **Application Response Time Metrics (continued)**

| Metric                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of responses by response time | 7-bucket histogram; see <a href="#">Setting Up Response Time Configuration, page 3-61</a> .                                                                                                                                                                                                                                                                                                                                                   |
| Client Bytes                         | Number of TCP bytes sent from a client during the monitoring interval.                                                                                                                                                                                                                                                                                                                                                                        |
| Server Bytes                         | Number of TCP bytes sent from a server                                                                                                                                                                                                                                                                                                                                                                                                        |
| Client Packets                       | Number of TCP packets sent from a client                                                                                                                                                                                                                                                                                                                                                                                                      |
| Server Packets                       | Number of TCP packets sent from a server                                                                                                                                                                                                                                                                                                                                                                                                      |
| Number of connections (new sessions) | Number of TCP connections (new sessions) made during the monitoring interval.                                                                                                                                                                                                                                                                                                                                                                 |
| Completed Sessions                   | Number of TCP connections closed                                                                                                                                                                                                                                                                                                                                                                                                              |
| Refused Sessions                     | Number of TCP connections refused by a server                                                                                                                                                                                                                                                                                                                                                                                                 |
| Unresponsive Sessions                | Number of times a server does not reply to TCP SYN requests within a timeout period                                                                                                                                                                                                                                                                                                                                                           |
| Session Duration                     | Average duration of the TCP sessions                                                                                                                                                                                                                                                                                                                                                                                                          |
| Application Delay (AD) - average     | AD is the time it takes a server application (for example, a web server application) to respond to a request. AD is the time between the client request arriving at the server application and the first response being returned by the application.                                                                                                                                                                                          |
| Application Delay - minimum          |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Application Delay - maximum          |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Network Delay (ND) - average         | The network round trip (flight time) between a client and a server through the NAM switch or router. ND is equal to the sum of CND and SND. The network round trip (flight time) between a client and a server through the NAM switch or router. ND is equal to the sum of CND and SND. NAM measures the ND using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported. |
| Network Delay - minimum              |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Network Delay - maximum              |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Client Network Delay (CND) - average | CND is the network round trip time (or flight time) between a client and the NAM switch or router.<br><br>In WAAS monitoring, CND from a WAE client data source represents the network RTT between the client and its edge WAE, while CND from the WAE server data source represents the WAN RTT (between the edge and core WAEs).                                                                                                            |
| Client Network Delay - minimum       |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Client Network Delay - maximum       |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Server Network Delay (SND) - average | SND is the network round-trip time between a server and the NAM switch or router.<br><br>In WAAS monitoring, CND from a Server data source represents the network RTT between the server and its core WAE.                                                                                                                                                                                                                                    |
| Server Network Delay - minimum       |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Server Network Delay - maximum       |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Total Delay (TD) - average           | TD is the total amount of time from the first packet of a client request until the client receives the first response packet from the application server. Total Delay (TD) is the sum of the Network Delay (ND) and the Application Delay (AD).<br><br>Use TD with care because it is not measured directly and mixes the response time metric (SRT) with the connection metric (CND).                                                        |
| Total Delay - minimum                |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Total Delay - maximum                |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Total Transaction Time - average     | Total amount of time from the first packet of a client request until the client receives the final response packet from the server. TTT is a key indicator for detecting application performance anomalies.<br><br>Transaction times might vary depending upon application types. Relative thresholds are useful in this situation.                                                                                                           |
| Total Transaction Time - minimum     |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Total Transaction Time - max         |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Number of Transactions               | The number of transactions completed during the measurement interval.                                                                                                                                                                                                                                                                                                                                                                         |

**Table 4-40**      **Application Response Time Metrics (continued)**

| Metric                          | Description                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Transfer Time - average    | 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. |
| Number of Packets Retransmitted | Number of TCP packets retransmitted during the monitoring interval. (The metric for the client-to-server direction is not provided.)                                                                                                                                                             |
| Number of Bytes Retransmitted   | The number of retransmitted server-to-client bytes. (The metric for the client-to-server direction is not provided.)                                                                                                                                                                             |
| Retransmission Delay - average  | Average time to retransmit lost packets per transaction.                                                                                                                                                                                                                                         |
| Round Trip Time (RTT)           | Average round trip time for the client to acknowledge (ACK) a server TCP packet.                                                                                                                                                                                                                 |

To view response time data, click **Monitor > Response Time**. NAM 4.1 provides network and application response time (ART) monitoring for the following:

- [Server Application Responses, page 4-72](#)
- [Viewing Server Application Responses, page 4-72](#)

## Server Application Responses

The Server Application Responses window displays by default when you click **Monitor > Response Time**. The All Data window also displays by default. Click to view the TopN Chart instead to view the most active network.

- [Viewing Server Application Responses, page 4-72](#)
- [Viewing Server Application Transactions, page 4-77](#)
- [Server Network Response Time, page 4-80](#)

## Viewing Server Application Responses

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

- Application delay
- Network delay
- Total delay



### 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.

Figure 4-41 shows the [Server Application Responses Window](#).

**Figure 4-41** *Server Application Responses Window*

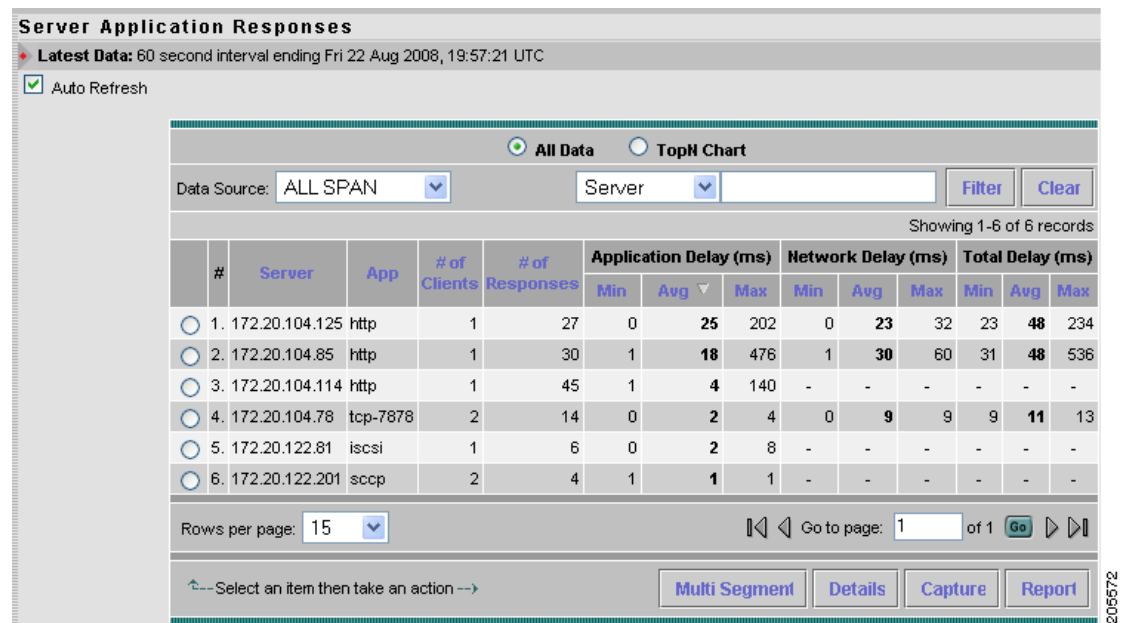


Table 4-41, [Server Application Responses](#), provides definitions of the Server Application Responses fields.

**Table 4-41** *Server Application Responses*

| Field             | Definition                                                                                                                                                                                                                                                                                 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server            | Name or IP address of the server                                                                                                                                                                                                                                                           |
| App               | Application currently running                                                                                                                                                                                                                                                              |
| # of Clients      | Total number of clients                                                                                                                                                                                                                                                                    |
| # of Responses    | Total number of responses observed during the monitoring interval                                                                                                                                                                                                                          |
| Application Delay | Minimum, average, and maximum values of AD, the time it takes a server application (for example, a web server application) to respond to a request. AD is the time between the client request arriving at the server application and the first response being returned by the application. |
| Network Delay     | Minimum, average, and maximum values of ND. ND the network round trip (flight time) between a client and a server through the NAM switch or router. ND is equal to the sum of CND and SND.                                                                                                 |
| Total Delay       | Total amount of time from the first packet of a client request until the client receives the first response packet from the application server.                                                                                                                                            |

Click **Multi Segment** to see response time metrics of the selected server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments](#), page 4-92 for more information.

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

## Viewing Server ART Details

To view details for a specific server, click the radio button in the Select column, then click **Details**. The Server ART Detail window displays detailed ART information from the server. [Table 4-42](#) provides a detailed description of the fields of the Server Application Response Time Details Window.

**Table 4-42 Server Application Response Time Details**

| Field                  | Description                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name            | Name or IP address of server being measured                                                                                                                                                                                                                                                                            |
| Server Address         | IP address of server                                                                                                                                                                                                                                                                                                   |
| Application            | Application being used by server                                                                                                                                                                                                                                                                                       |
| Number of Clients      | Total number of clients                                                                                                                                                                                                                                                                                                |
| Client Bytes           | Number of TCP bytes sent from a client during the monitoring interval.                                                                                                                                                                                                                                                 |
| Client Packets         | Number of TCP bytes sent from a client during the monitoring interval.                                                                                                                                                                                                                                                 |
| Server Bytes           | Number of TCP bytes sent from a server                                                                                                                                                                                                                                                                                 |
| Server Packets         | Number of TCP packets sent from a server                                                                                                                                                                                                                                                                               |
| Number of Responses    | Total number of responses observed during the monitoring interval                                                                                                                                                                                                                                                      |
| Application Delay      | This column displays the minimum, average, and maximum values of AD, the time it takes a server application (for example, a web server application) to respond to a request. AD is the time between the client request arriving at the server application and the first response being returned by the application.    |
| Network Delay          | This column displays the minimum, average, and maximum values of ND. ND the network round trip (flight time) between a client and a server through the NAM switch or router. ND is equal to the sum of CND and SND.                                                                                                    |
| Server Network Delay   | Also called Server Connection Time, this is the round-trip time between the server-site NAM (or WAAS-FA) and server during TCP connection setup. Measured on the server segment, this metric indicates the condition of a particular network segment. Server network delay is useful in isolating the problem.         |
| Total Delay            | Total amount of time from the first packet of a client request until the client receives the first response packet from the application server.                                                                                                                                                                        |
| Number of Transactions | The number of transactions completed during the measurement interval.                                                                                                                                                                                                                                                  |
| Transaction Time       | 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.<br><br>Transaction time is a key indicator when detecting application performance anomalies. |
| App Response Time      | Amount of time it takes a server to send the initial response to a client request as seen by the NAM.                                                                                                                                                                                                                  |



**Table 4-42 Server Application Response Time Details**

| Field                       | Description                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Transfer Time          | Time from the first server-response packet to the last server-response packet, excluding retransmission time. Data transfer time is always measured in the server-to-client direction and can be used to detect problems for a particular type of transaction of an application. |
| Average Retransmission Time | Average inter-packet time intervals started by retransmitted packets from server to client in each transaction, measured at server-site.                                                                                                                                         |
| Bytes Retransmitted         | The number of retransmitted server-to-client packets.                                                                                                                                                                                                                            |
| Packets Retransmitted       | The number of retransmitted server-to-client bytes.                                                                                                                                                                                                                              |
| Round Trip Time             | Time elapsed from a server-to-client packet to its client-to-server acknowledgement in each transaction. Round trip time is a key indicator for network-caused problems. Check WAN interface utilization, CND, and SND to isolate the problem.                                   |
| Number of Round Trips       | Number of times a server-to-client packet or client-to-server acknowledgement occurs in each transaction.                                                                                                                                                                        |
| Connections (New Sessions)  | Number of TCP connections (new sessions) made during the monitoring interval.                                                                                                                                                                                                    |
| Completed Sessions          | Number of TCP connections closed                                                                                                                                                                                                                                                 |
| Refused Sessions            | Number of TCP connections refused by a server                                                                                                                                                                                                                                    |
| Unresponsive Sessions       | The number of TCP connections unresponsive during the measurement interval, this metric indicates a WAN problem if client-site measurement is significantly large than the server-site measurement. Useful to compare client-side measurements with server-side measurements.    |
| Session Duration            | Average duration of the TCP sessions.                                                                                                                                                                                                                                            |

### Capturing Server ART Data

You can capture data from a specific server directly from the Server ART table.

Click the radio button in the Select column to choose the server from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

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

The Capture button is only available for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).



#### Note

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

## Viewing Reports from the Server Application Response Time Window

You can view reports directly from the Server Application Response Time window. Choose an item of interest from the active server/client application list, then click **Report**. If a report does not already exist for the entry, the NAM will create a response time metric report based on the parameters of the selected server and data source.

The report function is context sensitive. If you click **Monitor > Response Time > Server -- Response Times**, select an entry from those listed and click **Report**, the NAM would create a response time metric report (Average response time, client delay and server delay) for the selected entry.

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

## Viewing the Application Response Time TopN Chart

Click **TopN Chart** to view the most active network. To view the TopN Chart for Server Application Response Time:

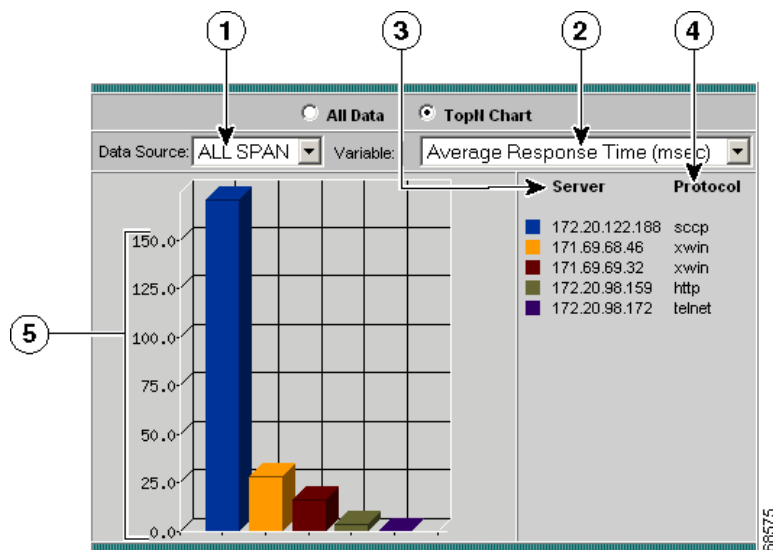
**Step 1** Click **Monitor > Response Time**.

The Server Application Response Time window displays.

**Step 2** Click the **TopN Chart** radio button.

The [Server Application Response Time Top N Chart](#) ([Figure 4-42](#)) displays.

**Figure 4-42 Server Application Response Time Top N Chart**



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

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

**Step 4** Choose the sorting option from the Variable list.

The specified option displays in the chart.

---

**Tip**

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

## Viewing Server Application Transactions

The Server Application Transaction window displays when you click **Monitor > Response Time > Server -- Transactions**. The All Data window also displays by default. You can also view the TopN Chart to view the most active network.

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.

---

Figure 4-43 shows the [Server Application Transactions Window](#).

**Figure 4-43** *Server Application Transactions Window*

| #  | Server         | App      | # of Clients | # of Trans | Trans Time (ms) | App Resp Time (ms) | Data Transfer Time (ms) | Retrans Time (ms) | Round Trip Time (ms) |
|----|----------------|----------|--------------|------------|-----------------|--------------------|-------------------------|-------------------|----------------------|
| 1. | 172.20.104.114 | http     | 1            | 45         | 12              | 3                  | 9                       | 0                 | 40                   |
| 2. | 172.20.104.78  | tcp-7878 | 1            | 10         | 10              | 2                  | 8                       | 0                 | 6                    |
| 3. | 172.20.122.81  | iscsi    | 1            | 6          | 0               | 1                  | 0                       | 0                 | 0                    |
| 4. | 172.20.122.201 | sccp     | 1            | 2          | 0               | 1                  | 0                       | 0                 | 9                    |

[Table 4-43, Server Application Transactions Metrics](#), provides definitions of each field of the Server Application Transactions window.

**Table 4-43** *Server Application Transactions Metrics*

| Field              | Description                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server             | Name or IP address of the server                                                                                                                                                                                                                                                                                       |
| App                | Application currently running                                                                                                                                                                                                                                                                                          |
| # of Clients       | Total number of clients                                                                                                                                                                                                                                                                                                |
| # of Trans         | Total number of transactions                                                                                                                                                                                                                                                                                           |
| Trans Time         | 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.<br><br>Transaction time is a key indicator when detecting application performance anomalies. |
| App Resp Time      | Amount of time it takes a server to send the initial response to a client request as seen by the NAM.                                                                                                                                                                                                                  |
| Data Transfer Time | 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.                       |
| Retrans Time       | Average time to retransmit lost packets, per transaction.                                                                                                                                                                                                                                                              |
| Round Trip Time    | Average round trip time for the client to acknowledge (ACK) a server TCP packet.                                                                                                                                                                                                                                       |

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

Click **Multi Segment** to see response time metrics of the select server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments, page 4-92](#) for more information.

## Viewing Server Application Transaction Details

To view details for a specific server, click the radio button in the Select column, then click **Details**. The Server ART Detail window displays. You can view detailed information from the server such as server network delay response time, a histogram, octet counts, and maximum and minimum values as well as a chart displaying the response time distribution.

[Table 4-42](#) provides a detailed description of the fields of the Server Application Transaction Window.

## Capturing Server Application Transaction Data

You can capture data from a specific server directly from the Server ART table.

Click the radio button in the Select column to choose the server from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

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

The Capture button is only available for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).



**Note**

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

## Viewing Reports from the Server Application Transactions Window

You can view reports directly from the Server Application Transactions window. Choose an item of interest from the active server/client application list, then click **Report**. If a report does not already exist for the entry, the NAM will create a transactions metrics report based on the parameters of the selected server and data source.

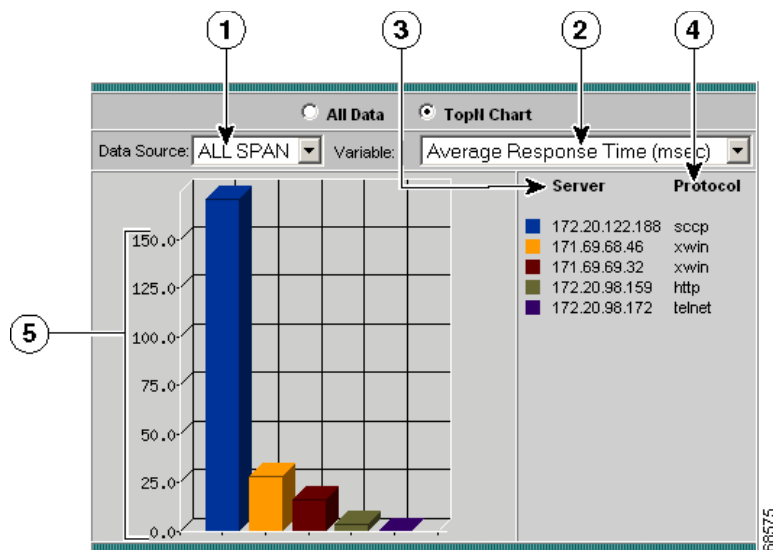
The report function is context sensitive. If you click **Monitor > Response Time > Server -- Transaction**, select an entry from those listed and click **Report**, the NAM will create an average transaction response time metric report for the selected entry.

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

## Viewing the Server Application Transactions TopN Chart

Click **TopN Chart** to view the most active network. To view the TopN Chart for Server Application Transactions:

- 
- Step 1** Click **Monitor > Response Time**.  
The Server Application Transactions window displays.
  - Step 2** Click the **TopN Chart** radio button.  
The [Server Application Response Time Top N Chart \(Figure 4-42\)](#) displays.

**Figure 4-44 Server Application Transactions Top N Chart**

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

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

**Step 4** Choose the sorting option from the Variable list.

The specified option displays in the chart.



**Tip**

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

## Server Network Response Time

The Server Network Response Time window shows the network connectivity and responsiveness between the server and the switch.

Figure 4-45 shows the Server Network Response Time Window.

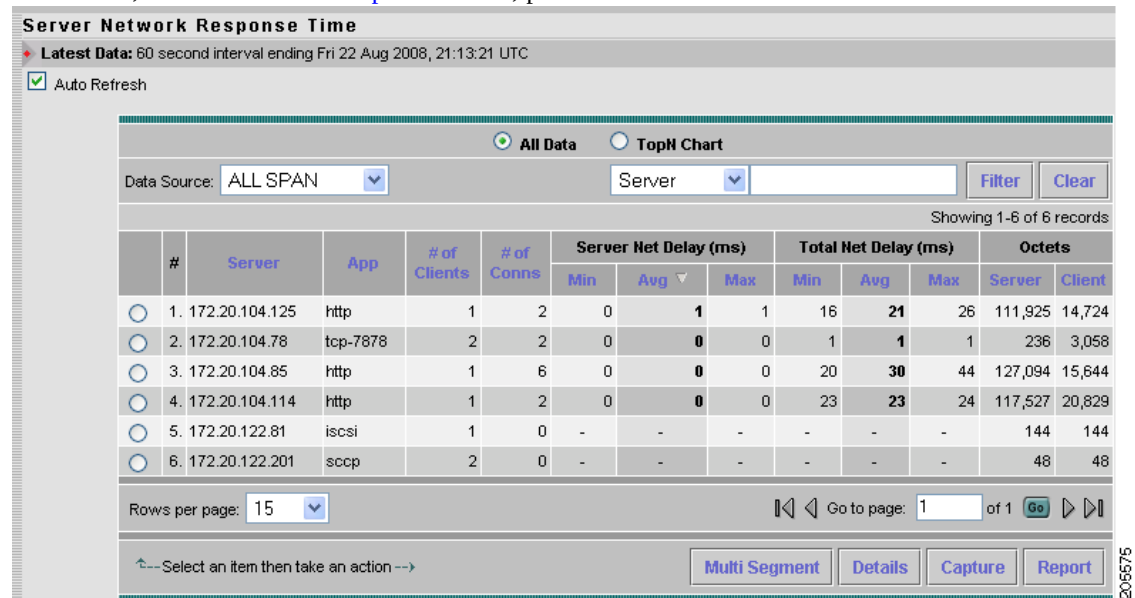


**Note**

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.

**Figure 4-45 Server Network Response Time Window**

Table 4-44, [Server Network Response Times](#), provides definitions of each field of the Server Network



Response Times window.

**Table 4-44 Server Network Response Times**

| Field                | Description                                                                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server               | Server name or IP address                                                                                                                                                                                                                                                                                            |
| App                  | Application in use                                                                                                                                                                                                                                                                                                   |
| # of Clients         | Number of active client sessions                                                                                                                                                                                                                                                                                     |
| # of Conns           | Number of active connections                                                                                                                                                                                                                                                                                         |
| Server Network Delay | SND is the network round trip time (or flight time) between a server and the NAM switch, router, or managed device (minimum, average, and maximum server network delay in ms.)                                                                                                                                       |
| Total Net Delay      | This column displays the minimum, average, and maximum values of TD. TD is the total amount of time from the first packet of a client request until the client receives the first response packet from the application server. Total Delay (TD) is the sum of the Network Delay (ND) and the Application Delay (AD). |
| Octets               | Number of server octets and client octets transmitted.                                                                                                                                                                                                                                                               |

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

Click **Multi Segment** to see response time metrics of the select server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments, page 4-92](#) for more information.

Click Capture to capture data from a specific server directly from the Server Network Response Time window. See [Capturing Data from the Server Network Response Time Window, page 4-82](#), for more information.

Click Reports to view reports directly from the Server Network Response Time window. See [Viewing Reports from the Server Network Response Time Window, page 4-83](#), for more information.

- [Viewing Server-Client Application Response Time](#)

## Viewing Server Network Response Time Details

[Table 4-45](#) provides a detailed description of the fields of the Server Network Response Time Window.

**Table 4-45 Server Network Response Time Window Details**

| Field                  | Description                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server                 | Name of server being measured                                                                                                                                                                                                                                                                                        |
| App                    | Application being used by server                                                                                                                                                                                                                                                                                     |
| # of Clients           | Number of clients attached to server                                                                                                                                                                                                                                                                                 |
| # of Conns             | Number of active connections with the server                                                                                                                                                                                                                                                                         |
| Server Net Delay (SND) | This column displays the minimum, average, and maximum values of SND. SND is the network round trip time (or flight time) between a server and the NAM switch or router.                                                                                                                                             |
| Total Net Delay        | This column displays the minimum, average, and maximum values of TD. TD is the total amount of time from the first packet of a client request until the client receives the first response packet from the application server. Total Delay (TD) is the sum of the Network Delay (ND) and the Application Delay (AD). |
| Octets                 | For server, number of octets (bytes) sent from the server to the client.<br>For client, number of octets (bytes) sent from the client to the server.                                                                                                                                                                 |

## Capturing Data from the Server Network Response Time Window

You can capture data from a specific server directly from the Server Network Response Time window.

Click the radio button in the Select column to choose the server from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

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

The Capture button is only available for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).



### Note

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



## Viewing Reports from the Server Network Response Time Window

You can view reports directly from the Server Network Response Time window. Choose the server you wish to view a report on, then click **Report**. If a report does not already exist for the entry, the NAM will create a transactions metrics report based on the parameters of the selected server and data source.

The report function is context sensitive. If you click **Monitor > Response Time > Server -- Network**, select an entry from those listed and click **Report**, the NAM will create a Total Response Time report for the selected entry.

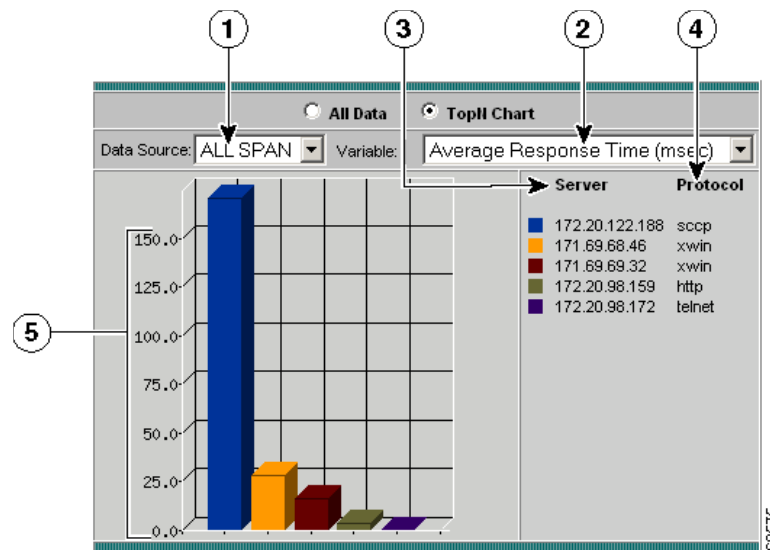
For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

## Viewing the Server Network Response Time Top N Chart

Click **TopN Chart** to view the most active network. To view the TopN Chart for Server Application Response Time:

- Step 1** Click **Monitor > Response Time**.  
The Server Application Response Time window displays.
- Step 2** Click **Server Network** in the menu area.  
The Server Network Response Time window displays.
- Step 3** Click the **TopN Chart** radio button.  
The [Server Network Response Time Top N Chart \(Figure 4-46\)](#) displays.

**Figure 4-46 Server Network Response Time Top N Chart**



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

**Step 4** Choose the data source to be monitored from the Data Source list.

**Step 5** Choose the sorting option from the Variable list.

The specified option displays in the chart.

---

**Tip**

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

## Server-Client Application Response Times

The Server/Client ART window provides a summary of the server/client application response time data. You can select an entry in the window to view more detailed information.

- [Viewing Server-Client Application Response Time, page 4-84](#)
- [Viewing the Server-Client Transactions, page 4-88](#)
- [Viewing the Server-Client Network Response Time, page 4-89](#)

### Viewing Server-Client Application Response Time

To view the Server-Client Application Response Time window:

---

**Step 1** Click **Monitor > Response Time**.

The Server Application Response Time window displays.

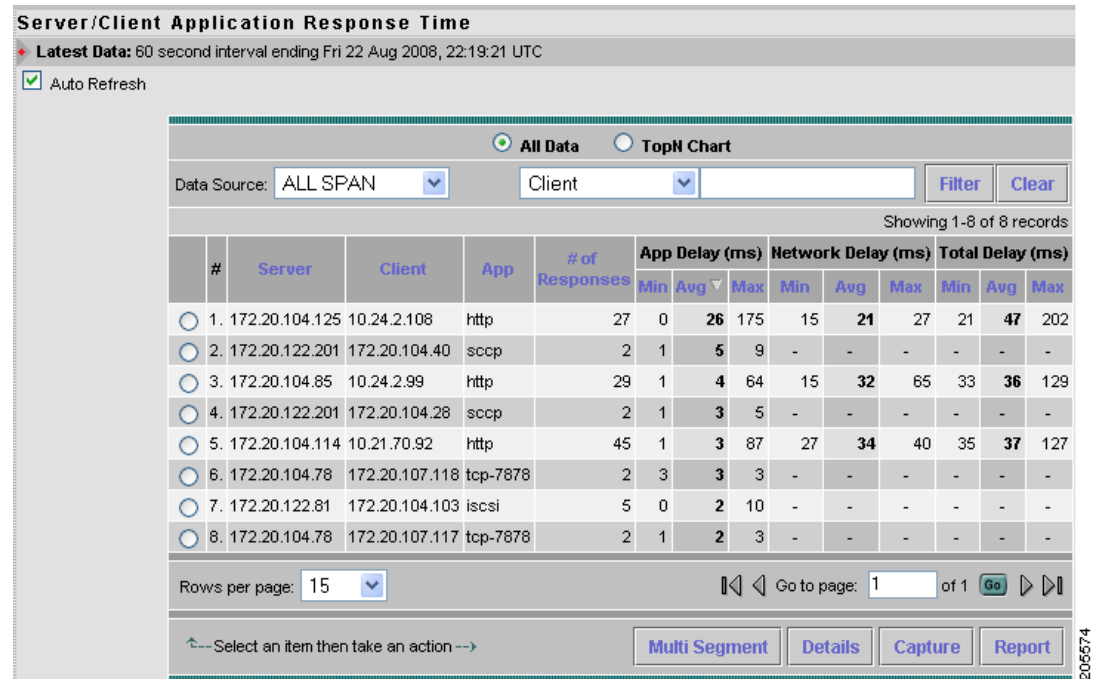
**Step 2** In the contents, click **Server-Client Application**.

[Figure 4-47](#) shows the Server/Client Application Response Time 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.

---

**Figure 4-47 Server/Client Application Response Time Window**

The [Server/Client Application Response Time Window](#) (Table 4-46) displays.

**Table 4-46 Server/Client Application Response Time Window**

| Field                  | Description                                                                                                                                                                                                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server                 | Host address of the server.                                                                                                                                                                                                                                                                                         |
| Client                 | Host address of the client.                                                                                                                                                                                                                                                                                         |
| App                    | Application being used by server                                                                                                                                                                                                                                                                                    |
| # of Responses         | Total number of responses observed during the monitoring interval                                                                                                                                                                                                                                                   |
| Application Delay (AD) | This column displays the minimum, average, and maximum values of AD, the time it takes a server application (for example, a web server application) to respond to a request. AD is the time between the client request arriving at the server application and the first response being returned by the application. |
| Network Delay (ND)     | This column displays the minimum, average, and maximum values of ND, the network round trip (flight time) between a client and a server through the NAM switch or router. ND is equal to the sum of CND and SND.                                                                                                    |
| Total Delay (TD)       | TD is the total amount of time from the first packet of a client request until the client receives the first response packet from the application server. Total Delay (TD) is the sum of the Network Delay (ND) and the Application Delay (AD).                                                                     |

- Step 3** Choose the data source to be monitored from the Data Source list.
- Step 4** Choose a variable to filter from the filter list.
- Step 5** Enter the name of the variable to filter in the filter box, then click **Filter**.

The specified variable displays.

---

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

Click **Multi Segment** to see response time metrics of the select server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments, page 4-92](#) for more information.

**Tip**

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

### Viewing Server-Client Application Response Time Details

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

### Capturing Protocol Data from the Server-Client Application Response Time Window

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

Choose the server protocol from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).

**Note**

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

---

### Viewing Reports from the Server-Client Application Response Time Window

You can view reports directly from the Server-Client Response Time table. Choose the protocol you wish to view a report on, then click **Report**. The Basic Reports graph displays a Total Response Time report based on the parameters of the selected server and data source entry. If a report does not already exist for the entry, the NAM will create a response time metrics report based on the parameters of the selected server and data source.

The report function is context sensitive. If you click **Monitor > Response Time > Server-Client -- Network**, select an entry from those listed and click **Report**, the NAM will create a Total Response Time report for the selected entry.

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

## Viewing the Server/Client Application Response Time Top N Chart

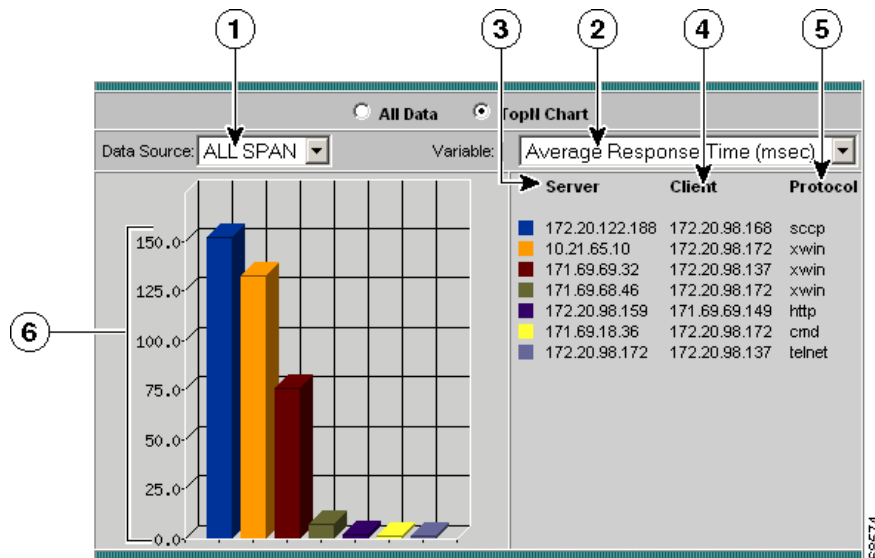
To view the Client/Server Response Time Top N chart:

**Step 1** In the contents menu, click **Server-Client Application**.

**Step 2** Click the TopN Chart radio button.

The **Client/Server Application Response Time Top N Chart** (Figure 4-48) displays.

**Figure 4-48** *Client/Server Application Response Time Top N Chart*



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

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

**Step 4** Choose the sorting option from the Variable list.

The specified option displays in the chart.



### Tip

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

## Viewing the Server-Client Transactions

The Server-Client Application Transaction window displays when you click **Monitor > Response Time > Server-Client -- Transactions**. The All Data window also displays by default. You can also view the TopN Chart to view the most active network.

The Server-Client 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 4-47** *Server-Client Transactions Response Time Window*

| Field              | Description                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server             | Host address of the server.                                                                                                                                                                                                                                                                      |
| Client             | Host address of the client.                                                                                                                                                                                                                                                                      |
| App                | Application being used by server                                                                                                                                                                                                                                                                 |
| # of Trans         | Total number of responses observed during the monitoring interval                                                                                                                                                                                                                                |
| Trans Time         | Total amount of time from the first packet of a client request until the client receives the final response packet from the server. TTT is a key indicator for detecting application performance anomalies.                                                                                      |
| App Resp Time      | Amount of time it takes a server to send the initial response to a client request as seen by the NAM.                                                                                                                                                                                            |
| Data Transfer Time | 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. |
| Retrans Time       | Average time to retransmit lost packets, per transaction.                                                                                                                                                                                                                                        |
| Round Trip Time    | Average round trip time for the client to acknowledge (ACK) a server TCP packet.                                                                                                                                                                                                                 |

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

Click **Multi Segment** to see response time metrics of the select server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments, page 4-92](#) for more information.

## Viewing the Server-Client Network Response Time

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

To view the Server/Client Network Response Time window:

- Step 1** In the contents, click **Server-Client Network**.

Figure 4-49 shows the Server-Client Network Response Time 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.

**Figure 4-49 Server-Client Network Response Time Window**

| Client/Server Network Response Time                                  |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
|----------------------------------------------------------------------|-----------------------|------------------------|------|------------|-----------------------|-----|-----|-----------------------|-----|-----|--------------------|-----|-----|
| Latest Data: 30 second interval ending Mon 11 Dec 2006, 09:06:27 UTC |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
| Auto Refresh                                                         |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
| All Data TopN Chart                                                  |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
| Data Source: [ ] [ ] Filter Clear                                    |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
| Showing 1-3 of 3 records                                             |                       |                        |      |            |                       |     |     |                       |     |     |                    |     |     |
| #                                                                    | Server                | Client                 | App  | # of Conns | Client Net Delay (ms) |     |     | Server Net Delay (ms) |     |     | Network Delay (ms) |     |     |
|                                                                      |                       |                        |      |            | Min                   | Avg | Max | Min                   | Avg | Max | Min                | Avg | Max |
| 1.                                                                   | namlab-kom4.cisco.com | sjc-vpn6-537.cisco.com | http | 2          | 0                     | 45  | 54  | 0                     | 0   | 1   | 0                  | 45  | 55  |
| 2.                                                                   | kabob.cisco.com       | 172.20.104.79          | sccp | 0          | -                     | -   | -   | -                     | -   | -   | -                  | -   | -   |
| 3.                                                                   | kabob.cisco.com       | 172.20.104.80          | sccp | 0          | -                     | -   | -   | -                     | -   | -   | -                  | -   | -   |

Rows per page: [ ] Go to page 1 of 1 Ga

Select an item then take an action --> Details Capture Report

Table 4-48 describes the fields of the Server-Client Network Response Time window.

**Table 4-48 Server-Client Network Response Time Window**

| Field                | Description                                                 |
|----------------------|-------------------------------------------------------------|
| Server               | Host address of the server.                                 |
| Client               | Host address of the client.                                 |
| App                  | Application being used by server                            |
| # of Conns           | Current number of connections                               |
| Client Network Delay | Minimum, average, and maximum values of time                |
| Server Network Delay | Minimum, average, and maximum values of total network delay |
| Network Delay        | Minimum, average, and maximum values of total network delay |

- Step 2** Choose the data source to be monitored from the Data Source list.
- Step 3** Choose a variable to filter from the filter list.
- Step 4** Enter the name of the variable to filter in the filter box, then click **Filter**.  
The specified variable displays.

Click **Details** to see the Server ART Details. See [Viewing Server ART Details, page 4-74](#) for more information.

Click **Multi Segment** to see response time metrics of the select server or client-server pair from applicable data sources. See [Viewing Response Time across Multiple WAAS Segments, page 4-92](#) for more information.

**Tip**

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

## Viewing Server-Client Response Time Details

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

## Capturing Protocol Data from the Server-Client Application Response Time Window

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

Choose the server protocol from the table, then click **Capture**. The Packet Browser displays. For more information on viewing packets using the Packet Browser, see the [“Viewing Detailed Protocol Decode Information” section on page 6-14](#).

The Capture button is available only for a subset of reported protocols. For protocols such as IP, IPv6, and GRE, you must set up a custom filter. For more information on setting up custom filters, see the [“Creating Custom Capture Filters” section on page 6-27](#).

**Note**

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

## Viewing Reports from the Server-Client Response Time Window

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

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

## Viewing the Server-Client Network Response Time TopN Chart

To view the Server-Client Network Response Time Top N chart:

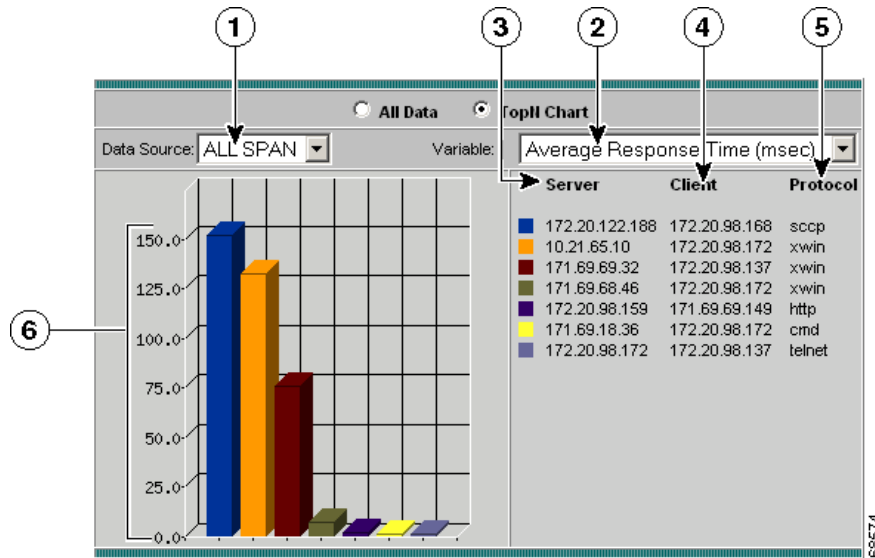


**Step 1** In the contents, click **Server-Client**.

**Step 2** Click the TopN Chart radio button.

The Server-Client Network Response Time Top N Chart (Figure 4-50) displays.

**Figure 4-50 Client/Server Network Response Time Top N Chart**



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

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

**Step 4** Choose the sorting option from the Variable list.

The specified option displays in the chart.



**Tip**

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

## Viewing Response Time across Multiple WAAS Segments

Use the Response Time Across Multiple Segments window to monitor WAAS traffic. This window provides correlation of data from different data sources and allows you to view and compare response time metrics from multiple WAAS segments (data sources).

From Any Response Time window, select a server or a client-server pair, then click **Multi Segment**. The Response Time Across Multiple Segments window displays, as shown in [Figure 4-51](#). The Individual Data Sources option displays by default and lists all configured data sources. See [Table 4-40](#), [Application Response Time Metrics](#), for a description of the metrics displayed on the Response Time Across Multiple Segments window.

**Figure 4-51** Viewing Response Time Across Multiple Segments - Individual Data Sources

Current Data: as of Wed 17 Jun 2009, 06:59:41 UTC

Response Time across Multiple Segments (Data Sources)

Individual Data Source View

Correlated WAAS Segment View

Server: 10.96.1.2

Client: 10.95.1.2

Application:

Filter

Clear

Showing 1-6 of 6 records

| #  | Data Source               | Server    | Client    | App  | Client Net/WAN Delay (ms) | Server Net Delay (ms) | App Delay (ms) | Total Delay (ms) | Transaction Time (ms) | Server Bytes | Client Bytes |
|----|---------------------------|-----------|-----------|------|---------------------------|-----------------------|----------------|------------------|-----------------------|--------------|--------------|
| 1. | WAE-172.20.122.121-Client | 10.96.1.2 | 10.95.1.2 | ftp  | 1                         | 4                     | 8              | 12               | 26                    | 320,260      | 93,368       |
| 2. | WAE-172.20.122.121-Client | 10.96.1.2 | 10.95.1.2 | http | 1                         | 14                    | 14             | 29               | 29                    | 10,441,050   | 377,175      |
| 3. | WAE-172.20.122.122-Server | 10.96.1.2 | 10.95.1.2 | ftp  | 13                        | 0                     | 2              | 6                | 17                    | 317,580      | 92,587       |
| 4. | WAE-172.20.122.122-Server | 10.96.1.2 | 10.95.1.2 | http | 3                         | 1                     | 0              | 14               | 1                     | 10,346,266   | 373,751      |
| 5. | WAE-172.20.122.122-SvrWAN | 10.96.1.2 | 10.95.1.2 | ftp  | 13                        | 0                     | 9              | 13               | 21                    | 477,904      | 392,525      |
| 6. | WAE-172.20.122.122-SvrWAN | 10.96.1.2 | 10.95.1.2 | http | 3                         | 1                     | 1              | 15               | 16                    | 1,678,779    | 674,861      |

Rows per page: 15

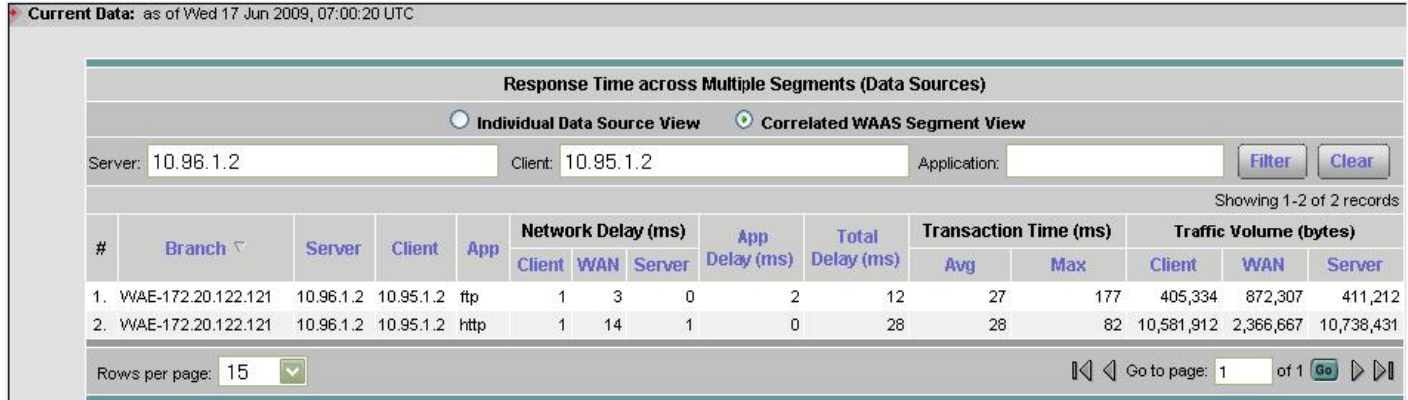
Go to page: 1 of 1

The Response Time Across Multiple Segments window shows response time metrics of the selected server or client-server pair from applicable data sources. More relevant metrics are shown in bold font. To view Correlated Data Sources, shown in [Figure 4-52](#), click the Correlated Data Sources radio button.



### Note

The Correlated Data Sources option is available only for Server/Client, not server response time.

**Figure 4-52 Viewing Response Time Across Multiple Segments - Correlated Data Sources**

See [Table 4-40, Application Response Time Metrics](#), for more information.

## Viewing Port/Interface Statistics Data

To view the various data collected for the switch or router, click **Monitor**, then **Switch** or **Router**. The Port Stats or Interface Stats table displays with three radio buttons above it.

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

- [Viewing the Port Stats Current Rates Table, page 4-93.](#)
- [Viewing the Top N Port Stats Chart, page 4-97.](#)
- [Viewing the Port Stats Cumulative Data Table, page 4-100.](#)

For Interface Stats you can click a radio button for:

- [Viewing the Interface Stats Current Rates Table, page 4-95.](#)
- [Viewing the Top N Interface Stats Chart, page 4-99.](#)
- [Viewing the Interface Stats Cumulative Data Table, page 4-101.](#)



### Note

For NM-NAM or NME-NAM devices, if you have set up **Interfaces** under **Setup > Data Sources**, you will be able to view hosts, conversations, and applications in the Details window.

## Viewing the Port Stats Current Rates Table

The Port Stats Current Rates table enables you to view the various data collected for the switch. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94.](#)

The Count Types drop down menu enables you to view the default Traffic Rates

To view the Port Stats Current Rates Table (Traffic Rates):

**Step 1** Click the Current Rates Table radio button.

The [Port Stats Current Rates Table \(Traffic Rates\)](#) (Table 4-49) lists the fields displayed when the Count Type is set to Traffic Rates.

**Table 4-49 Port Stats Current Rates Table (Traffic Rates)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Name           | Port number.<br><br>Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1.<br><br>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. |
| Utilization %       | Utilization percentage of the port.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Bytes/s             | Number of bytes collected on the port per second.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Packets/s           | Number of packets collected on the port per second.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Broadcast Packets/s | Number of broadcast packets collected per second.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Multicast Packets/s | Number of multicast packets collected per second.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Errors              | Number of all types of errors detected. See <a href="#">Table 4-50</a> for a list of all errors.                                                                                                                                                                                                                                                                                                                                                                                    |

The [Port Stats Current Rates Table \(Error Rates\)](#) (Table 4-50) lists the fields displayed when the Count Type is set to Error Rates.

**Table 4-50 Port Stats Current Rates Table (Error Rates)**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Name           | Port number<br><br>Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1.<br><br>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. |
| Utilization %       | Utilization percentage of the port                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Dropped Events/s    | Number of dropped events per second                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CRC Align Errors/s  | Number of CRC align errors collected per second                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Undersize packets/s | Number of packets collected under 64 octets in length                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Oversize Packets/s  | Number of packets collected over 1518 octets in length                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Fragments/s         | Number of packets collected per second that were less than 64 octets in length and had bad a Frame Check Sequence (FCS)                                                                                                                                                                                                                                                                                                                                                            |

**Table 4-50 Port Stats Current Rates Table (Error Rates) (continued)**

| Field        | Description                                                                                                                           |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Jabbers/s    | Number of collected packets collected per second that were longer than 1518 octets in length and had a bad Frame Check Sequence (FCS) |
| Collisions/s | Number of collisions collected per second on the Ethernet segment                                                                     |

**Note**

[Table 4-49](#) and [Table 4-50](#) are also valid for the Cumulative Data radio button.

**Step 2**

Enter the port name to filter in the Port Name text box, then press **Filter**.  
The specified port name displays.

**Tip**

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

## Viewing the Interface Stats Current Rates Table

The Interface Stats Current Rates table enables you to view the various data collected for the router. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Interface Stats Current Rates table:

**Step 1**

Click the Current Rates radio button.

The [Interface Stats Current Rates Table \(Table 4-51\)](#) displays.

**Table 4-51 Interface Stats Current Rates Table**

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

**Table 4-51**      **Interface Stats Current Rates Table (continued)**

| Field        | Description                            |
|--------------|----------------------------------------|
| In Errors/s  | Number of errors collected per second. |
| Out Errors/s | Number of errors sent out per second.  |

- Step 2**      Enter the name of the to filter in the Filter text box, then click **Filter**.  
The specified interface name displays.

**Tips**

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

## Viewing Port/Interface Details

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

Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1. 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 Gi1/2/1to represent a Gigabit port on switch 1, module2, port 1.

**Note**

For NM-NAM or NME-NAM devices, if you have set up an interface on the **Setup > Data Source > Interface** window, applications, hosts, and conversation TopN tables are displayed in the detail window.

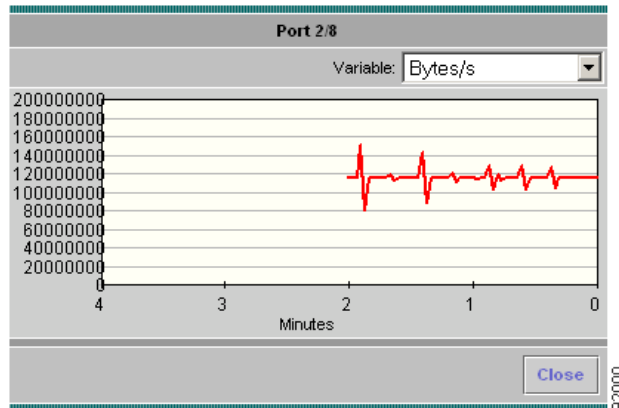
## Viewing Real-Time Traffic Data from the Port/Interface Stats Table

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

Choose the switch port or interface from the table, then click **Real-Time**. The Real-Time Graph ([Figure 4-53](#)) displays.

**Note**

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

**Figure 4-53 Real-Time Graph**

## Viewing Reports from the Port/Interface Stats Table

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

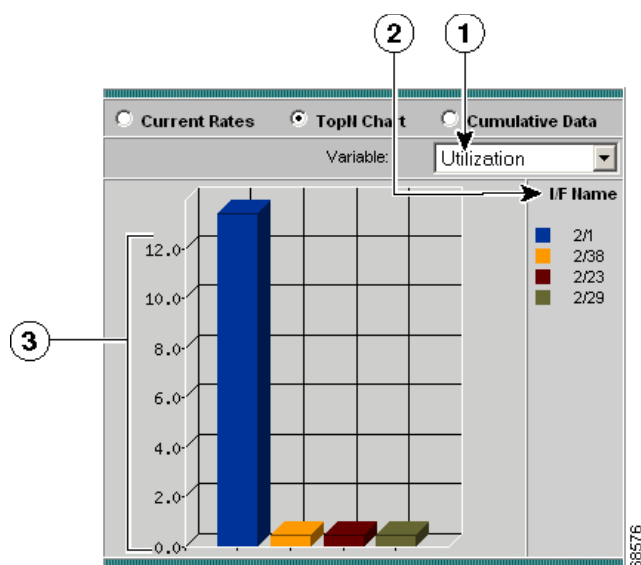
For more information on viewing and creating reports, see [Chapter 5, “Creating and Viewing Reports.”](#)

## Viewing the Top N Port Stats Chart

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

To view the Top N Port Stats chart:

- 
- Step 1** Click the TopN Chart radio button.  
The Top N Port Stats Chart ([Figure 4-54](#)) displays.

**Figure 4-54 Top N Port Stats Chart**

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

**Step 2** Choose one of the following from the Variable list:

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



**Tip**

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



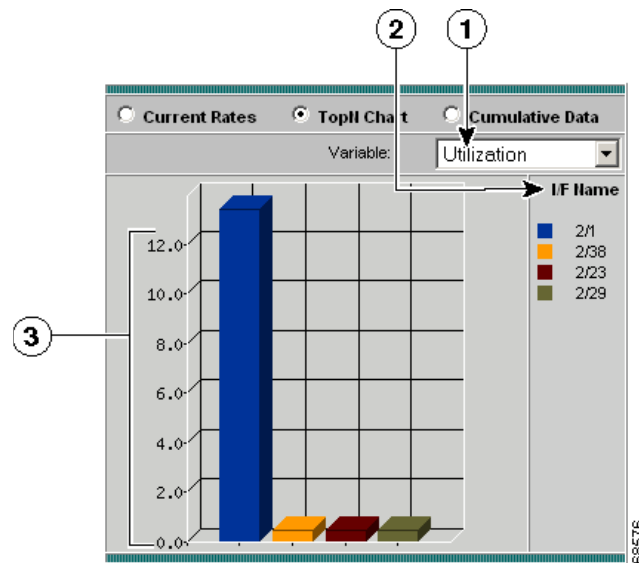
## Viewing the Top N Interface Stats Chart

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

To view the Top N Interface Stats chart:

- Step 1** Click the TopN Chart radio button.  
The [Top N Interface Stats Chart](#) (Figure 4-55) displays.

**Figure 4-55 Top N Interface Stats Chart**



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

- Step 2** Choose one of the following from the Variable list:
- In Packets/s—Sorts the interface number based packets collected per second.
  - Out Packets/s—Sorts the interface number based on the number of packets sent out per second.
  - In Bytes/s—Sorts the interface number based on the number of bytes collected per second.
  - Out Bytes/s—Sorts the interface number based on the number of bytes sent out per second.
  - In Non-Unicast Pkts/s—Sorts the interface number based on the number of non-unicast packets collected per second.
  - Out Non-Unicast Pkts/s—Sorts the interface number based on the number of non-unicast packets sent out per second.
  - In Errors/s—Sorts the interface number based on the number of errors collected per second.

- Out Errors/s—Sorts the interface number based on the number of errors sent out per second.
- In Discards/s—Sorts the interface number based on the number of discards collected per second.
- Out Discards/s—Sorts the interface number based on the number of discards sent out per second.

**Tip**

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

## Viewing the Port Stats Cumulative Data Table

The Port Stats Cumulative Data table enables you to view the various data collected for the switch. The information displayed represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Port Stats Cumulative Data table:

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

The [Port Stats Cumulative Data Table](#) (Table 4-52) displays. When you select Traffic Rates, only the traffic data are shown along with a field for total errors. When you select Error Rates, the Port Name and Utilization fields are shown with fields for each error type. Choose All to view all traffic rates and all errors at once.

**Table 4-52** *Port Stats Cumulative Data Table*

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Name         | Port number.<br><br>Depending on the IOS running on the Supervisor, port names are displayed differently. Earlier versions of CatOS displayed port names as 2/1 and 3/1 meaning module 2, port 1 and module 3 port 1.<br><br>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, module 2, port 1. |
| Utilization       | Utilization percentage of the port.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Bytes             | Number of bytes collected on the port.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Packets           | Number of packets collected on the port.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Broadcast Packets | Number of broadcast packets collected.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Multicast Packets | Number of multicast packets collected.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Errors            | Total of all errors<br><b>Note</b> This field is shown only when you select Traffic Rates.                                                                                                                                                                                                                                                                                                                                                                |
| Dropped Events    | Number of dropped events.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CRC Align Errors  | Number of CRC align errors collected.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Undersize packets | Number of collected packets under 64 octets long.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Oversize Packets  | Number of collected packets over 1518 octets long.                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 4-52** Port Stats Cumulative Data Table (continued)

| Field      | Description                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------|
| Fragments  | Number of collected packets collected that were less than 64 octets long and had bad Frame Check Sequence (FCS).     |
| Jabbers    | Number of collected packets collected that were longer than 1518 octets long and had bad Frame Check Sequence (FCS). |
| Collisions | Number of collected collisions on the Ethernet segment.                                                              |

**Step 2** To refresh the data in the table, click **Refresh**.

**Step 3** Enter the port name to filter in the Port Name text box, then press **Filter**.  
The specified port name displays.

## Viewing the Interface Stats Cumulative Data Table

The Interface Stats Cumulative Data table enables you to view the various data collected for the router. The displayed information represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94](#).

To view the Interface Stats Cumulative Data table:

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

The [Interface Stats Cumulative Data Table \(Table 4-53\)](#) displays.

**Table 4-53** Interface Stats Cumulative Data Table

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

**Step 2** To refresh the data in the table, click **Refresh**.

- Step 3** Enter the interface name to filter in the Filter text box, then click **Filter**.  
The specified interface name displays.
- 

## Viewing Interface Details

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

# Viewing System Health

You can use the NAM Traffic Analyzer to view system health data. To view system health data collected for the switch or router, choose **Monitor** > **Router** or **Monitor** > **Switch** then select **Health** from the Content Menu.

Depending on the type of device, one of the following windows displays:

- [Switch Health](#)
- [Router Health](#)
- Appliance Health (Managed Device)

## Switch Health

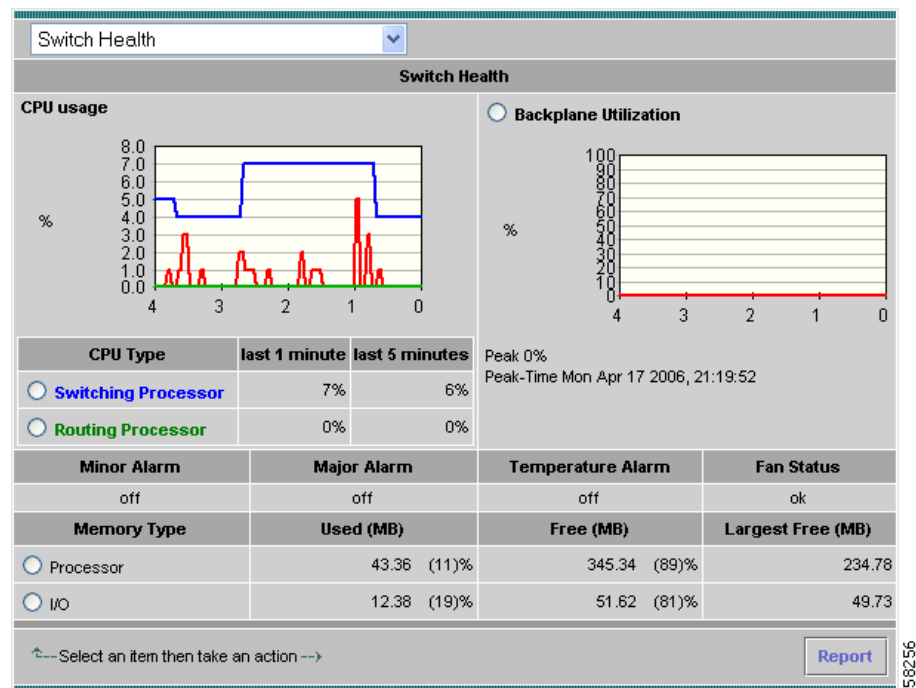
The Switch Health window displays with a drop-down menu that provides the following options:

- [Switch Health](#)
- [Switch Information](#)
- [Crossbar Switching Fabric](#)
- [Ternary Content Addressable Memory Information](#)

## Switch Health

The Switch Health window ([Figure 4-56](#)) displays two real-time graphs.

**Figure 4-56**      **Switch Health Window**



**CPU usage within the last five seconds**

CPU type

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

**Traffic Bandwidth**

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

The Switch 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 4-54 Switch Memory Information**

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

**Switch Information**

The Switch Information window ([Figure 4-57](#)) displays.

**Figure 4-57 Switch Information Window**

|                                                   |                               |                               |
|---------------------------------------------------|-------------------------------|-------------------------------|
| Switch Information                                |                               |                               |
| <b>Switch Information</b>                         |                               |                               |
| Name: namlab-sup6.cisco.com.cisco.com             |                               |                               |
| Hardware: Cisco Systems WS-C6509 9 slot switch    |                               |                               |
| Backplane: giga16                                 |                               |                               |
| Supervisor Software Version: CatOS Version 8.4(1) |                               |                               |
| UpTime: 24 days, 6 hours, 09 minutes              |                               |                               |
| Location: N/A                                     |                               |                               |
| Contact: N/A                                      |                               |                               |
| Modem: Disabled                                   |                               |                               |
| Baud: 9600                                        |                               |                               |
| <b>Power Supply</b>                               | <b>Type</b>                   | <b>Status</b>                 |
| 1                                                 | wscac1300                     | ok                            |
| 2                                                 | none                          | other                         |
| <b>Power Redundancy Mode</b>                      | <b>Total (centiAmpsAt42v)</b> | <b>Drawn (centiAmpsAt42v)</b> |
| redundant                                         | 2746                          | 2368                          |

129641

**Table 4-55 Switch Information**

| Field                       | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.                                                                        |
| Hardware                    | A textual description which should contain the manufacturer's name for the physical entity and be set to a distinct value for each version or model of the physical entity. |
| Backplane                   | The chassis backplane type.                                                                                                                                                 |
| Supervisor Software Version | The full name and version identification of the system's software operating-system and networking software.                                                                 |
| UpTime                      | The time (in hundredths of a second) since the network management portion of the system was last re-initialized.                                                            |
| Location                    | The physical location of this node.                                                                                                                                         |
| Contact                     | The textual identification of the contact person for this managed node and information on how to contact this person.                                                       |
| Modem                       | Indicates whether the RS-232 port modem control lines are enabled.                                                                                                          |
| Baud rate                   | The baud rate in bits per second of the RS-232 port.                                                                                                                        |
| Power Supply                | Description of the power supply being instrumented.                                                                                                                         |
| Power Supply Type           | The power supply source:<br>unknown<br>ac<br>dc<br>externalPowerSupply<br>internalRedundant                                                                                 |
| Power Supply Status         | The current state of the power supply being instrumented.<br>1: normal<br>2: warning<br>3: critical<br>4: shutdown<br>5: notPresent<br>6: notFunctioning                    |
| Power Redundancy Mode       | Power Redundancy Mode:<br>The power-supply redundancy mode.<br>1: not supported<br>2: redundant<br>3: combined                                                              |

**Table 4-55 Switch Information**

| Field       | Description                                                                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power Total | Total current available for FRU usage.<br><br>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.<br><br>When Redundancy Mode is combined, the total current available will be the sum of the capacities of all operating power supplies. |
| Power Drawn | Total Current Drawn by powered-on FRUs.                                                                                                                                                                                                                                                                                                                   |

## Crossbar Switching Fabric

This option shows the Crossbar Switching Fabric information.

**Table 4-56 Crossbar Switching Fabric Information**

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crossbar Switching Fabric | Physical and configuration information about the module:<br><br><b>Active slot</b> —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.<br><br><b>Backup slot</b> —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.<br><br><b>Bus Only Mode Allowed</b> —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.<br><br><b>Truncated Mode Allowed</b> —Indicates whether truncated mode is administratively enabled on the device or not. |
| Module Switching Mode     | Indicates switching mode of the module:<br><br><b>busmode</b> —Module does not use fabric. Backplane is used for both lookup and data forwarding.<br><br><b>crossbarmode</b> —Module uses the backplane for forwarding decision and fabric for data forwarding.<br><br><b>dcefmode</b> —Module uses fabric for data forwarding and local forwarding is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Module-Channel            | Module slot number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Module-Status             | Status of the fabric channel at the module                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fabric Status             | Status of the fabric channel at the slot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Speed (MB)                | Speed (MB/second) of the module                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



**Table 4-56** Crossbar Switching Fabric Information (continued)

| Field               | Description                                                                            |
|---------------------|----------------------------------------------------------------------------------------|
| Module-Channel      | Channel for the module                                                                 |
| In Errors           | The total number of error packets received since this entry was last initialized.      |
| Our Errors          | The total number of error packets transmitted since this entry was last initialized.   |
| Dropped             | The total number of dropped packets transmitted since this entry was last initialized. |
| In Utilization (%)  | Input utilization of the channel for the module.                                       |
| Our Utilization (%) | Output utilization of the channel for the module.                                      |

## Ternary Content Addressable Memory Information

Shows the Ternary Content Addressable Memory (TCAM) (Figure 4-58) usage information. Table 4-57 lists and describes the TCAM information.

**Figure 4-58** Ternary Content Addressable Memory Information

| Ternary Content Addressable Memory Usage |      |        |
|------------------------------------------|------|--------|
| Resource Type                            | Used | Free   |
| Security Acl Mask Module 1               | 7    | 4081   |
| Security Acl Value Module 1              | 16   | 32688  |
| Dynamic Security Acl Mask Module 1       | 1    | 95     |
| Dynamic Security Acl Value Module 1      | 8    | 760    |
| Qos Acl Mask Module 1                    | 0    | 4086   |
| Qos Acl Value Module 1                   | 0    | 32688  |
| Dynamic Qos Acl Mask Module 1            | 0    | 256    |
| Dynamic Qos Acl Value Module 1           | 0    | 2048   |
| Layer 4 Port Operator Module 1           | 0    | 64     |
| Interface Mapping Module 1               | 2    | 507    |
|                                          |      | 129643 |

**Table 4-57** Ternary Content Addressable Memory Information

| Field                      | Description                                                             |
|----------------------------|-------------------------------------------------------------------------|
| Security Acl Mask          | Indicates that TCAM space is allocated to store ACL masks.              |
| Security Acl Value         | Indicates that TCAM space is allocated to store ACL value.              |
| Dynamic Security Acl Mask  | Indicates that TCAM space is allocated to dynamically store ACL masks.  |
| Dynamic Security Acl Value | Indicates that TCAM space is allocated to dynamically store ACL values. |
| Qos Acl Mask               | Indicates that TCAM space is allocated to store QoS masks.              |
| Qos Acl Value              | Indicates that TCAM space is allocated to store QoS value.              |

**Table 4-57 Ternary Content Addressable Memory Information (continued)**

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

## Router Health

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

- [Router Health](#)
- [Router Information](#)

## Router Health

The Router Health window displays a real-time graph and out information about the health of a router as shown in [Figure 4-59](#). [Table 4-58](#) describes the contents of the Router Health window.

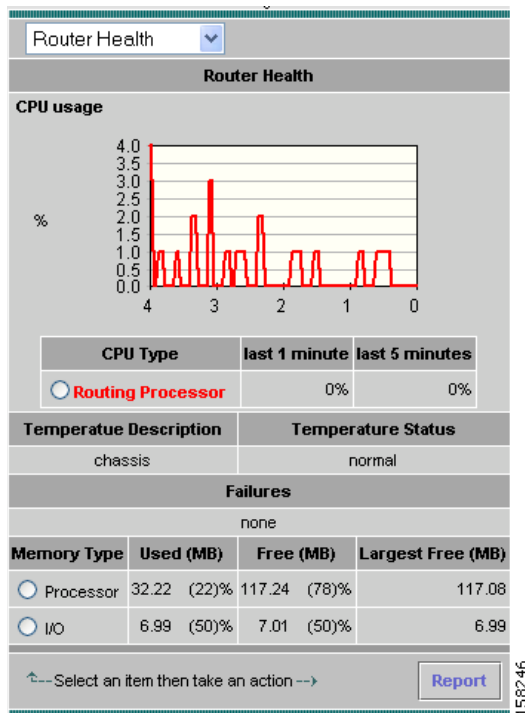
**Figure 4-59 Router Health Window**

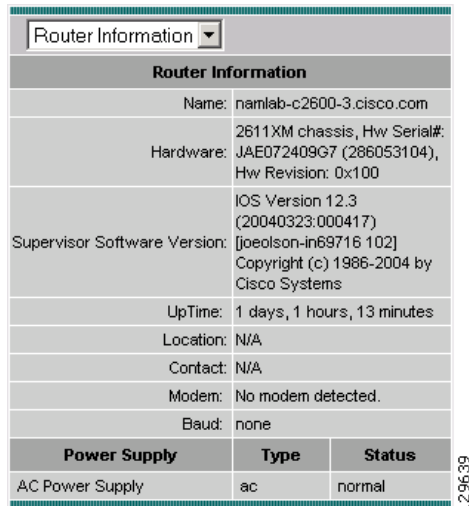
**Table 4-58 Router Health Information**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Usage (graph)       | Overall CPU busy percentage in the last 5 second period                                                                                                                                                                                                                                                                                                                                                                                           |
| CPU Type                | Describes type of CPU being monitored                                                                                                                                                                                                                                                                                                                                                                                                             |
| Last 1 minute           | Overall CPU busy percentage in the last 1 minute period.                                                                                                                                                                                                                                                                                                                                                                                          |
| Last 5 minutes          | Overall CPU busy percentage in the last 5 minute period.                                                                                                                                                                                                                                                                                                                                                                                          |
| Temperature Description | Description of the test point being measured                                                                                                                                                                                                                                                                                                                                                                                                      |
| Temperature Status      | <p>The current state of the test point being instrumented; one of the following are the states:</p> <ul style="list-style-type: none"> <li>• Normal</li> <li>• Warning</li> <li>• Critical</li> <li>• Shutdown</li> <li>• Not Present</li> <li>• Not Functioning</li> <li>• Unknown</li> </ul>                                                                                                                                                    |
| Failures                | <p>The failing component of the power supply being measured:</p> <ul style="list-style-type: none"> <li>• None—No failure</li> <li>• inputVoltage—Input power lost in one of the power supplies</li> <li>• dcOutputVoltage—DC output voltage lost in one of the power supplies</li> <li>• Thermal—Power supply thermal failure.</li> <li>• Multiple—Multiple failures.</li> <li>• Fan—Fan failure</li> <li>• Overvoltage—Over voltage.</li> </ul> |
| Memory Type             | Type of memory including processor and I/O.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Used                    | Number of used MB for a particular memory type.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Free                    | Number of free MB for a particular memory type.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Largest Free            | Number of largest contiguous free MB for a particular memory type.                                                                                                                                                                                                                                                                                                                                                                                |

## Router Information

The Router Information window (Figure 4-60) displays router information. Table 4-59 lists and describes the fields of the Router Information window.

**Figure 4-60 Router Information Window**



| Router Information           |                                                                                                          |        |
|------------------------------|----------------------------------------------------------------------------------------------------------|--------|
| Name:                        | namlab-c2600-3.cisco.com                                                                                 |        |
| Hardware:                    | 2611XM chassis, Hw Serial#: JAE072409G7 (286053104), Hw Revision: 0x100                                  |        |
| Supervisor Software Version: | IOS Version 12.3 (20040323:000417)<br>[joeolson-in69716 102]<br>Copyright (c) 1986-2004 by Cisco Systems |        |
| UpTime:                      | 1 days, 1 hours, 13 minutes                                                                              |        |
| Location:                    | N/A                                                                                                      |        |
| Contact:                     | N/A                                                                                                      |        |
| Modem:                       | No modem detected.                                                                                       |        |
| Baud:                        | none                                                                                                     |        |
| Power Supply                 | Type                                                                                                     | Status |
| AC Power Supply              | ac                                                                                                       | normal |

**Table 4-59 Router Information**

| Field                       | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Name an administrator assigned to this managed node, this is the node's fully-qualified domain name.                                                                        |
| Hardware                    | A textual description which should contain the manufacturer's name for the physical entity and be set to a distinct value for each version or model of the physical entity. |
| Supervisor Software Version | The full name and version identification of the system's software operating-system and networking software.                                                                 |
| Up Time                     | The time (in hundredths of a second) since the network management portion of the system was last re-initialized.                                                            |
| Location                    | The physical location of this node.                                                                                                                                         |
| Contact                     | The textual identification of the contact person for this managed node and information on how to contact this person.                                                       |
| Modem                       | Indicates whether the RS-232 port modem control lines are enabled.                                                                                                          |
| Baud                        | The baud rate in bits per second of the RS-232 port.                                                                                                                        |
| Power Supply                | Description of the power supply being instrumented.                                                                                                                         |

**Table 4-59 Router Information**

| Field               | Description                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power Supply Type   | The power supply source:<br>unknown<br>ac<br>dc<br>externalPowerSupply<br>internalRedundant                                                              |
| Power Supply Status | The current state of the power supply being instrumented.<br>1: normal<br>2: warning<br>3: critical<br>4: shutdown<br>5: notPresent<br>6: notFunctioning |

## Viewing NBAR

You can use the NAM Traffic Analyzer to view Network Based Application Recognition (NBAR) data. To view the NBAR data collected for a switch or router, select **Monitor > Router** or **Switch > NBAR**.

The NBAR Current Rates Table displays with three radio buttons above it.

You can click a radio button for:

- [Viewing the NBAR Current Rates Table, page 4-111.](#)
- [Viewing the Top N NBAR Chart, page 4-112.](#)
- [Viewing the NBAR Cumulative Data Table, page 4-113.](#)

## Viewing the NBAR Current Rates Table

The NBAR Current Rates table enables you to view the protocol data collected for the device. The information displayed represents the data collected per second over the last time interval. For information on setting the time interval, see the [“Setting Global Preferences” section on page 3-94.](#)

To view the NBAR Current Rates table:

- 
- Step 1** Click the Current Rates radio button.
- The [NBAR Current Rates Table \(Table 4-60\)](#) displays.

**Table 4-60 NBAR Current Rates Table**

| Field         | Description                             |
|---------------|-----------------------------------------|
| Protocol/s    | Protocol type.                          |
| In Packets/s  | Number of packets collected per second. |
| Out Packets/s | Number of packets sent out per second.  |

**Table 4-60 NBAR Current Rates Table (continued)**

| Field          | Description                           |
|----------------|---------------------------------------|
| In Bytes/s     | Number of bytes collected per second. |
| Out Bytes/s    | Number of bytes sent out per second.  |
| In Bit rate/s  | In bound bit rate per second.         |
| Out Bit rate/s | Out bound bit rate per second.        |

**Step 2** (Optional) Enter the protocol name to filter in the Filter text box, then click **Filter**.

The specified protocol displays.

**Step 3** (Optional) Choose the interface name in the drop-down box.

The specified interface displays.

**Step 4** (Optional) Choose a protocol and click Real-Time.

A Real-Time graph of the specified protocol displays.



**Tip**

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

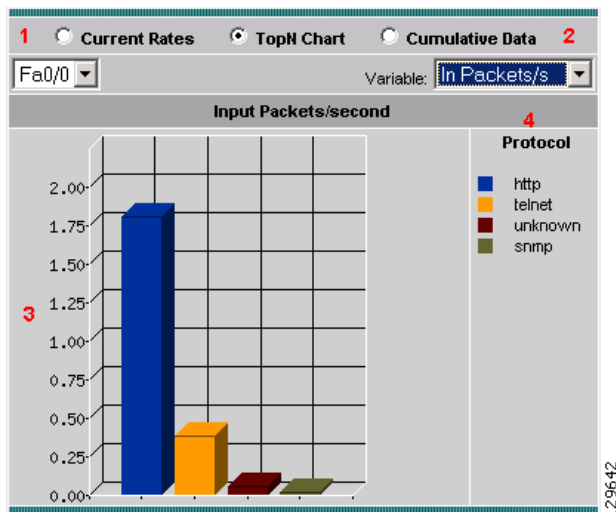
## Viewing the Top N NBAR Chart

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

To view the NBAR Top N chart:

**Step 1** Click the TopN Chart radio button.

The [Top N NBAR Chart \(Figure 4-61\)](#) displays.

**Figure 4-61 Top N NBAR Chart**

|   |                                                                                                 |   |                                               |
|---|-------------------------------------------------------------------------------------------------|---|-----------------------------------------------|
| 1 | Interface list (for example, Fa0/0)                                                             | 3 | Variable value (per second) for each protocol |
| 2 | Variable list (In Packets/s, Out Packets/s, In Bytes/s, Out Bytes/s, In Bit Rate, Out Bit Rate) | 4 | Top N protocols                               |

**Step 2** Choose an interface from the Interface list:

**Step 3** Choose one of the following from the Variable list:

- In Packets/s—Sorts the interface number based on the number of in packets/s.
- Out Packets/s—Sorts the interface number based on the number of out packets/s.
- In Bytes/s—Sorts the interface number based on the number of in bytes/s.
- Out Bytes/s—Sorts the interface number based on the number of out bytes/s.
- In Bit Rate—Sorts the interface number based on the in bit rate.
- Out Bit Rate—Sorts the interface number based on the out bit rate.



**Tip**

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

## Viewing the NBAR Cumulative Data Table

The NBAR Cumulative Data table enables you to view the various data collected for the switch or router. The information displayed represents the total data collected since the collection was created or since the NAM was restarted. For information on setting the time interval, see [Setting Global Preferences](#), page 3-94.

To view the NBAR Cumulative Data table:

- Step 1** Click the Cumulative Data radio button.  
The [NBAR Cumulative Data Table](#) (Table 4-61) displays.

**Table 4-61** *NBAR Cumulative Data Table*

| Field          | Description                             |
|----------------|-----------------------------------------|
| Protocol       | Name of protocol.                       |
| In Packets/s   | Number of packets collected per second. |
| Out Packets/s  | Number of packets sent out per second.  |
| In Bytes/s     | Number of bytes collected per second.   |
| Out Bytes/s    | Number of bytes sent out per second.    |
| In Bit rate/s  | In bound bit rate per second.           |
| Out Bit rate/s | Out bound bit rate per second.          |

- Step 2** (Optional) Enter the protocol name to filter in the Filter text box, then click **Filter**.  
The specified protocol displays.
- Step 3** (Optional) Choose the interface name in the drop-down box.  
The specified interface displays.
- Step 4** (Optional) Choose a protocol and click Real-Time.  
A Real-Time graph of the specified protocol displays.



# Viewing MPLS Traffic Statistics

When data packets containing MPLS tag are spanned to the NAM, the traffic can be monitored by the tag inside the data packet. This feature is especially useful in a network that deploys MPLS/VPN where each VPN is uniquely identified by an MPLS tag. When NAM encounters stacked MPLS tags, only the relevant inner-most tag is used for monitoring.

This section describes the following topics:

- [Viewing VRF Statistics, page 4-115](#)
- [Viewing Virtual Circuit Statistics, page 4-116](#)
- [Viewing All Labels, page 4-117](#)

## Viewing VRF Statistics

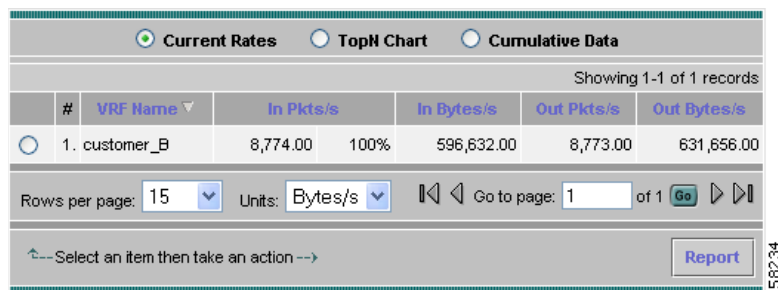
To view VRF statistics:

- Step 1** Click **Monitor > MPLS**.
- Step 2** In the content menu, click **VRF Statistics**.

The GUI displays the MPLS VRF Statistics Current Rates Table, the default view. You can also choose two other display formats, the TopN Chart or Cumulative Data.

VRF statistics are displayed in the same format as shown in [Figure 4-62](#).

**Figure 4-62 VRF Statistics**



| Showing 1-1 of 1 records |            |               |            |            |             |
|--------------------------|------------|---------------|------------|------------|-------------|
| #                        | VRF Name   | In Pkts/s     | In Bytes/s | Out Pkts/s | Out Bytes/s |
| 1.                       | customer_B | 8,774.00 100% | 596,632.00 | 8,773.00   | 631,656.00  |

Rows per page: 15 Units: Bytes/s Go to page: 1 of 1 Go Report

[Table 4-63](#) explains the fields of the VRF Statistics window.

**Table 4-62 VRF Statistics Window**

| Field       | Description                         |
|-------------|-------------------------------------|
| VRF/VC Name | Name of the VRF data source         |
| InPackets   | The number of packets received      |
| In Bytes    | The total number of bytes received  |
| Out Packets | The total number of bytes delivered |
| Out Bytes   | The number of packets delivered     |

## Viewing Virtual Circuit Statistics

**Step 1** Click **Monitor > MPLS**.

**Step 2** In the content menu, click **L2 Virtual Circuit Statistics**.

The GUI displays the MPLS Virtual Circuit Statistics Current Rates Table, the default view. You can also choose two other display formats, the TopN Chart or Cumulative Data.

Virtual Circuit statistics are displayed in the same format as shown in [Figure 4-63](#).

**Figure 4-63 Virtual Circuit Statistics Window**

| <input checked="" type="radio"/> Current Rates <input type="radio"/> TopN Chart <input type="radio"/> Cumulative Data |            |           |            |            |             |
|-----------------------------------------------------------------------------------------------------------------------|------------|-----------|------------|------------|-------------|
| Showing 1-1 of 1 records                                                                                              |            |           |            |            |             |
| #                                                                                                                     | VRF Name   | In Pkts/s | In Bytes/s | Out Pkts/s | Out Bytes/s |
| 1.                                                                                                                    | customer_B | 8,774.00  | 596,632.00 | 8,773.00   | 631,656.00  |
| Rows per page: 15 Units: Bytes/s Go to page: 1 of 1                                                                   |            |           |            |            |             |
| Select an item then take an action -->                                                                                |            |           |            |            |             |
| Report                                                                                                                |            |           |            |            |             |

[Table 4-63](#) explains the fields of the Virtual Circuit Statistics window.

**Table 4-63 Virtual Circuit Statistics Window**

| Field       | Description                         |
|-------------|-------------------------------------|
| VRF/VC Name | Name of the VRF or VC data source   |
| InPackets   | The number of packets received      |
| In Bytes    | The total number of bytes received  |
| Out Packets | The total number of bytes delivered |
| Out Bytes   | The number of packets delivered     |

## Viewing All Labels

To view MPLS traffic statistics,

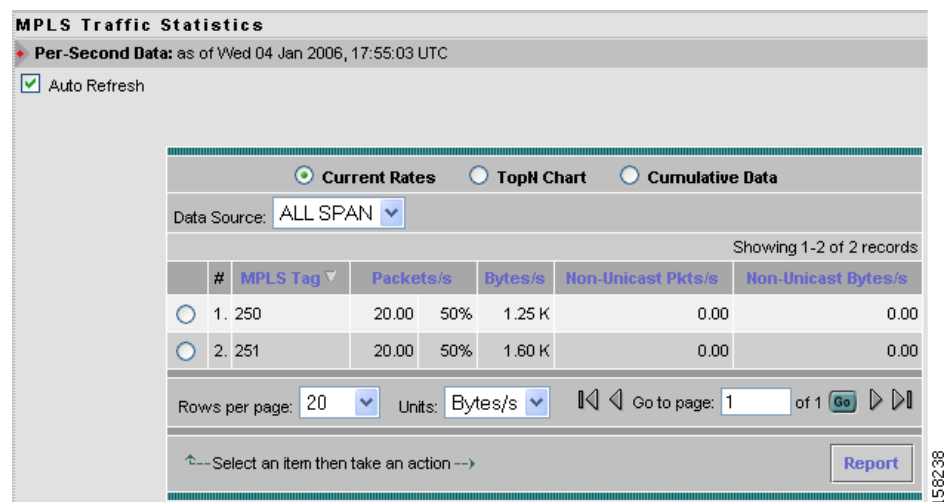
**Step 1** Click **Monitor > MPLS**.

**Step 2** In the content menu, click **All Labels**.

The GUI displays the MPLS Traffic Statistics Current Rates Table, the default view. You can also choose two other display formats, the TopN Chart or Cumulative Data.

Figure 4-64 shows the MPLS Traffic Statistics display for all MPLS-tagged traffic received from the NAM data ports.

**Figure 4-64 Viewing MPLS Traffic Statistics**



### Traffic Statistics per MPLS Tag

Like VLAN monitoring, you should be able to see traffic statistics broken down by tag. MPLS tagged traffic statistics can be monitored by the following:

- Total number of packets
- Total number of bytes
- Total number of non-unicast packets
- Total number of non-unicast bytes

### Custom RMON Data Source

To enable RMON monitoring, you must first configure a data source. To enable monitoring of MPLS traffic, create a form of virtual interface to be tied to a particular MPLS tag. You can select a particular MPLS tag and create a custom data source for that tag.

### Monitoring Application per MPLS Tag

After you create a custom data source, you can enable application monitoring on the data source. This capability gives you insight into the applications being carried using a particular MPLS tag.

### Monitoring Host per MPLS Tag

After you create a custom data source, you can enable host monitoring on this data source. This capability gives you insight into the traffic being generated by hosts using a particular MPLS tag.

### Monitoring Host Conversation per MPLS Tag

After you create a custom data source, you can enable application monitoring on this data source. This capability gives you insight into host conversations being carried using a particular MPLS tag.



# CHAPTER 5

## Creating and Viewing Reports

The reports function allows you to store and retrieve up to 100 days of historical data about the network traffic monitored by the NAM. The Reports window (Figure 5-1) provides options for creating and viewing basic, custom, and scheduled exports. The submenu of the Reports window provides the following options:

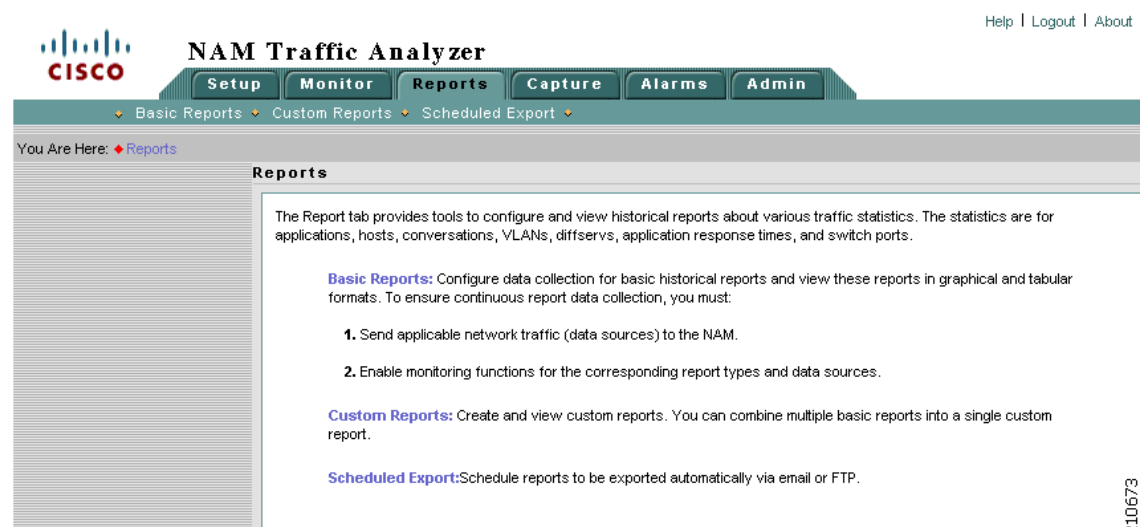
- [Basic Reports, page 5-2](#), enables you to configure data collection for basic historical reports and view these reports in several different formats.
- [Custom Reports, page 5-25](#), enables you to create and view custom reports. You can also combine multiple basic reports into a single custom report.
- [Scheduled Exports, page 5-28](#), enables you to schedule a report to be generated automatically and exported by Email or FTP transfer.



### Note

NAM 4.1 supports IPv6 for all reporting functionality.

**Figure 5-1** Reports Window



210673

# Basic Reports

The Basic Reports option enables you to view reports about a specific target like a network host, a protocol, or the TopN list of the most active hosts or the TopN list of the most active top protocols.

When a basic report is created, a background process periodically polls the datasource and stores the data in the database. You can configure the polling interval when you create the basic report. See the section [Creating a Basic Report, page 5-4](#), for more information.

Figure 5-2 shows an example of the Basic Reports window.

Figure 5-2 Basic Reports Window

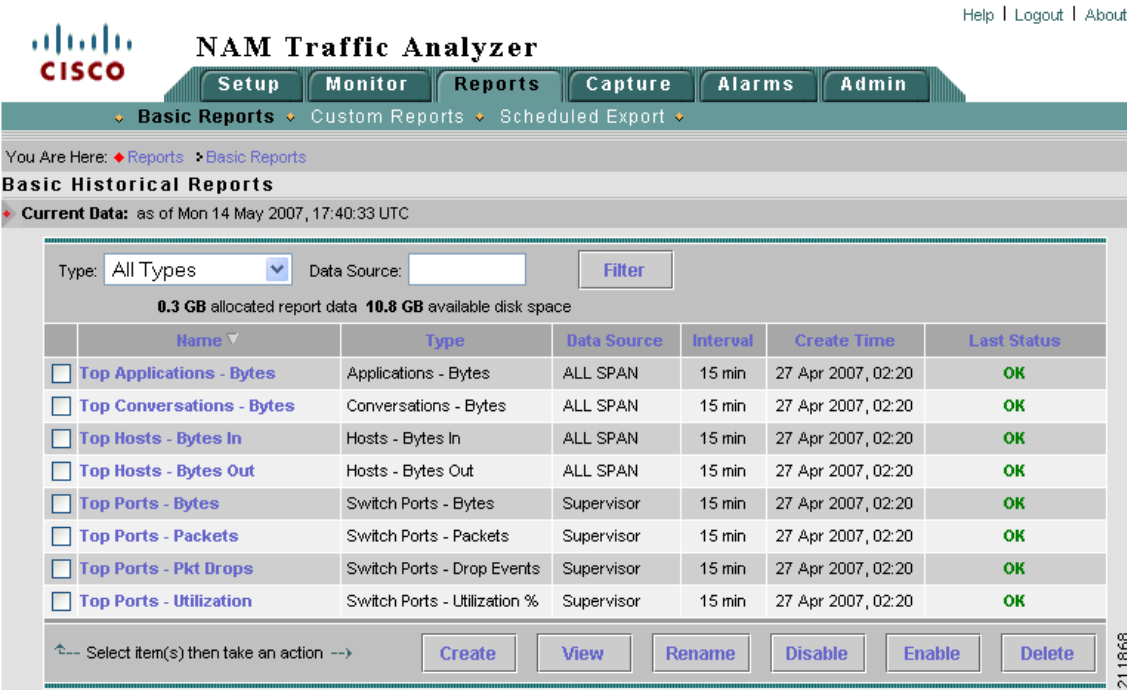


Table 5-1 lists and describes the fields of the Basic Reports window.

Table 5-1 Basic Reports Table

| Field             | Description                                               |
|-------------------|-----------------------------------------------------------|
| Basic Report Type | Filters the list of reports by report type                |
| Name              | Name of the basic report                                  |
| Type              | Type of the report data                                   |
| Data Source       | The data source from which the report data were collected |

**Table 5-1 Basic Reports Table (continued)**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interval    | <p>The polling interval of the report data collection. The default is 15 minutes. A more frequent polling interval allows the report to have finer granularity but requires more data storage space.</p> <p><b>Note</b> Polling intervals are based on a 60-minute clock that begins at the top of the hour. If you use the default polling interval and start collecting data for a report at seven minutes past the hour, the first polling interval will end at 15 minutes past the hour and have a duration of eight minutes. Similarly, the current polling interval might also show as less than the polling interval.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Create Time | Time the report was created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Last Status | <p><b>Note</b> See <a href="#">Table 5-16, Last Status Conditions</a>, for a complete list status conditions and their definitions.</p> <ul style="list-style-type: none"> <li>• OK—Enabled and data is being collected.</li> <li>• Disabled—No data is being collected.</li> <li>• Pending—Report is enabled, but no data collected.</li> <li>• Inactive Data Source—Data source was deleted.</li> <li>• No Data—No data was collected for this period. This can be due to the report being disabled, the NAM not running, or the Report Data Collection task not running.</li> <li>• No Activity—The NAM does not detect any traffic activity for this target. This might be caused by an inactive target or a data source configuration problem. See <a href="#">Table 5-15</a> or <a href="#">Table 5-16</a> for more information about reports that show no activity.</li> </ul> <p>However for certain monitoring metrics when the system is missing data on errors, special conditions, and similar measurements, the status <i>No Activity</i> is substituted by a more appropriate term such as <i>No Drops Stats</i> or <i>No Concealment Stats</i>.</p> <p>This means there was no information on drops or concealment, but does not imply there was no normal activity during the reported period.</p> <ul style="list-style-type: none"> <li>• Not Monitored—The monitoring function for this type of traffic statistic is not enabled or is not available for the NAM and/or switch.</li> </ul> <p><b>Note</b> If no data was collected, a time stamp displays the last collection.</p> |

WS-SVC-NAM-1 and WS-SVC-NAM-2 devices have the following reports created by default:

- Top Applications—Bytes
- Top Conversations—Bytes
- Top Hosts—Bytes In
- Top Hosts—Bytes Out
- Top Ports—Bytes
- Top Ports—Packets

- Top Ports—Packet Drops
- Top Ports—Utilization

NME-NAM devices have the following reports created by default:

- Top Applications—Bytes
- Top Conversations—Bytes
- Top Hosts—Bytes In
- Top Hosts—Bytes Out
- Top Interfaces—Bytes In
- Top Interfaces—Bytes Out
- Top Interfaces—Utilization In
- Top Interfaces—Utilization Out

NAM appliances have the following reports created by default:

- Top Applications—Bytes
- Top Conversations—Bytes
- Top Hosts—Bytes In
- Top Hosts—Bytes Out
- Top Ports—Bytes
- Top Ports—Packets
- Top Ports—Packet Drops
- Top Ports—Utilization


**Note**

If you turn off collections on a data source on which a report is running, the reports function will automatically turn the collections back on.

The following sections describe how to manage your basic reports:

- [Creating a Basic Report, page 5-4](#)
- [Viewing Basic Reports, page 5-20](#)
- [Renaming a Report, page 5-25](#)
- [Enabling Reports, page 5-24](#)
- [Disabling Reports, page 5-25](#)
- [Deleting a Report, page 5-25](#)

Basic reports can be customized and combined to create custom reports. See [Custom Reports, page 5-25](#), for more information about customized reports.

## Creating a Basic Report

Before you can create reports, you should make sure the applicable network traffic is being sent to the NAM and that monitoring functions are enabled for the type of statistic and data sources. For more information on enabling monitoring functions, see the [“Monitoring” section on page 3-54](#).



To create a basic report:

---

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#). Using a NAM-1 or NAM-2 device, you can create the following reports:

- Applications—See [Creating an Applications Report](#), page 5-6
- Application Groups—See [Creating an Application Groups Report](#), page 5-8
- Hosts—See [Creating a Hosts Report](#), page 5-8
- Conversations—See [Creating a Conversations Report](#), page 5-10
- VLANs—See [Creating a VLANs Report](#), page 5-11
- Differentiated Services—See [Creating a DiffServ Report](#), page 5-12
- Response Time—See [Creating a Response Time Report](#), page 5-13
- Switch Port—See [Creating a Switch Port Report](#), page 5-14
- Switch Health—[Creating a Switch Health Report](#), page 5-15
- MPLS—See [Creating an MPLS Stats Report](#), page 5-18
- Voice Over IP/RTP Stream Statistics—[Creating a Voice Over IP/RTP Stream Report](#), page 5-19

Using NME-NAM devices, you can create the following reports:

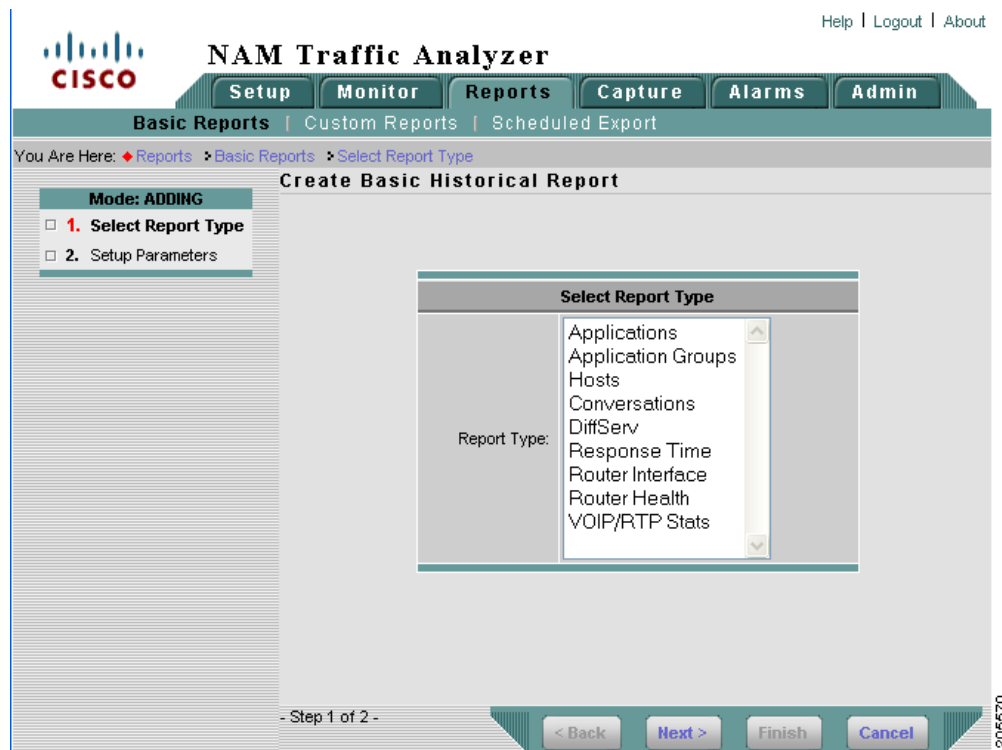
- Applications—See [Creating an Applications Report](#), page 5-6
- Application Groups—See [Creating an Application Groups Report](#), page 5-8
- Hosts—See [Creating a Hosts Report](#), page 5-8
- Conversations—See [Creating a Conversations Report](#), page 5-10
- Differentiated Services—See [Creating a DiffServ Report](#), page 5-12
- Response Time—See [Creating a Response Time Report](#), page 5-13
- Router Interface—See [Creating a Router Interface Report](#), page 5-16
- Router Health—[Creating a Router Health Report](#), page 5-17
- Voice Over IP/RTP Stream Statistics—[Creating a Voice Over IP/RTP Stream Report](#), page 5-19

**Step 3** Choose the report type, then click **Next**.

**Step 4** Enter the parameters required for your selected report type.

**Step 5** Click **Finish**.

---

**Figure 5-3** Creating a Basic Historical Report

## Creating an Applications Report

To create an Application Protocols report:

- 
- Step 1** Click **Reports > Basic Reports**.  
The Basic Historical Reports window displays.
- Step 2** Click **Create**.  
The Create Basic Historical Report window displays as shown in [Figure 5-3](#).
- Step 3** Choose **Applications**, then click **Next**.  
The Create Applications Report window displays as shown in [Figure 5-4](#).

**Figure 5-4 Create Application Report Window**

Table 5-2 describes the Applications report parameters.

**Table 5-2 Applications Report Parameters**

| Field                          | Description                                                                          | Usage Notes                                                                                                                   |
|--------------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Application                    | Application check box                                                                | Check Application (the default) to choose a specific application (Encapsulation and Protocol).                                |
| Encapsulation                  | Protocol encapsulation type                                                          | Choose an encapsulation from the list of IP, IPIP4, GRE.IP, IPv6, or Others.                                                  |
| Protocol                       | Name of the application protocol.                                                    | Choose a protocol from the list.                                                                                              |
| TopN Applications              | Reports on most active application protocols based on bytes/second or packets/second | Check TopN Applications to create a report about the most active applications.                                                |
| TopN Application TCP/UDP Ports | Reports on most active TCP and UDP ports based on bytes/second or packets/second     | Check TopN Application TCP/UDP Ports to create a report about the most active TCP and UDP ports.                              |
| <b>Report Settings</b>         |                                                                                      |                                                                                                                               |
| Report Name                    | Name of the report.                                                                  | The report name is generated automatically. To change the name of the report, select <b>Customized</b> , then enter the name. |
| Data Type                      | The type of data.                                                                    | Choose a type from the list.                                                                                                  |
| Polling Interval               | The interval in which the report data will be polled                                 | Choose an interval from the list.                                                                                             |
| Data Source                    | The network traffic source from which report data will be collected                  | Choose a source from the list.                                                                                                |

**Step 4** Enter the parameters required for an Applications report.

**Step 5** Click **Finish**.

### Creating an Application Groups Report

To create an Application Groups report:

- Step 1** Choose **Reports > Basic Reports**.  
The Basic Historical Reports window displays.
- Step 2** Click **Create**.  
The Create Basic Historical Report window as shown in [Figure 5-3](#) displays.
- Step 3** Choose Application Group type, then click **Next**.  
The Create Application Group Report Parameters dialog box displays. [Table 5-3](#) describes the Application Group report parameters.

**Table 5-3 Application Group Report Parameters**

| Field             | Description                                                          | Usage Notes                                                                                                                   |
|-------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Application Group | Name of the application group.                                       |                                                                                                                               |
| Report Name       | Name of the report.                                                  | The report name is generated automatically. To change the name of the report, select <b>Customized</b> , then enter the name. |
| Data Type         | The type of data.                                                    | Choose a type from the list.                                                                                                  |
| Polling Interval  | The interval in which the report data will be polled.                | Choose an interval from the list.                                                                                             |
| Data Source       | The network traffic source from which report data will be collected. | Choose a source from the list.                                                                                                |

- Step 4** Enter the required parameters required for an Application Group report.
- Step 5** Click **Finish**.

### Creating a Hosts Report

To create a Hosts report:

- Step 1** Click **Reports > Basic Reports**.  
The Basic Historical Reports window displays.
- Step 2** Click **Create**.  
The Create Basic Historical Report window displays as shown in [Figure 5-3](#).
- Step 3** Choose the Hosts report type, then click **Next**.  
The Create Hosts Report window displays as shown in [Figure 5-5](#).

**Figure 5-5 Create Hosts Report Window**

Table 5-4 describes the Hosts report parameters.

**Table 5-4 Hosts Report Parameters Dialog Box**

| Field                   | Description                                                                                         | Usage Notes                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Host Name or IP Address | The name of the host from which data is polled                                                      | Enter the host name or IP address of the host.                                                                        |
| Host Application        | Check to report on a specific application of the host                                               | When checked, choose protocol and encapsulation type.                                                                 |
| Encapsulation           | Protocol encapsulation type                                                                         | Choose an encapsulation from the list.                                                                                |
| Protocol                | Name of the application protocol                                                                    | Choose a protocol from the list (optional).                                                                           |
| TopN Hosts              | Reports on most active host address based on bytes/second (in or out) or packets/second (in or out) | Check TopN Hosts to create a report about the most active hosts                                                       |
| <b>Report Settings</b>  |                                                                                                     |                                                                                                                       |
| Report Name             | Name of the report                                                                                  | The name of the report is generated generated. To change the name, click <b>Customized</b> , then enter the new name. |
| Data Type               | The type of data                                                                                    | Choose a type from the list                                                                                           |
| Polling Interval        | The interval in which the report data will be polled                                                | Choose an interval from the list                                                                                      |
| Data Source             | The network traffic source from which report data will be collected                                 | Choose a source from the list                                                                                         |

**Step 4** Enter the parameters required for a Hosts report.

**Step 5** Click **Finish**.

# Creating a Conversations Report

To create a Conversations report:

- Step 1

Click **Reports > Basic Reports**.  
The Basic Historical Reports window displays.
- Step 2

Click **Create**.  
The Create Basic Historical Report window displays as shown in [Figure 5-3](#).
- Step 3

Choose **Conversations**, then click **Next**.  
The Create Host Conversation Report window displays as shown in [Figure 5-6](#).

**Figure 5-6** Create Host Conversation Report Window

[Table 5-5](#) describes the Conversations report parameters.

**Table 5-5** Conversations Report Parameters

| Field              | Description                                                  | Usage Notes                                                                                                                                                        |
|--------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conversation       | Conversation check box                                       | Check Conversation (the default) to enter specific host names or IP addresses.                                                                                     |
| Host 1 and Host 2  | The identification of the conversation hosts to be reported. | <ul style="list-style-type: none"> <li>Host 1—Enter the host name or IP address of host 1.</li> <li>Host 2—Enter the host name or IP address of host 2.</li> </ul> |
| Encapsulation      | Protocol encapsulation type.                                 | Choose an encapsulation from the list.                                                                                                                             |
| Protocol           | Name of the application protocol.                            | Choose a protocol from the list.                                                                                                                                   |
| TopN Conversations | TopN Conversations check box                                 | Check TopN Conversations to create a report about the most active host conversations based on bytes/second or packets/second.                                      |

**Table 5-5** Conversations Report Parameters (continued)

| Field                         | Description                                                          | Usage Notes                                                                                                                                                                 |
|-------------------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Top Conversations (App-Layer) | Top Conversations (Application Layer) check box                      | Check Top Conversations (App-Layer) to create a report about the most active host conversations based on bytes/second or packets/second occurring in the application layer. |
| <b>Report Settings</b>        |                                                                      |                                                                                                                                                                             |
| Report Name                   | Name of the report.                                                  | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name.                                                          |
| Data Type                     | The type of data.                                                    | Choose a type from the list.                                                                                                                                                |
| Polling Interval              | The interval in which the report data will be polled.                | Choose an interval from the list.                                                                                                                                           |
| Data Source                   | The network traffic source from which report data will be collected. | Choose a source from the list.                                                                                                                                              |

**Step 4** Enter the parameters required for the Conversations report.

**Step 5** Click **Finish**.

## Creating a VLANs Report



### Note

This section is not applicable to NM-NAM or NME-NAM devices.

To create a VLAN report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose the VLAN report type, then click **Next**.

The Create VLAN Report Parameters dialog box displays. [Table 5-6](#) describes the VLAN report parameters.



### Note

VLAN reports are not available for NetFlow data sources.

**Table 5-6** VLAN Report Parameters

| Field       | Description                                | Usage Notes                                       |
|-------------|--------------------------------------------|---------------------------------------------------|
| VLAN Number | Name or number of the VLAN to be reported. | Enter the VLAN name or number.                    |
| Top N VLANs | Reports the top N VLANs.                   | Click to select the reporting of the top N VLANs. |

**Table 5-6** VLAN Report Parameters (continued)

| Field            | Description                                                          | Usage Notes                                                                                                                              |
|------------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Report Name      | Name of the report.                                                  | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name.                       |
| Data Type        | The type of data.                                                    | Choose a type from the list.                                                                                                             |
| Polling Interval | The interval in which the report data will be polled.                | Choose an interval from the list.                                                                                                        |
| Data Source      | The network traffic source from which report data will be collected. | Choose a source from the list.<br><b>Note</b> Supervisor engine module- based data sources require Supervisor II engine module or later. |

**Step 4** Enter the parameters required for a VLAN report.

**Step 5** Click **Finish**.

## Creating a DiffServ Report

To create a Differentiated Services (DiffServ) report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose the **DiffServ**, then click **Next**.

The Create DiffServ Report Parameters dialog box displays. [Table 5-7](#) describes the DiffServ parameters.

**Table 5-7** Differentiated Services Report Parameters

| Field                | Description                                                                             | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiffServ Information | The identification of the differentiated services (DiffServ) statistics to be reported. | <ul style="list-style-type: none"> <li>DiffServ Profile—Choose the name of the DiffServ profile.</li> <li>Aggregation Group—Choose the aggregation group.</li> <li>Encapsulation—If the Protocol checkbox is selected, select an encapsulation from the list.</li> <li>Protocol—If the Protocol checkbox is selected, select a protocol from the list.</li> <li>Host Name—If the Host checkbox is selected, enter the hostname or IP address of the host (optional).</li> </ul> |
| Report Name          | Name of the report.                                                                     | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name.                                                                                                                                                                                                                                                                                                                                                              |
| Data Type            | The type of data.                                                                       | Choose a type from the list.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



**Table 5-7**      **Differentiated Services Report Parameters**

| Field            | Description                                                          | Usage Notes                                                                            |
|------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Polling Interval | The interval in which the report data will be polled.                | Choose an interval from the list.                                                      |
| Data Source      | The network traffic source from which report data will be collected. | Choose a source from the list.<br><b>Note</b> NetFlow is not an available data source. |

**Step 4** Enter the parameters required for a DiffServ report.

**Step 5** Click **Finish**.

## Creating a Response Time Report

To create an Application Response Time report:

**Step 1** Choose **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose **Response Time**, then click **Next**.

The Create Response Time Report Parameters dialog box displays. [Table 5-8](#) describes the Response Time report parameters.

**Table 5-8**      **Response Time Report Parameters**

| Field                | Description                                                                          | Usage Notes                                                                                                                                                                                                                                                                                     |
|----------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Info     |                                                                                      |                                                                                                                                                                                                                                                                                                 |
| Target Report        | The identification of the application response time (ART) statistics to be reported. | <ul style="list-style-type: none"><li>• Encapsulation—Choose an encapsulation from the list.</li><li>• Protocol—Choose a protocol from the list.</li><li>• Server—Enter the name or IP address of the server.</li><li>• Client—Enter the name or IP address of the client (optional).</li></ul> |
| Top N Servers        | Creates a response time statistics report based on the top network servers.          | Use the radio button to select a report for Top Server or Top N Client/Server networks.                                                                                                                                                                                                         |
| Top N Client/Servers | Creates a response time statistics report based on the top client/server networks.   |                                                                                                                                                                                                                                                                                                 |
| Report Settings      |                                                                                      |                                                                                                                                                                                                                                                                                                 |
| Report Name          | Name of the report.                                                                  | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name.                                                                                                                                                                              |

**Table 5-8**      **Response Time Report Parameters (continued)**

| Field            | Description                                                          | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Type        | The type of data.                                                    | Choose a data type from the list of the following options: Avg App Delay, Avg Nwk Delay, Avg Clt Nwk Delay, Avg Svr Nwk Delay, Avg Transaction, Max App Delay, Max Nwk Delay, Max Clt Nwk Delay, Max Svr NwkDelay, Max Transaction, Min App Delay, Min Nwk Delay, Min Clt Nwk Delay, Min Svr Nwk Delay, Min Transaction, # Transactions, # Connections, # Retries, # Timeout/Late, Client Bytes, Client Packets, Server Bytes, Server Packets, Total Sessions, Closes Conns, Refused Sessions, Unresponsive Conns, Session Duration, Data XmtTime, Retransmission Delay |
| Polling Interval | The interval in which the report data will be polled.                | Choose an interval from the list: 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 8 hours.<br><b>Note</b> The minimum polling interval for TopN report type cannot be set to 1 minute.                                                                                                                                                                                                                                                                                                                                                        |
| Data Source      | The network traffic source from which report data will be collected. | Choose a source from the list.<br><b>Note</b> NetFlow is not an available data source.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Step 4** Enter the parameters required for an Application Response Time report.

**Step 5** Click **Finish**.

## Creating a Switch Port Report



### Note

This section also applies to the Cisco 2200 Series NAM appliances. Menu options for the NAM appliances would use Managed Device Port Report.



### Note

This section is not applicable to NM-NAM or NME-NAM devices.

To create a Switch Port Statistics report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose **Switch Port Statistics** or for the NAM appliance choose **Managed Device Port Statistics**, then click **Next**.

The Create Switch Port Statistics Report Parameters dialog box displays. [Table 5-9](#) describes the Switch Port Statistics parameters.

**Table 5-9 Switch Port Statistics Report Parameters Dialog Box**

| Field              | Description                                                                                                                                                                                                                         | Usage Notes                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Switch Module/Port | List of switch modules and the corresponding ports available on the module.                                                                                                                                                         | Choose a switch module and port to generate reports from.                                                                   |
| Top N Ports        | Reports the top N switch ports.                                                                                                                                                                                                     | Click to select reporting of the top N ports.<br><br>This requires mini-RMON to be enabled on the Supervisor engine module. |
| Report Name        | Name of the report.                                                                                                                                                                                                                 | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name.          |
| Data Type          | Type of data to be reported: <ul style="list-style-type: none"> <li>• Bytes/sec</li> <li>• Packets/sec</li> <li>• Utilization %</li> <li>• Broadcast Bytes/sec</li> <li>• Multicast Bytes/sec</li> <li>• Drop Events/sec</li> </ul> | Choose the data type from the list.                                                                                         |
| Polling Interval   | The interval in which the report data will be polled.                                                                                                                                                                               | Choose an interval from the list.                                                                                           |

**Step 4** Enter the parameters required for the Switch Port Statistics report.

**Step 5** Click **Finish**.

## Creating a Switch Health Report



### Note

This section also applies to the Cisco 2200 Series NAM appliances. Menu options for the NAM appliances would use Managed Device Health Report.



### Note

This section is not applicable to NM-NAM or NME-NAM devices.

A Switch Health report is a historical report about the switch health statistics. To create a Switch Health report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose **Switch Health** or for the NAM appliance choose **Managed Device Health**, then click **Next**.

The Create Switch Statistics Report Parameters dialog box displays. [Table 5-10](#) describes the Switch Health report parameters.

**Table 5-10**      **Switch Statistics Report Parameters Dialog Box**

| Field            | Description                                           | Usage Notes                                                                                                        |
|------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Component        | Component upon which to report                        | Choose from Switch DRAM Memory, Switch Backplane, Switching CPU, or Routing CPU.                                   |
| Report Name      | Name of the report                                    | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name. |
| Data Type        | Type of data to be reported                           | Utilization percentage of the selected component.                                                                  |
| Polling Interval | The interval in which the report data will be polled. | Choose an interval from the list.                                                                                  |

**Step 4**      Enter the parameters required for a Switch Statistics report.

**Step 5**      Click **Finish**.

## Creating a Router Interface Report



### Note

This section is only applicable to NM-NAM or NME-NAM devices.

A router interface report contains a history of a router's interface statistics. To create an Router Interface report:

**Step 1**      Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

**Step 2**      Click **Create**.

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3**      Choose **Router Interfaces**, then click **Next**.

The Create Interface Stats Report Parameters dialog box displays. [Table 5-11](#) describes the Router Interfaces report parameters.

**Table 5-11**      **Router Interfaces Report Parameters**

| Field            | Description                  | Usage Notes                                                                                                        |
|------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Interface        | List of interfaces           | Choose an interface to generate reports from.                                                                      |
| Top N Interfaces | Reports the top N interfaces | Click to select reporting of the top N interfaces.                                                                 |
| Report Name      | Name of the report           | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name. |

**Table 5-11 Router Interfaces Report Parameters (continued)**

| Field            | Description                                      | Usage Notes                                                                                                                                 |
|------------------|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Data Type        | Type of data to be reported                      | Choose the data type from the list: Bytes/sec, Packets/sec, Non-unicasts Packets/sec, Discarded Packets/sec, Error Packets/sec, Utilization |
| Polling Interval | Interval in which the report data will be polled | Choose an interval from the list.                                                                                                           |

**Step 4** Enter the parameters required to create a Router Interfaces report.

**Step 5** Click **Finish**.

## Creating a Router Health Report



### Note

This section applies only to NM-NAM or NME-NAM devices.

A Router Health report is a historical report about the router health statistics. To create a Router Health report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-7](#).

**Step 3** Choose **Router Health**, then click **Next**.

The Setup Router Health Report Parameters dialog box displays. [Table 5-12](#) describes the Router Health Report parameters.

**Figure 5-7 Set Up Router Health Report Parameters**

**Setup Report Parameters**

**Component:** I/O Memory

**Report Settings**

Report Name: I/O Memory ☐ Customized

Data Type: Utilization %

Polling Interval: 15 minutes

**Table 5-12 Router Statistics Report Parameters Dialog Box**

| Field                  | Description                    | Usage Notes                                               |
|------------------------|--------------------------------|-----------------------------------------------------------|
| Component              | Component upon which to report | Choose from Routing CPU, Processor Memory, or I/O Memory. |
| <i>Report Settings</i> |                                |                                                           |

**Table 5-12 Router Statistics Report Parameters Dialog Box (continued)**

| Field            | Description                                           | Usage Notes                                                                                                        |
|------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Report Name      | Name of the report                                    | The report name is automatically generated. To change the report name, click <b>Customized</b> and enter the name. |
| Data Type        | Utilization %                                         | Utilization percentage of the selected component.                                                                  |
| Polling Interval | The interval in which the report data will be polled. | Choose an interval from the list.                                                                                  |

**Step 4** Enter the parameters required for a Switch Statistics report.

**Step 5** Click **Finish**.

## Creating an MPLS Stats Report



### Note

This section is not applicable to NM-NAM or NME-NAM devices.

An MPLS report contains a collection of MPLS data. You can set up a report about a specific MPLS tag. To create an MPLS report:

**Step 1** Click **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** Choose **MPLS Stats**, then click **Next**.

The Create MPLS Report Parameters dialog box displays. [Table 5-13](#) describes the MPLS Report Parameters dialog box.

**Table 5-13 MPLS Stats Report Parameters**

| Field                  | Description                  | Usage Notes                                                                                                      |
|------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------|
| MPLS Type              | Specific MPLS type           | Selects one of VRF, VC, Label, or All Labels; this selects the MPLS data source type.                            |
| Name                   | Name of the MPLS data source | Selects the MPLS data source (if defined) for one of the selected MPLS types.                                    |
| Top N MPLS             | System-wide Top N report     | Selects the system-wide Top N report for one of the selected MPLS types.                                         |
| <i>Report Settings</i> |                              |                                                                                                                  |
| Report Name            | Name of the report.          | Choose one of the following: Bytes/sec (default), Packets/sec, Non-unicast Bytes/sec, or Non-unicast Packets/sec |
| Data Type              | Type of data                 | Choose one of the following: 5 minutes (default), 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 8 hours   |

**Table 5-13 MPLS Stats Report Parameters**

| Field            | Description                                                              | Usage Notes                                                                                                     |
|------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Customized       |                                                                          |                                                                                                                 |
| Polling Interval | The network traffic source from which the report data will be collected. | Choose one of the following: 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, or 8 hours. |

**Step 4** Enter the parameters required for an MPLS report.

**Step 5** Click **Finish**.

## Creating a Voice Over IP/RTP Stream Report

You can configure the NAM to create a report for a specific VOIP phone or to gather report data for the following:

- Worst phones
- Worst calls
- Call Volume
- Top RTP Streams

To create a VOIP/RTP Streams report:

**Step 1** Choose **Reports > Basic Reports**.

The Basic Historical Reports window displays.

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

The Create Basic Historical Report window displays as shown in [Figure 5-3](#).

**Step 3** From the pull-down menu, choose VOIP/RTP Stats.

The Setup Report Parameters window displays as shown in [Figure 5-8, Setup VOIP Report Parameters](#).

**Step 4** Click a radio button to choose the type of report to create.

[Table 5-14, VOIP Report Types](#), describes the different types of reports you can create.

**Table 5-14 VOIP Report Types**

| Report Type       | Description                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------|
| Target VOIP Phone | Enter the IP address of a specific phone to generate a report based on the Metrics and polling interval. |
| Worst Phones      | Creates a report of the worst quality phones based on the Metrics and polling interval.                  |
| Worst Calls       | Creates a report of the worst quality calls based on the Metrics and polling interval.                   |
| Call Volume       | Creates a report of total call volume.                                                                   |
| Top RTP Streams   | Creates a report of Top N RTP Streams based on chosen metrics.                                           |

**Figure 5-8 Setup VOIP Report Parameters**

**Create VOIP Report**

**Setup Report Parameters**

**Report Type**

☒ Target VOIP Phone  
Address:

☐ Worst Phones

☐ Worst Calls

☐ Call Volume

☐ Top RTP Streams

**Report Settings**

Report Name:  ☐ Customized

Metrics:  ▼

Polling Interval:  ▼

**Step 5** Under Report Settings, enter a name for the report.

**Step 6** Use the pull-down menu to choose the Metrics upon which to base the report.

|                      |                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------|
| MOS                  | Mean opinion score is a number from 1 to 5 where the higher number indicates better quality. |
| Jitter               | Delay and delay variation of a call stream                                                   |
| Adjusted Packet Loss | Adjusted percentage of packets lost                                                          |
| Actual Packet Loss   | Actual percentage of packets lost                                                            |
| SSC                  | Seconds of severe concealment                                                                |
| SOC                  | Seconds of concealment                                                                       |

**Step 7** Use the pull-down menu to choose the Polling Interval upon which to base the report.

The Polling Interval determines how often the metrics for the chosen report type are collected. The Polling Interval can be from one minute to eight hours; the default Polling Interval is 15 minutes.

**Step 8** Click **Finish**.

After clicking Finish, the report is added to the list of Basic Reports.

**Step 9** Click to choose the report, then click **Enable** to begin gathering data for the report.

## Viewing Basic Reports

Report data is stored in the NAM database for 100 days. Report data older than 100 days is overwritten sequentially by new report data.

To view a basic report, click **Reports > Basic Reports**.

The Basic Reports Window displays and lists all basic reports that have been set up for data collection as shown in [Figure 5-2](#).

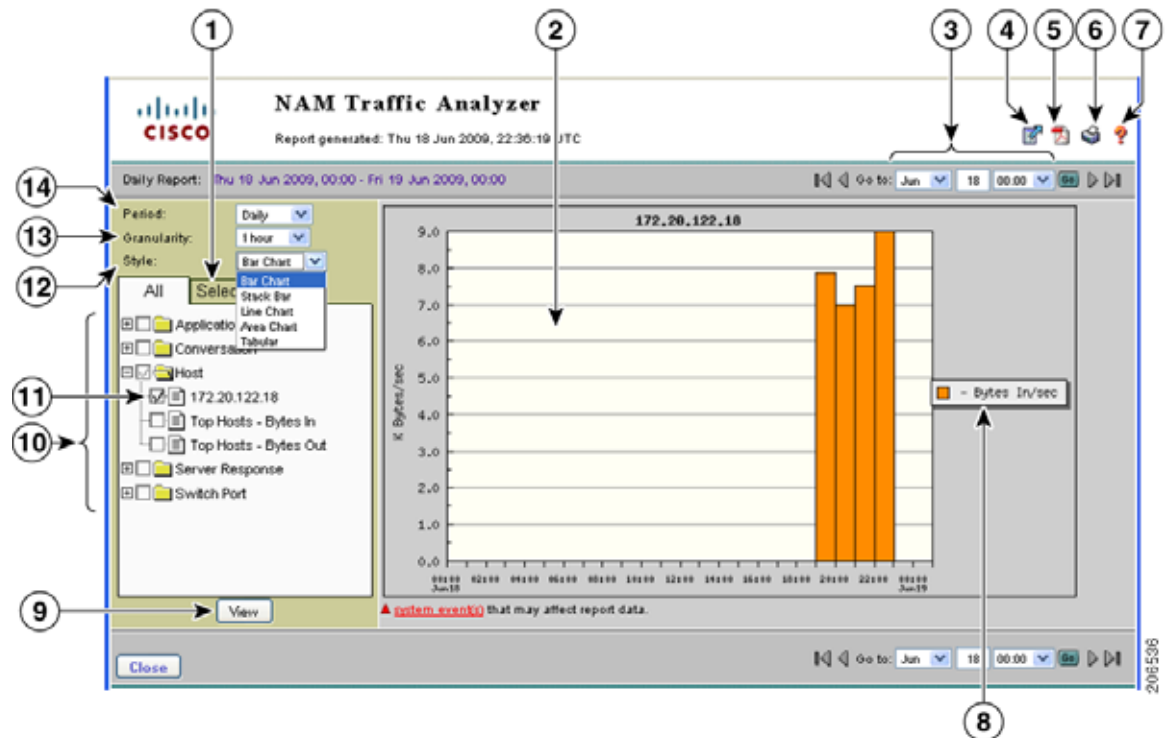


## Viewing Report Details

To view the details of a report, click the report name in the Basic Reports window, or select report and click **View**.

Figure 5-9 shows an example of an Application report window.

**Figure 5-9 Viewing Report Details**



|   |                                   |    |                                                                                                                |
|---|-----------------------------------|----|----------------------------------------------------------------------------------------------------------------|
| 1 | Displays the selected reports.    | 8  | Report type.                                                                                                   |
| 2 | Report graph.                     | 9  | Choose the target reports to be displayed.                                                                     |
| 3 | Navigated between time periods.   | 10 | Report file structure.                                                                                         |
| 4 | Downloads the report to a file.   | 11 | Selected report.                                                                                               |
| 5 | Generates PDF file of the report. | 12 | Style of the graph; not all styles are available for all reports. See <a href="#">Viewing Report Options</a> . |
| 6 | Prints the report.                | 13 | Granularity of the report.                                                                                     |
| 7 | Launches the online help.         | 14 | Length of the report time period.                                                                              |

You can select multiple target reports and display them all in the same graph. If you select multiple reports with different units, they will be displayed as subreports in the report graph area.



### Note

You can select only one Top N report.

## Viewing Report Options

You can view generated reports as tables or graphs. Tables provide exact values, while graphs show bars, area, or line charts with differing orders of magnitude. It is often difficult to determine the actual value of shorter bar graphs when the bar values differ by several orders of magnitude. Smaller bars might not be visible, and zero values are not visible using the bar or area style. Zero values are only apparent in tables and in line charts.

The NAM enables you to view reports in different ways using the menus provided for Period, Granularity, Show, and Style shown in [Figure 5-10](#).

**Figure 5-10 Report Options**

Figure 5-10 shows a 'Report Options' panel with four dropdown menus:

- Period: Daily
- Granularity: 1 hour
- Show: Top 10
- Style: Tabular

A vertical label '200824' is visible on the right side of the panel.

### Period

The Period menu enables you to choose the length of time between reports. The time period might be hourly, daily, every eight hours, every day, every three days, every week, or every month, depending on the requirements for the report.

### Granularity

Report granularity cannot exceed the polling frequency of the report. For example, a report with a 15-minute polling interval cannot be displayed with a 5-minute granularity. If you select a report granularity lower than the polling frequency, the report data will be aggregated accordingly.

### Show

The show menu, when available, enables you to choose among the Top 10, Top 5, Top 3, Top 1 objects of this report to view.

### Style

The style menu enables you to choose from among Bar Chart, Line Chart, Area Chart, Tabular, or Stack Area (stacked) presentation style. Stack Area style limits your report to *showing the Top 10 or less*. Other options such as Top 20 or Top 50 produce reports that cannot be read. Not all reports support the Stack style.

## Disable Reports and Errors

A red exclamation displays in the report selector for disabled reports and reports with error conditions. For more information on reports with error conditions, see [Table 5-15, Report Error Conditions](#). Also see [Table 5-16, Last Status Conditions](#), for a complete list status conditions and what they mean.

**Table 5-15 Report Error Conditions**

| Error Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Not Started     | The report has not been created and data collection has not been started for this time period.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Data Pending    | Data for the current period is being collected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| No Data         | No data was collected for this period. This can be due to: <ul style="list-style-type: none"> <li>• Report is disabled.</li> <li>• NAM is not running.</li> <li>• Report Data Collection task is not running.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Blank data      | No traffic to display during selected period.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| No Activity     | <p>The NAM does not detect any traffic activity for this target. This can be caused by an inactive target or a data source configuration problem. The NAM does not detect any traffic activity for this target. This might be caused by an inactive target or a data source configuration problem.</p> <p>However for certain monitoring metrics when the system is missing data on errors, special conditions, and similar measurements, the status <i>No Activity</i> is substituted by a more appropriate term such as <i>No Drops Stats</i> or <i>No Concealment Stats</i>.</p> <p>This means there was no information on drops or concealment, but does not imply there was no normal activity during the reported period.</p> |
| Not Monitored   | The monitoring function for this type of traffic statistic is not enabled or is not available for the NAM and/or switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Data Expired    | Indicates that the data is more than 100 days old and no longer be available; NAM stores historical data for up to 100 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Viewing the System Event Log

System events that affect report data collection and are displayed as red triangles in the Reports Window. Events that are logged include system restarts, SPAN changes and the enabling, disabling, creating, editing, and deleting of reports.

To view the System Events Log, click **system events**. The System Config Log is displayed with the system configuration event, the time of the event and the user. The events that are displayed correspond to the report period. For example, if you are viewing a weekly report, the System Config Log will display events that occurred during the week.



### Tip

- Move the mouse cursor over the report name in the report selector to see more information about the report.
- Use the tabular report style to view numeric data and information about the errors or exception conditions related to the report data collection.

## Enabling Reports

Enable a report to activate the background process that polls the data for the report. You can enable reports directly from the Basic Reports window. To enable a report, choose a report from those listed, then click **Enable**. When a report is enabled, it continues to run until it is disabled.


**Note**

Reports in the Basic Reports table are enabled by default. In other words.

After you enable a report, you can check the status of the report in the right-most column on the **Reports > Basic Reports** window. [Table 5-16](#) provides status definitions of the conditions you might see under the Last Status column.

**Table 5-16**      **Last Status Conditions**

| Condition            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK                   | Report is enabled and collecting data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Disabled             | Report is not enabled and no data is being collected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Pending              | Data for the current period is being collected but is not yet displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Inactive Data Source | Report is enabled, but the data source for which this report is configured is in either the inactive or disabled state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| No Data              | No data was collected for this period. This can be due to: <ul style="list-style-type: none"> <li>• Report is disabled</li> <li>• NAM is not running</li> <li>• Report Data Collection task is not running</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Not Monitored        | The monitoring function for this type of traffic statistic is not enabled or is not available for the NAM and/or switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Data Expired         | Indicates that the data is more than 100 days old and no longer be available; NAM stores historical data for up to 100 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Counter Reset        | Indicates that the data collection was reset by the monitoring daemon.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Data Error           | Indicates an internal error with NAM reporting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| No Activity          | <p>No Activity—The NAM does not detect any traffic activity for this target. This might be caused by an inactive target or a data source configuration problem.</p> <p>However for certain monitoring metrics when the system is missing data on errors, special conditions, and similar measurements, the status <i>No Activity</i> is substituted by a more appropriate term such as <i>No Drops Stats</i> or <i>No Concealment Stats</i>.</p> <p>This means there was no information on drops or concealment, but does not imply there was no normal activity during the reported period.</p> <p><b>Note</b> If no data was collected, a time stamp displays the last collection.</p> |
| No Retries Stats     | Indicates that traffic is normal and there are no <i>retry</i> statistics to be reported for <i>ART retries</i> and <i>retries bytes</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| No Timeouts          | Indicates that traffic is normal and there are no <i>ART timeout</i> statistics to be reported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 5-16** Last Status Conditions (continued)

| Condition            | Description                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Outage Stats      | Indicates that traffic is normal and there are no <i>outage</i> statistics to be reported ART refused sessions, unresponsive connections, and VOIP MOS-based and jitter-based metrics reports. |
| No Utilization Stats | Indicates that traffic is normal and there are no <i>retry</i> statistics to be reported for ART retries.                                                                                      |
| No Drops Stats       | Indicates that traffic is normal and there are no <i>drop</i> statistics to be reported. No packets were dropped for any of the chassis ports.                                                 |
| No Packet Loss Stats | Indicates that traffic is normal and there are no actual packet loss or adjusted packet loss statistics to be reported for VOIP.                                                               |
| No Concealment Stats | Indicates that traffic is normal and there are no <i>concealment</i> statistics to be reported for VOIP seconds of concealment (SOC) and severe seconds of concealment (SSC).                  |

## Disabling Reports

Disable a report to suspend the background process that polls the data for the report. You can still view the data collected previously, but no new data are added to the database. You can disable reports directly from the Basic Reports window. To disable a report, select the report from those listed, then click **Disable**.

## Renaming a Report

- 
- Step 1** Choose a report from the Basic Reports window and click **Rename**.  
A text window appears.
- Step 2** Enter the new name of the report and do one of the following:
- To accept the changes, click **OK**.
  - To delete the changes and return to the Basic Reports table, click **Cancel**.
- 

## Deleting a Report

To delete a report, select the report from the Basic Reports window and click **Delete**.

## Custom Reports

After you create reports in the Basic Reports table, you can combine and customize them. The following sections describe how to manage your custom reports:

- [Creating a Custom Report, page 5-26](#).
- [Editing a Custom Report, page 5-27](#).

- [Deleting a Custom Report, page 5-27.](#)
- [Viewing a Custom Report, page 5-27.](#)

## Creating a Custom Report

To create a custom report:

**Step 1** Choose **Reports > Custom Reports**.

The Custom Reports table displays.

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

The Create Custom Report Dialog Box ([Table 5-17](#)) displays.

**Table 5-17** Create Custom Report Dialog Box

| Field       | Usage Note                                                                                                                                                                                                                                          |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Name | Enter the name of the custom report                                                                                                                                                                                                                 |
| Folder      | Choose the folder you want the report to be in.                                                                                                                                                                                                     |
| Period      | Choose the length of the report time period.                                                                                                                                                                                                        |
| Granularity | Choose the date granularity of the report.                                                                                                                                                                                                          |
| Style       | Choose the style of the graph.                                                                                                                                                                                                                      |
| Report Data | Choose the basic reports to include in the custom report. You can select multiple target data report types, but you can only include one TopN report type in a custom report.<br><br>To view all of your selected reports, click the Selection tab. |

**Step 3** Do one of the following:

- To accept the changes, click **Submit**.
- To clear the changes, click **Reset**.

## Creating a New Folder

You can create a new folder directly from the Custom Reports table to store additional custom reports.

**Step 1** Click **New Folder**.

A text box appears.

**Step 2** Enter the name of the folder, then click **OK**.

The new folder appears in the Custom Reports table.

## Editing a Custom Report

To edit a custom report:

- 
- Step 1** Choose **Reports > Custom Reports**.  
The Custom Reports table displays.
- Step 2** Choose the custom report to edit, then click **Edit**.  
The Edit Custom Reports dialog box displays.
- Step 3** Make the necessary changes, then do one of the following:
- To accept the changes, click **Submit**.
  - To leave the configuration unchanged, click **Reset**.
- 

## Deleting a Custom Report

To delete a custom report, select it in the Custom Report window, then click **Delete**.

## Viewing a Custom Report

To view a custom report:

- 
- Step 1** Choose **Reports > Custom Reports**.  
The Custom Reports window displays.
- Step 2** Choose the custom report to view, then click **View**.  
The [Viewing Report Details](#) (Figure 5-9) displays.
- 

## Moving a Custom Report to a Different Folder

To move a custom report to a different folder:

- 
- Step 1** Click **Reports > Custom Reports**.  
The Custom Reports window displays.
- Step 2** Choose the custom report to edit, then click **Edit**.  
The Edit Custom Reports dialog box displays.
- Step 3** Choose a new folder from the Folder drop-down list and click **Submit**.
-

# Scheduled Exports

The Scheduled Exports option enables you to schedule a report to be generated automatically and to be exported at a specific time. The format of the report can be PDF, HTML, CSV, or XML. The NAM transmits the HTML reports by Email. The other formats can be transmitted by EMail or FTP.

## Scheduling a Report Export

To schedule a report export:

- Step 1

To schedule a report export, you must first create a basic or customized report.  
See either section [Basic Reports, page 5-2](#), or section [Custom Reports, page 5-25](#) for information about creating a report.
- Step 2

Click **Reports > Scheduled Exports**.  
The Scheduled Exports window displays. [Figure 5-11](#) shows an example of the Scheduled Export window.

Figure 5-11 Create Scheduled Exports

Schedule Report - create

Report Type:

Daily Report

Schedule Report On:

Day

Everyday

Hour

0

Minute

0

Report File Type:

☒ PDF

☐ HTML

☐ CSV

☐ XML

Delivery Option:

☒ Email

☐ FTP Location

Report:

Granularity:

15 mins

Style:

Bar Chart

Application

Conversation

Custom Reports

Host

Switch Port

Apply

Reset

Table 5-18, [Scheduled Exports Window Options](#), describes the Scheduled Exports options available.



**Table 5-18**      **Scheduled Exports Window Options**

| Field              | Description                     | Usage Notes                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Type        | Type of report                  | Choose an option from among Daily, Weekly, or Monthly                                                                                                                                                                                                                                                                                                                              |
| Schedule Report On | Day and time to export report   | Choose an option from the list and enter the time (hour and minute) to export the report: <ul style="list-style-type: none"> <li>Daily—Report is exported every day</li> <li>Weekly—Choose a day of the week to export the report</li> <li>Monthly—Choose a day of the month to export the report; choose a specific date or choose the first or last day of the month.</li> </ul> |
| Report File Type   | File format of exported report  | You can export report in one of four formats: PDF, HTML, CSV, or XML.                                                                                                                                                                                                                                                                                                              |
| Delivery Option    | Method of report delivery       | Choose EMail and provide one or more valid EMail addresses separated by a space.<br><br><b>Note</b> You might schedule different reports to go to different individuals.<br><br>Choose FTP Location and choose a location from those in the drop-down list. See section <a href="#">FTP Configuration, page 2-19</a> , for information about configuring the FTP delivery option.  |
| Granularity        | Frequency of report             | Choose an option from among 15 minutes, 30 minutes, 1 hour, 4 hours, 8 hours, 12 hours, or 1 day.<br><br>Granularity specifies the frequency of the data points to be showed in the report. For example a daily report can have 24 hourly data points or 96 15-minute data points. The later will have more granularity.                                                           |
| Style              | Output style of report          | Choose from among Bar Chart, Stack Bar, Line Chart, Area Chart, or Tabular.                                                                                                                                                                                                                                                                                                        |
| Report             | Folders with configured reports | Each folder contains reports that have been configured and can be exported.                                                                                                                                                                                                                                                                                                        |

**Step 3** Choose the Report Type from the options in the list.

**Step 4** Choose the day on which to export the report.

This option depends on the Report Type you select. If you select Daily Report, the default (and only option) is Every Day. For a Weekly Report, select the day of the week on which to run the report. For a Monthly Report, select the date on which to run the report.

**Step 5** Enter the hour and minute for the time you want to export the report.

**Step 6** Choose the Report File Type.

**Step 7** Click to choose a Delivery Option for the report export, then enter the Email address or choose the FTP Location.

**Step 8** Choose the Granularity and Report style.

- Step 9** After specifying Scheduled Export parameters, click **Apply** to commit the scheduled export, or click **Reset** to abandon the scheduled export.
- 

## Editing a Report Export

After you schedule a report to be exported, you can modify its configuration. To edit a report export:

- 
- Step 1** Choose **Reports > Scheduled Exports**.  
The Schedule Export window displays.
- Step 2** Choose a report from those listed by clicking its check box, then click **Edit**.  
The selected Scheduled Export - edit window displays and lists the current configuration for that report.
- Step 3** Make any changes to the report export and click **Apply**, or click **Reset** to cancel your changes.  
See [Table 5-18, Scheduled Exports Window Options](#), for information about the configuration options.
-



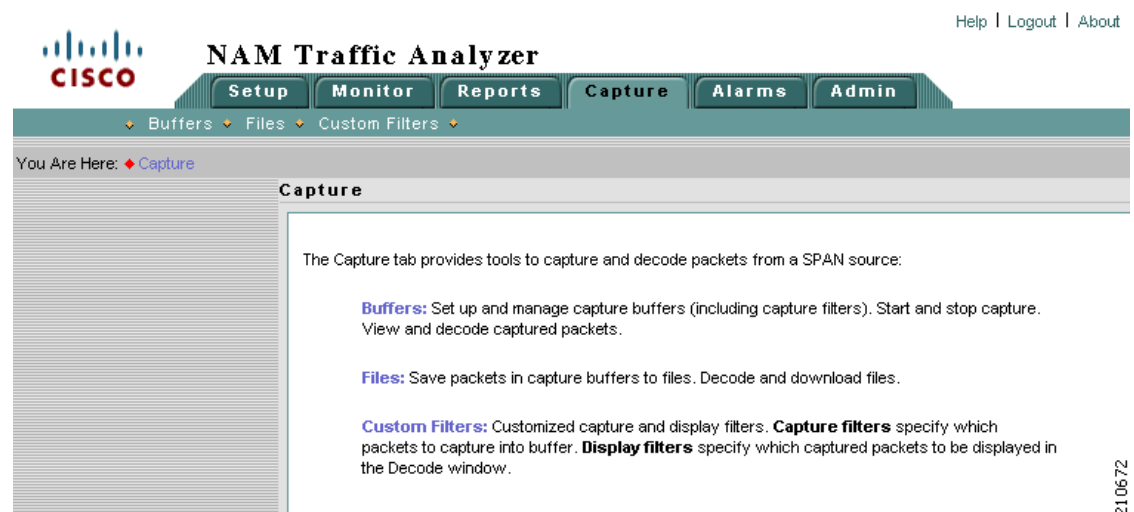
# CHAPTER 6

## Capturing and Decoding Packet Data

The Capture tab allows you to set up multiple buffers for capturing, filtering, and decoding packet data, manage the data in a file control system, and display the contents of the packets.

The Capture Tab (Figure 6-1) shows the options available for capturing and decoding packet data.

**Figure 6-1** Capture Tab



From the Capture tab, you can select three options:

- [Buffers, page 6-2](#)

Use the Buffers option to access the basic operations for capturing, viewing and decoding packet data on the NAM.

The Cisco NAM 2200 Series appliances can also configure Hardware Assisted Capture.

- [Files, page 6-22](#)

Use the Files option to save, decode, or download files.

- [Custom Capture Filters, page 6-27](#)

Use the Custom Filters option to create customized capture and display filters.



**Note**

NAM 4.1 supports IPv6 for all capture functionality.

# Buffers



Note

Cisco NAM 2200 Series appliances also provide Hardware Assisted Capture. See [Hardware Assisted Capture Sessions](#), page 6-15 for more information.

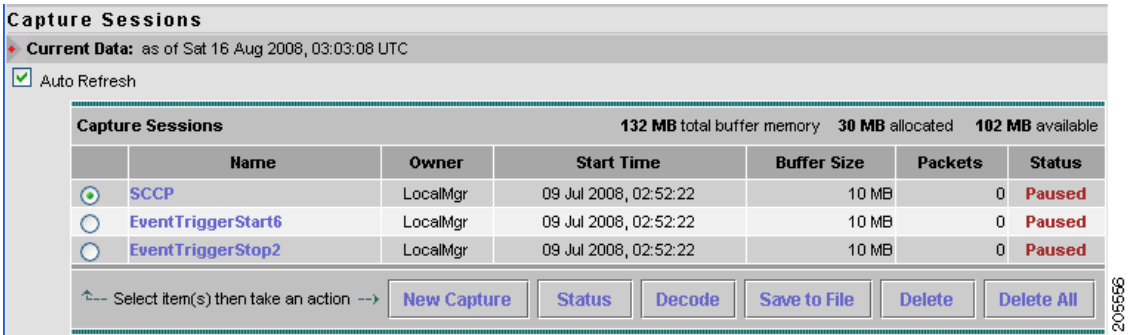
The Capture Buffers ([Figure 6-2](#)) window shows the list of capture buffers. You can configure multiple capture buffers and multiple automatic capture buffers.



Note

If you check the Auto Refresh check box, the Capture Buffers window refreshes automatically every 60 seconds.

**Figure 6-2** Capture Buffers



[Capture Buffer Fields](#), [Table 6-1](#), describes the Capture Buffers fields.

**Table 6-1** Capture Buffer Fields

| Operation   | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Name of the capture buffer                                                                                                                                                                                                                                                                                                                                                                        |
| Owner       | Owner of the buffer                                                                                                                                                                                                                                                                                                                                                                               |
| Start Time  | Time capture starts                                                                                                                                                                                                                                                                                                                                                                               |
| Buffer Size | Size of the buffer                                                                                                                                                                                                                                                                                                                                                                                |
| Packets     | Number of packets                                                                                                                                                                                                                                                                                                                                                                                 |
| Status      | <p>The current status of the capture:</p> <ul style="list-style-type: none"> <li>Running—Packet capture is in progress</li> <li>Paused—Packet capture is paused. Captured packets remain in buffer, but no new packets are captured</li> <li>Cleared—Capture is stopped (by user) and capture buffer is cleared</li> <li>Locked—Capture is locked (stopped) because the buffer is full</li> </ul> |

[Capture Buffer Operations](#) (Table 6-2) describes the operations that you can perform from the Capture Buffers window.

**Table 6-2** *Capture Buffer Operations*

| Operation    | Description                                                                              |
|--------------|------------------------------------------------------------------------------------------|
| New Capture  | Click to create a new capture buffer. See <a href="#">Configuring Capture Settings</a> . |
| Status       | Click to display status and settings of selected capture.                                |
| Decode       | Click to view decoded packets. See <a href="#">Viewing Packet Decode Information</a> .   |
| Save to File | Click to save a buffer to a file on the NAM hard disk. See <a href="#">Files</a> .       |
| Delete       | Click to delete a buffer.                                                                |
| Delete All   | Click to delete all buffers.                                                             |

## Configuring Capture Settings

The Capture Settings window enables you to configure the settings for a new capture and control the capture process. You can also configure capture filters to narrow down the packets to be captured.

To configure a new capture buffer:

- 
- Step 1** Go to the **Capture > Buffers** window.
- Step 2** Choose **New Capture** to set up a new capture, or choose an existing buffer and click **Status** to modify, pause, clear, or restart capture settings.

The NAM Traffic Analyzer displays the Capture Settings ([Figure 6-3](#)) window. The Capture Settings window provides a field for you to enter a name for the capture and four status indicators described in [Table 6-3](#).

**Table 6-3** *Capture Settings Status Indicators*

| Status Indicator | Description                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capture Status   | <p>The current status of the capture:</p> <ul style="list-style-type: none"> <li>Running—Packet capture is in progress.</li> <li>Paused—Packet capture is paused. Captured packets remain in buffer, but no new packets are captured.</li> <li>Cleared—Capture is stopped (by user) and capture buffer is cleared.</li> <li>Locked—Capture is locked because the buffer is full.</li> </ul> |
| Packets Captured | <p>The number of packets captured and stored in the capture buffer.</p> <p><b>Note</b> When the capture buffer is full and capture is in wrap-when-full mode, the number of packets captured may fluctuate as new packets arrive and old packets are discarded from the buffer.</p>                                                                                                         |
| First Started    | Shows when the current capture started. You can pause and restart the capture as many times as necessary. If you stop the capture and start a new capture, this field shows the start time of the <i>new</i> capture.                                                                                                                                                                       |
| Buffer           | Current buffer or file state—Empty, Space Available, Full (Wrap), or Full (Locked).                                                                                                                                                                                                                                                                                                         |

**Figure 6-3** Capture Settings

**Step 3** Enter information in the Capture Settings Fields (Table 6-4) as appropriate.

**Table 6-4** Capture Settings Fields

| Field             | Description                                                              | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capture Name      | Name of the capture                                                      | Enter a capture name.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Capture from      | Data source from which to capture packets                                | Choose an entry from the list.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Start Event       | Alarm event that starts the capture                                      | <p>You can configure Alarm Events from the <b>Setup &gt; Alarms &gt; Alarm Event</b> window. When an alarm event threshold is crossed, the alarm event starts or stops the capture session.</p> <p><b>Note</b> When a capture is configured to start with a Start Event, the capture session waits in the <i>Paused</i> state until the Start Event occurs.</p>                                                                                                                |
| Stop Event        | Alarm event that stops the capture                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Packet Slice Size | The slice size in bytes; used to limit the size of the captured packets. | <p>Enter a value of 64 or higher. Enter zero (0) to not perform slicing.</p> <p>If you have a small buffer but want to capture as many packets as possible, use a small slice size.</p> <p>If the packet size is larger than the specified slice size, the packet is <i>sliced</i> before it is saved in the capture buffer. 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 buffer.</p> |

**Table 6-4** Capture Settings Fields (continued)

| Field                          | Description                                              | Usage Notes                                                                                                                                                                                                                                                                                         |
|--------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capture to Buffer              | Check to store captures in buffers                       | Enter values for <b>Buffer Size</b> and <b>Wrap when Full</b> .                                                                                                                                                                                                                                     |
| Buffer Size                    | Size of the capture buffer in MB.                        | Use this field to define the buffer size for this capture. Enter a number from 1 up to your platform maximum. If system memory is low, the actual buffer size allocated might be less than the number specified here. See <a href="#">Table 6-5</a> for maximum buffer sizes for each NAM platform. |
| Wrap when Full                 | Check to wrap data in buffer when it exceeds buffer size | Check <b>Wrap when Full</b> to enable continuous capture.<br><b>Note</b> When the buffer is full, older packet data is removed to make room for new incoming packets.                                                                                                                               |
| Capture to Disk                | Check to store captures in files                         | Enter values for <b>File Size</b> and <b>No. Files</b> .<br><b>Note</b> About 400MB 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.                                                          |
| File Size (MB)                 | Maximum size of each capture file                        | File size can be from 1 to 2 GB or up to 10 GB for the NAM appliances.                                                                                                                                                                                                                              |
| File Location                  | Choose an option from the pull-down menu.                | Local disk is the default, or choose a previously configured remote storage location. You can add (NFS and iSCSI) remote storage locations by clicking <b>Admin &gt; System</b> and choosing Capture Data Storage from the Content menu.                                                            |
| No. Files                      | Number of files to use for continuous capture            | Number of files can be from 1 to 200.                                                                                                                                                                                                                                                               |
| Rotate Files                   | Check to rotate files in continuous capture              | Available only for remote storage or NAM 2200 Series appliances<br>See section <a href="#">Capture Data Storage, page 2-19</a> , for information about configuring remote storage.                                                                                                                  |
| <b>Capture Filter:</b> Include |                                                          | Include filters capture only packets that match the filter conditions (recommended)                                                                                                                                                                                                                 |
| <b>Capture Filter:</b> Exclude |                                                          | Exclude filters capture packets that <i>exclude</i> the filter conditions (recommended)                                                                                                                                                                                                             |

[Table 6-5](#) lists the hardware platforms NAM 4.1 supports and their maximum buffer size.

**Table 6-5** Maximum Capture Buffer Sizes for NAM Platforms

| NAM Platform                                      | Maximum Buffer Size |
|---------------------------------------------------|---------------------|
| WS-SVC-NAM-1                                      | 125 MB              |
| WS-SVC-NAM-1 with memory upgrade (MEM-C6KNAM-2GB) | 200 MB              |
| WS-SVC-NAM-1-250S                                 | 200 MB              |
| WS-SVC-NAM-2                                      | 300 MB              |
| WS-SVC-NAM-2 with memory upgrade (MEM-C6KNAM-2GB) | 500 MB              |
| WS-SVC-NAM-2-250S                                 | 500 MB              |
| NAM2204-RJ45                                      | 2 GB                |

**Table 6-5** Maximum Capture Buffer Sizes for NAM Platforms

| NAM Platform | Maximum Buffer Size |
|--------------|---------------------|
| NAM2204-SFP  | 2 GB                |
| NAM2220      | 10 GB               |
| NME-NAM-80S  | 132 MB              |
| NME-NAM-120S | 300 MB              |

- Step 4** If capturing to buffers, check **Capture to Buffer**, enter MB size in **Buffer Size**, and check **Wrap when Full** if you want to continuously capture most recent data.

This type of capture stores packet data up to the size you set in Buffer Size. If you do not check **Wrap when Full**, capture will end when amount of data reaches size of buffer.

- Step 5** If capturing to files, check **Capture to File(s)**, and enter values in **File Size** and **No. Files**.

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.

**Note**

When configuring capture to disk sessions, it's important to keep track of your free disk space and manage your capture files. An anomaly in NAM software allows you to create more capture files than you have the free disk space to store. For example, you might have 400 MB of free disk space when you set up two capture sessions that each store 160 MB of capture files. A little later, before the previous capture sessions have each written 160 MB of data, you might notice you still have 160 MB of free disk space and set up another capture session to store an addition 120 MB of capture files. The anomaly allows you to configure the capture session, even though you will eventually run out of disk space causing all active capture sessions to end with errors.

- Step 6** If capturing to files, check **Rotate Files** to continuously capture the most recent packet data.

The Rotate Files option can only be used with remote storage or the NAM 2200 Series appliance's local disk. See the section [Capture Data Storage, page 2-19](#), for information about configuring remote storage.

**Note**

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 timestamp.

- Step 7** In the Capture Filter pane, check Include or Exclude.

Include filters capture only packets that match the filter conditions. Exclude captures packets that *exclude* the filter conditions.

- Step 8** Choose one of the following check boxes to enable the applicable filter types:

- **Address** to filter traffic based on a type of IP, IPIP4, IPv6, GRE.IP, or MAC address. (See the [“Capturing Using an Address Filter”](#) section on page 6-8.)
- **Protocols** to filter traffic based on specific protocols. (See the [“Capturing Using a Protocol Filter”](#) section on page 6-9.)
- **Ports** to use a port filter. (see the [“Capturing Using a Port Filter”](#) section on page 6-10.)
- **Custom Filter** to use a customized filter. (See the [“Capturing Using a Custom Filter”](#) section on page 6-10.)



For more information on creating and editing a custom capture filter, see the [“Custom Capture Filters” section on page 6-27](#).

- Step 9** Choose one of the operations listed in [Table 6-6, Capture Settings Operations](#).

**Table 6-6** Capture Settings Operations

| Operation     | Description                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Start</b>  | Click to start a capture operation.                                                                                                                             |
| <b>Pause</b>  | Click to pause a capture operation. Capture data remains in the capture buffer, but no new data is stored. Click Start to resume the capture.                   |
| <b>Clear</b>  | Click to stop a capture and clear the capture buffer. You must clear the capture buffer before you change capture settings.                                     |
| <b>Decode</b> | Click to display the capture buffer. (This could take a few minutes.)<br><b>Note</b> Capture sessions appear in the <i>Paused</i> state when decoding a buffer. |
| <b>Close</b>  | Click to close the capture window.                                                                                                                              |

For example, to capture only HTTP and HTTPS packets in the 111.122 Class B network, do the following:

- Step 1** Click the **Inclusive** check box.
- Step 2** Click the **Address** check box.
- Step 3** Click the IP button.
- Step 4** Choose the **Both Directions** check box.
- Step 5** In the Source, enter **111.122.0.0**.
- Step 6** In the Source Mask, enter **255.255.0.0**.
- Step 7** Click the **Protocol** check box.
- Step 8** Press **Shift-Click** to select HTTP and HTTPS from the list.

# Capturing Using an Address Filter

If you selected the **Address** check box, enter information in the [Capture Settings Address Filter Dialog Box](#), [Table 6-7](#), as appropriate.



**Note**

When filtering on tunnel addresses such as IPIP4 or GRE.IP, the filters will match the addresses on the inner and outer IP header.

**Table 6-7** Capture Settings Address Filter Dialog Box

| Field            | Description                                                            | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address          | Indicates by which address to filter.                                  | <ul style="list-style-type: none"> <li>Choose MAC to use the source/ destination MAC address of the packets.</li> <li>Choose IP to use the source/destination IP addresses of the packets.</li> <li>Choose IPIP4 for IP addresses including those tunneled over IP protocol 4.</li> <li>Choose GRE.IP for IP addresses including those tunneled over GRE.</li> <li>Choose IPv6 for addresses using IP version 6.</li> <li>Choose GTP.IPv4 for IPv4 address for tunneled packet over GTP.</li> <li>Choose GTP.IPv6 for IPV6 address for tunneled packet over GTP.</li> </ul>                                                                              |
| Both directions. | Indicates whether the filter is applied to traffic in both directions. | <p>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.</p> <p>If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| Source           | Source address of the packets.                                         | <ul style="list-style-type: none"> <li>For IP, IPIP4, GRE.IP or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format <i>n.n.n.n</i>, where <i>n</i> is 0 to 255.</li> <li>For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: <ul style="list-style-type: none"> <li>1080::8:800:200C:417A</li> <li>::FFF:129.144.52.38</li> </ul> </li> </ul> <p><b>Note</b> See RFC 2373 for valid text representations.</p> <ul style="list-style-type: none"> <li>For MAC address, enter <i>hh hh hh hh hh hh</i>, where <i>hh</i> is a hexadecimal number from 0 to 9 or a to f.</li> </ul> |

**Table 6-7** Capture Settings Address Filter Dialog Box (continued)

| Field       | Description                                                                                                                                                                                                                                                                                       | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Mask | <p>The mask applied to the source address.</p> <ul style="list-style-type: none"> <li>If a bit in the Source Mask is set to 1, the corresponding bit in the address is relevant.</li> <li>If a bit in the Source Mask is set to 0, the corresponding bit in the address is ignored.</li> </ul>    | <ul style="list-style-type: none"> <li>For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format <i>n.n.n.n</i>, where <i>n</i> is 0 to 255. The default (if blank) is 255.255.255.255.</li> <li>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</li> </ul> <p><b>Note</b> See RFC 2373 for valid text representations.</p> <p>For MAC address, enter <i>hh hh hh hh hh hh</i>, where <i>hh</i> is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.</p>                          |
| Destination | Destination address of the packets.                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format <i>n.n.n.n</i>, where <i>n</i> is 0 to 255. The default (if blank) is 255.255.255.255.</li> <li>For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: <ul style="list-style-type: none"> <li>1080::8:800:200C:417A</li> <li>::FFF:129.144.52.38</li> </ul> </li> </ul> <p><b>Note</b> See RFC 2373 for valid text representations.</p> <p>For MAC address, enter <i>hh hh hh hh hh hh</i>, where <i>hh</i> is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.</p> |
| Dest. Mask  | <p>The mask applied to the destination address.</p> <ul style="list-style-type: none"> <li>If a bit in the Dest. Mask is set to 1, the corresponding bit in the address is relevant.</li> <li>If a bit in the Dest. Mask is set to 0, the corresponding bit in the address is ignored.</li> </ul> | <ul style="list-style-type: none"> <li>For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format <i>n.n.n.n</i>, where <i>n</i> is 0 to 255. The default (if blank) is 255.255.255.255.</li> <li>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</li> </ul> <p><b>Note</b> See RFC 2373 for valid text representations.</p> <p>For MAC address, enter <i>hh hh hh hh hh hh</i>, where <i>hh</i> is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.</p>                          |

## Capturing Using a Protocol Filter

If you selected the **Protocol** check box, select one or more protocols to capture from the drop-down list. Use Shift + Click to select multiple protocols.

## Capturing Using a Port Filter

From the Capture Settings window, select the Ports check box and enter one or more ports separated by commas.

## Capturing Using a Custom Filter

**Step 1** Click the **Custom** check box.



**Note** The Address Filter and Protocol Filter check boxes are disabled if you select the Custom Filter check box and vice versa.

**Step 2** Choose one or more custom capture filters from the list. Use Shift + click to select multiple filters. If you select multiple custom filters, the filters' conditions will be ORed together (match any).



**Note** If the list is empty, see the [“Creating Custom Capture Filters”](#) section on page 6-27 for instructions on creating custom capture filters.

To view or edit the selected custom capture filter, choose **Custom Filters > Capture Filters**.

## 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 [Setting Up Alarm Events, page 3-82](#), 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 [Setting Alarm Thresholds, page 3-84](#), for more information.

**Step 3** Set up a capture buffer from the **Capture > Buffers** window. Click **New Capture**.

Choose the Start Event and/or the Stop Event for the associated Alarm Event. See [Configuring Capture Settings, page 6-3](#), for more information.

## Viewing Packet Decode Information

After some packets have been captured in the buffer, 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 the “[Viewing Detailed Protocol Decode Information](#)” section on page 6-14).
- Packet hexadecimal dump.

To view packet decode information:

**Step 1** Choose **Capture > Buffers** or **Capture > Files**.

**Step 2** Choose a capture buffer or file then click **Decode**.

The Packet Decoder window displays as shown in [Figure 6-4](#).

**Figure 6-4** Packet Decoder Window

The screenshot shows the NAM Traffic Analyzer interface. The title bar reads "NAM Traffic Analyzer" and "Packet Decoder - Capture2\_1.pcap file". Below the title bar, there are controls for "Packets: 1-202 of 202", "Stop", "Prev", "Next", "1000", "Go to 1", "Display Filter", and "TCP Stream".

| Pkt | Time(s) | Size | Source                   | Destination           | Protocol | Info                                 |
|-----|---------|------|--------------------------|-----------------------|----------|--------------------------------------|
| 1   | 0.000   | 827  | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | HTTP     | GET /capture/settings.php?capname=Ca |
| 2   | 0.000   | 827  | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | HTTP     | GET /capture/settings.php?capname=Ca |
| 3   | 0.117   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 4   | 0.116   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 5   | 0.120   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 6   | 0.120   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 7   | 0.119   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 8   | 0.119   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4568 > 80 [ACK] Seq=511117448 Ack=16 |
| 9   | 0.135   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4569 > 80 [ACK] Seq=283785185 Ack=16 |
| 10  | 0.134   | 64   | dhcp-171-69-65-1.cisc... | namlab-kom7.cisco.com | TCP      | 4569 > 80 [ACK] Seq=283785185 Ack=16 |

Below the packet list, the details for Packet 1 are shown:

**Packet** Number: 1 - Time: Dec 13, 2005 19:07:47.329 - Packet Length: 827 bytes - Capture Length: 500 bytes

- + **ETH** Ethernet II, Src: Cisco\_db:08:0a (00:06:2a:db:08:0a), Dst: Cisco\_e4:cb:b8 (00:02:7e:e4:cb:b8)
- + **VLAN** 802.1Q Virtual LAN
- + **IP** Internet Protocol, Src: dhcp-171-69-65-1.cisco.com (171.69.65.1), Dst: namlab-kom7.cisco.com (172.20.104.72)
- + **TCP** Transmission Control Protocol, Src Port: 4568 (4568), Dst Port: 80 (80), Seq: 511116679, Ack: 1688814722, Len: 769
- + **HTTP** Hypertext Transfer Protocol
- + **SHORT** [Packet size limited during capture: HTTP truncated]

At the bottom, a hexadecimal dump is shown:

```

0000 00 02 7e e4 cb b8 00 06 2a db 08 0a 81 00 00 02 ..~.....*.....
0010 08 00 45 00 03 29 7e fe 40 00 77 06 81 2d ab 45 ..E...)~.@.w...-E
0020 41 01 ac 14 68 48 11 d8 00 50 1e 77 05 87 64 a9 A...hH...P.w...d.
0030 44 82 50 18 fe 9e 7d da 00 00 47 45 54 20 2f 63 D.P...}...GET /c

```

Table 6-8 describes the packet decoder operations.



**Note**

If you enable DNS on the **Admin > System > Preferences** window, packet decoding can take a very long time due to DNS name resolution.

**Table 6-8** *Packet Decoder Operations*

| Button         | Description                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| Stop           | Stop packet loading                                                                                                            |
| Prev           | Load and decode the previous block of packets from the NAM                                                                     |
| Next           | Load and decode the next block of packets from the NAM                                                                         |
| Go To          | Load and decode a block of packets starting from the specified packet number.                                                  |
| Display Filter | Launch the Display Filter dialog. See <a href="#">Filtering Packets Displayed in the Packet Decoder, page 6-13</a> .           |
| TCP Stream     | Follow the TCP stream of the selected TCP packet.<br><b>Note</b> This might take a long time depending on the traffic pattern. |

[Table 6-9](#) describes the information displayed in the packet browser pane.

**Table 6-9** *Packet Browser*

| Field       | Description                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pkt         | Packet numbers, listed numerically in capture sequence. If the decode (display) filter is active, the packet numbers might not be consecutive.                                                                       |
| Time        | Time the packet was captured relative to the first packet displayed (not the first packet in the buffer).<br><b>Note</b> To see the absolute time, see the Detail window.                                            |
| Size        | Size of the packet, in bytes.                                                                                                                                                                                        |
| Source      | Packet source, which might be displayed as hostname, IP, IPX, or MAC address.<br><b>Note</b> To turn hostname resolution on and off for IP addresses, click the Setup tab and change this setting under Preferences. |
| Destination | Packet destination, which might be displayed as hostname, IP, IPX, or MAC address.                                                                                                                                   |
| Protocol    | Top-level protocol of the packet.                                                                                                                                                                                    |
| Info        | Brief text information about the packet contents.                                                                                                                                                                    |

## 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 buffer.



**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 (Figure 6-5) displays.

**Figure 6-5** Packet Decoder - Display Filter Window

The screenshot shows the 'Packet Decoder - Display Filter' window. It has a title bar with a close button. The window is divided into several sections. The 'Filter Mode' section has two radio buttons: 'Inclusive' (selected) and 'Exclusive'. The 'Address Filter' section has two radio buttons: 'IP addr / host' (selected) and 'MAC addr'. Below these are two text input fields for 'Source' and 'Destination', and a checkbox for 'Both Directions'. The 'Protocol Filter' section has two radio buttons: 'Match any (or)' (selected) and 'Match all (and)'. Below these are two columns of dropdown menus: 'Protocols' and 'Fields (optional)'. The 'Custom Filter' section has a single dropdown menu. At the bottom of the window are four buttons: 'Clear Filter', 'OK', 'Cancel', and 'Apply'. The status bar at the bottom of the window says 'Java Applet Window'.

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



**Note**

You can type the first few letters of the protocol name to go directly to the protocol. If you make a typo, type **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](#) for how to set up a custom display filter.
- Step 3** Specify the protocol name, IP address, MAC address, matching text, or custom decode filter.
- Step 4** Click **Filter**.
- Step 5** To display packets that *exclude* the filter conditions, select the **exclusive** check box next to the Filter button.
- 

## 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.
- Click 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.



## Hardware Assisted Capture Sessions



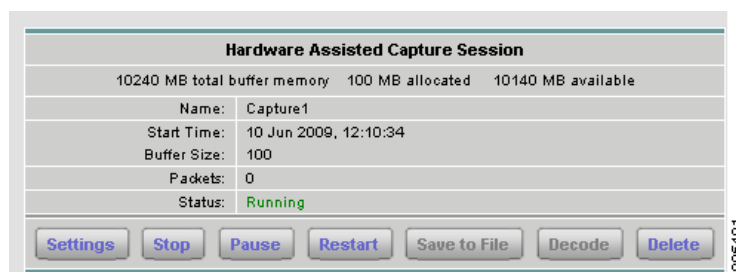
### Note

This section is valid only for the Cisco NAM 2200 Series Appliances.

Hardware Assisted Capture enables you to improve capture performance by providing hardware-specific filters to help you eliminate as much extraneous traffic as possible. The packets filtered out by hardware filters are not processed by the NAM and capture performance improves.

Click **Capture > Buffers** to view the status and settings of the hardware assisted capture feature of the Cisco NAM appliance. [Figure 6-6](#) shows the Hardware Assisted Capture Sessions dialog box.

**Figure 6-6 Hardware Assisted Capture Session**



Click **Settings** to configure a hardware assisted capture session. The Capture Buffers window displays as shown in [Figure 6-7](#). The settings are similar to the NAM software capture, except that the Hardware-Assisted Capture Session provides additional hardware and software filters.

Hardware Assisted Capture Session uses a combination of the hardware filters and the software filters you define. For filtering to be successful, you must match one of the hardware filters (if there are any) AND one of the software filters (if there are any). You can perform filtering without using both hardware and software filters.

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

Use the other buttons on the Hardware Assisted Capture Session window for the following:

- Click **Stop** to stop a currently active capture session.
- Click **Pause** to pause a currently active capture session.
- Click **Restart** to restart a paused or stopped capture session.
- Click **Save to File** to save the capture buffer session to a file.

This option is enabled only when a capture session has been stopped or paused.



### Note

Do not add a file suffix when you provide the filename. The suffix **.pcap** is added automatically.

- Click **Decode** to display the packets in a file.

This option is enabled only when a capture session has been stopped or paused.

- Click **Delete** to delete a capture buffer session file.

## Configuring the Hardware Assisted Capture Session

The Capture Buffers window, shown in Figure 6-7, displays the status and settings of the Hardware-Assisted Capture if a capture has been defined.

**Figure 6-7** Configuring Capture Buffers

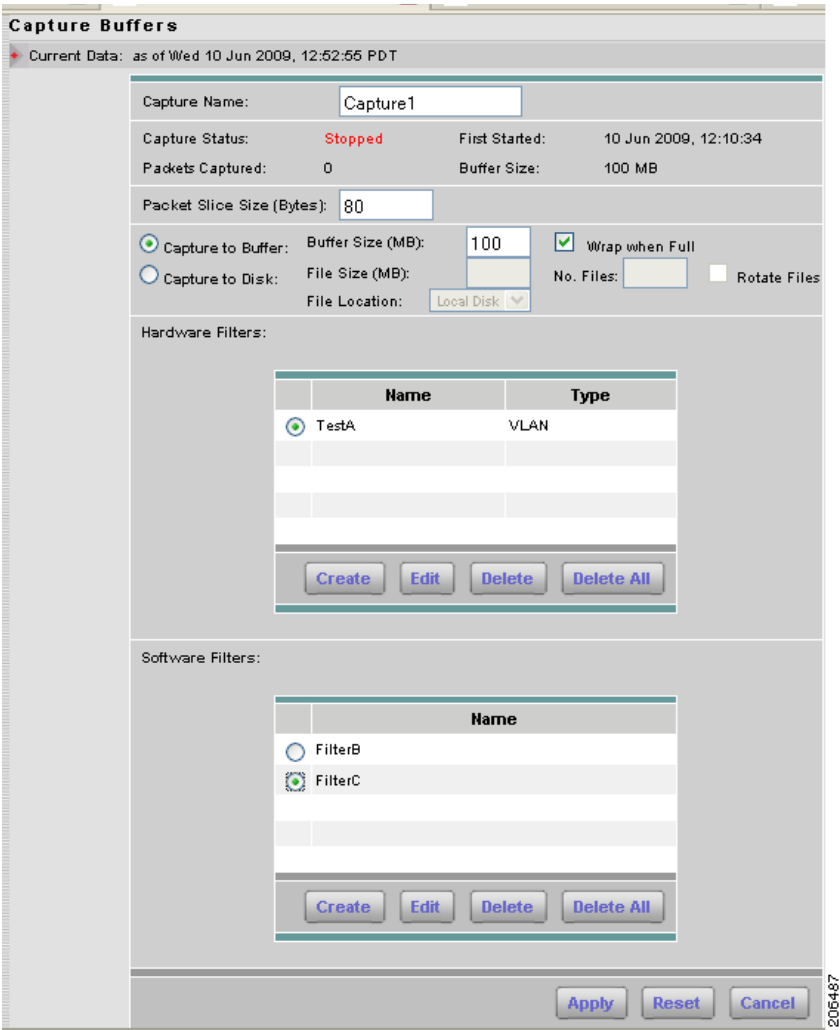


Table 6-10 describes the fields of the Capture Buffers window. To configure a capture:

- Step 1** Enter a name in the Capture Name field.
- Step 2** Enter a value for the number of bytes in a Packet Slice Size.
- Step 3** Choose either Capture to Buffer or Capture to Disk, and provide the necessary values based on your selection.
  - For Capture to Buffer, provide Buffer Size (MB) and whether to Wrap When Full.
  - For Capture to Disk, provide file size, location, number of files, and whether to rotate files.
- Step 4** To define a hardware or software filter, click **Create** in the appropriate field.

Depending on the type of filter, see one of the following:

- [Configuring Hardware Filters](#)
- [Configuring Software Filters](#)



#### Note

When configuring capture to disk sessions, it's important to keep track of your free disk space and manage your capture files. An anomaly in NAM software allows you to create more capture files than you have the free disk space to store. For example, you might have 400 MB of free disk space when you set up two capture sessions that each store 160 MB of capture files. A little later, before the previous capture sessions have each written 160 MB of data, you might notice you still have 160 MB of free disk space and set up another capture session to store an addition 120 MB of capture files. The anomaly allows you to configure the capture session, even though you will eventually run out of disk space causing all active capture sessions to end with errors.

- Step 5** Click **Apply** to complete the configuration of the capture session. Otherwise, click **Reset** to revert to the previous settings, or click **Cancel** to abort.

**Table 6-10** Capture Buffers Settings

| Field                            | Description                                                              | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Capture Name</b>              | Name of the capture                                                      | Enter a capture name.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Capture Status                   | The current status of the capture.                                       | <ul style="list-style-type: none"> <li>• Running—Packet capture is in progress.</li> <li>• Paused—Packet capture is paused. Captured packets remain in buffer, but no new packets are captured.</li> <li>• Cleared—Capture is stopped (by user) and capture buffer is cleared.</li> <li>• Locked—Capture is locked because the buffer is full.</li> </ul>                                                                                                                      |
| Packets Captured                 | The number of packets captured and stored in the capture buffer.         | When the capture buffer is full and capture is in wrap-when-full mode, the number of packets captured may fluctuate as new packets arrive and old packets are discarded from the buffer.                                                                                                                                                                                                                                                                                       |
| First Started                    | Shows when the current capture started.                                  | You can pause and restart the capture as many times as necessary. If you stop the capture and start a new capture, this field shows the start time of the <i>new</i> capture.                                                                                                                                                                                                                                                                                                  |
| Buffer Size (MB)                 | Current buffer or file state                                             | Currently allocated buffer size.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Packet Slice Size (Bytes)</b> | The slice size in bytes; used to limit the size of the captured packets. | <p>Enter a value of 64 or higher. Enter zero (0) to not perform slicing.</p> <p>If you have a small buffer but want to capture as many packets as possible, use a small slice size.</p> <p>If the packet size is larger than the specified slice size, the packet is <i>sliced</i> before it is saved in the capture buffer. 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 buffer.</p> |
| <b>Capture to Buffer</b>         | Default; captures to buffer that you define                              | Enter values for <b>Buffer Size (MB)</b> and click whether to <b>Wrap when Full</b> .                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 6-10** Capture Buffers Settings (continued)

| Field                    | Description                                                  | Usage Notes                                                                                                                                                                                                                                                                                         |
|--------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buffer Size (MB)         |                                                              | Use this field to define the buffer size for this capture. Enter a number from 1 up to your platform maximum. If system memory is low, the actual buffer size allocated might be less than the number specified here. See <a href="#">Table 6-5</a> for maximum buffer sizes for each NAM platform. |
| Wrap when Full           | Check to wrap data in buffer when it exceeds buffer size.    | Check <b>Wrap when Full</b> to enable continuous capture.<br><b>Note</b> When the buffer is full, older packet data is removed to make room for new incoming packets.                                                                                                                               |
| Capture to Disk          | Check to store captures in files                             | Enter values for <b>File Size</b> and <b>No. Files</b> .<br><b>Note</b> About 400MB of free disk space is reserved for working files. If available disk space is below 400MB, you will not be able to start new capture-to-disk sessions.                                                           |
| File Size (MB)           | Maximum size of each capture file                            | File size can be from 1 to 2 GB or up to 10 GB for the NAM appliances.                                                                                                                                                                                                                              |
| File Location            | Choose an option from the pull-down menu.                    | Local disk is the default, or choose a previously configured remote storage location. You can add (NFS and iSCSI) remote storage locations by clicking <b>Admin &gt; System</b> and choosing Capture Data Storage from the Content menu.                                                            |
| No. Files                | Number of files to use for continuous capture                | Number of files can be from 1 to 200.<br><b>Note</b> Due to an anomaly in NAM 4.1 software, when configuring the number of files for the Cisco NAM 2204 appliance capture, ensure that you do not create more files than you can store in your available disk space.                                |
| Rotate Files             | Check to rotate files in continuous capture                  | Available only for remote storage or NAM 2200 Series appliances<br>See section <a href="#">Capture Data Storage, page 2-19</a> , for information about configuring remote storage.                                                                                                                  |
| <b>Hardware Filters:</b> | Lists any hardware filters configured for a capture session. | Click a radio button to select one of the hardware filters in the list. Click <b>Create</b> to define hardware filters to use for the capture buffer session. See <a href="#">Configuring Hardware Filters</a> .                                                                                    |
| <b>Software Filters:</b> | Lists any software filters configured for a capture session. | Click a radio button to select one of the software filters in the list. Click <b>Create</b> to define software filters to use for the capture buffer session. See <a href="#">Configuring Software Filters</a> .                                                                                    |

## Configuring Hardware Filters

To configure a hardware filter:

- 
- Step 1** Enter a filter name.
- Step 2** From the pull-down menu, select a hardware filter type.
- Choose one of the following hardware filter types:
- [VLAN](#)
  - [VLAN and IP](#)

- [IP](#)
- [IP and TCP/UDP](#)
- [IP and Payload Data](#)
- [Payload Data](#)

- Step 3** Under VLAN, choose either Range or Individuals. For range, enter a range of VLANs. For Individuals, enter up to four individual VLANs.
- Step 4** Click **Apply** to complete the configuration of the hardware filter. 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** 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.
- Step 3** Click **Apply**.
- 

## VLAN and IP

To configure a VLAN and IP hardware filter:

- Step 1** Enter a Filter Name.
- Step 2** Enter the ID of the desired VLAN.  
The VLAN ID can range from 1-4095.
- Step 3** Choose an IP Version.



**Note** The following address and mask formats must match the IP version.

---

If you do not enter values for the optional fields in steps 5 through 9, the filter will match based on the VLAN ID and the IP version. A filter with settings like this might be useful when trying to filter all IPv6 traffic from a specific VLAN.

- Step 4** Optionally, enter a Source Address.
- Step 5** Optionally, enter a Source Mask.
- Step 6** Optionally, enter a Destination Address.
- Step 7** Optionally, enter a Destination Mask.
- Step 8** Optionally, choose an IP Protocol (Layer 4).
- Step 9** Click **Apply**.
-

## IP

To configure an IP hardware filter:

---

**Step 1** Enter a Filter Name.

**Step 2** Choose an IP Version.



**Note** The following address and mask formats must match the IP version.

---

If you do not enter values in the optional fields for steps 3 through 7, the filter will match based only on IP Version. A filter using only the IP Version field and none of the optional fields might be useful when trying to filter IPv6 traffic.

**Step 3** Optionally, enter a Source Address.

**Step 4** Optionally, enter a Source Mask.

**Step 5** Optionally, enter a Destination Address.

**Step 6** Optionally, enter a Destination Mask.

**Step 7** Optionally, choose an IP Protocol (Layer 4)

**Step 8** Click **Apply**.

---

## IP and TCP/UDP

To configure an IP and TCP/UDP hardware filter:

---

**Step 1** Enter a Filter Name.

**Step 2** Choose an IP Version.



**Note** The following address and mask formats must match the IP version.

---

If you do not enter values in the optional fields for steps 3 through 9, an IP and TCP/UDP filter will match based on IP Version and IP Protocol (TCP or UDP). A filter with settings like this might be useful when the desired traffic is all IPv4 TCP. By adding a port, you can make an FTP Data filter (IPv4, TCP and Source Port 20).

**Step 3** Optionally, enter a Source Address.

**Step 4** Optionally, enter a Source Mask.

**Step 5** Optionally, enter a Destination Address.

**Step 6** Optionally, enter a Destination Mask.

**Step 7** Choose an IP Protocol, either TCP or UDP.

**Step 8** Optionally, enter a TCP/UDP Source Port.

**Step 9** Optionally, enter a TCP/UDP Destination Port.

**Step 10** Click **Apply**.

---

## IP and Payload Data

To configure an IP and Payload Data hardware filter:

---

**Step 1** Enter a Filter Name.

**Step 2** Choose an IP Version.



**Note** The following address and mask formats must match the IP version.

If you do not enter values in the optional fields for steps 3 through 6, the filter will match based on IP Version, IP Protocol (TCP or UDP), and Payload. A filter with settings like this might be useful when the desired traffic is all IPv4, TCP packets beginning with a specific payload signature.

**Step 3** Optionally, enter a Source Address.

**Step 4** Optionally, enter a Source Mask.

**Step 5** Optionally, enter a Destination Address.

**Step 6** Optionally, enter a Destination Mask.

**Step 7** Choose an IP Protocol, either TCP or UDP.

**Step 8** Enter an Offset from 1-1023.

The offset is relative to the beginning of the payload (Layer 5).

**Step 9** Enter a Value of up to four bytes (eight hex characters).

**Step 10** Enter a Mask of up to four bytes (eight hex characters).

**Step 11** Repeat steps 8, 9 and 10 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 12** Click **Apply**.

---

## Payload Data

To configure a Payload Data hardware filter:

---

**Step 1** Enter a Filter Name.

**Step 2** Choose an IP Protocol, either TCP or UDP.

**Step 3** Enter an Offset from 1-1023.

The offset is relative to the beginning of the payload (Layer 5).

**Step 4** Enter a Value of up to four bytes (eight hex characters).

**Step 5** Enter a Mask of up to four bytes (eight hex characters).

**Step 6** Repeat steps 3, 4 and 5 for up to four payload data segments.

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 7** Click **Apply**.

---

## Configuring Software Filters

To configure a software filter:

---

- Step 1** Enter a filter name.
- Step 2** From the IP Type pull-down menu, choose either IPv4 or IPv6.
- Step 3** Enter the Source IP address.
- Step 4** Enter the Source IP address netmask.
- Step 5** Enter the Destination IP address.
- Step 6** Enter the Destination IP address netmask.
- Step 7** From the Protocol pull-down menu, choose Any (default), TCP, or UDP.

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

- An individual or range of source ports
- An individual or range of destination ports
- An individual or range of VLAN identifiers

- Step 8** Enter values in the appropriate fields depending on whether you want to filter on the source ports, destination ports, or VLAN identifiers.
  - Step 9** Click **Apply** to complete the configuration of the hardware filter. Otherwise, click **Reset** to revert to the previous settings, or click **Cancel** to abort.
- 

## Files

Use the Files option to analyze, decode, merge, download, or delete saved capture files. See the section [Buffers](#), [page 6-2](#) and [Table 6-2](#) for information about how to save capture buffers to files. You can download files from the Sniffer **.enc** or **.pcap** file formats. See [Setting Global Preferences](#), [page 3-94](#), for information about setting the Sniffer download file format.

Choose **Capture > Files** to display the Capture Files window ([Figure 6-8](#)).

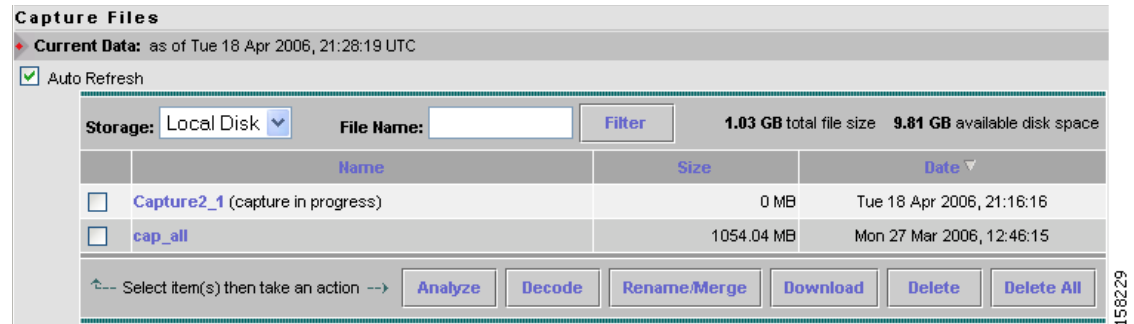


### Note

If you check the Auto Refresh check box, the Capture Files window refreshes automatically every 60 seconds.

---



**Figure 6-8** Capture Files Window

The Capture Files window provides the following options:

- Choose a storage location from the pull-down list to view capture files in that location. Subdirectories of remote storage are listed only if the NAM has full access rights to those remote directories.
- Choose a capture and click **Analyze** to display the packets in a file.
- Choose a capture and click **Decode** to display the packets in a file.
- Click **Convert/Rename/Merge** to merge packets of files. The packets in the file are merged in chronological order.



**Note** Do not add a file suffix when you provide the filename. The suffix **.pcap** is added automatically.

- Click **Download** to download a file to your computer in Sniffer **.enc** or **.pcap** file format.
- Click **Delete** or **Delete All** to delete files.



**Note**

Capture files on the NAM 2200 Series 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 > Files** window.

## Analyzing Capture Files

The Analyze button of the Capture Files window enables you to obtain different statistics including traffic rate (bytes/second) over a capture period, lists of hosts, conversations, and applications associated with network traffic. [Figure 6-9](#) shows an example of the Capture Analysis window.

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.

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 clicking **Drill-Down**. You can also drill down on a specific **Protocol** or **Host/subnet** address.

**Figure 6-9** Capture Statistical Analysis Window

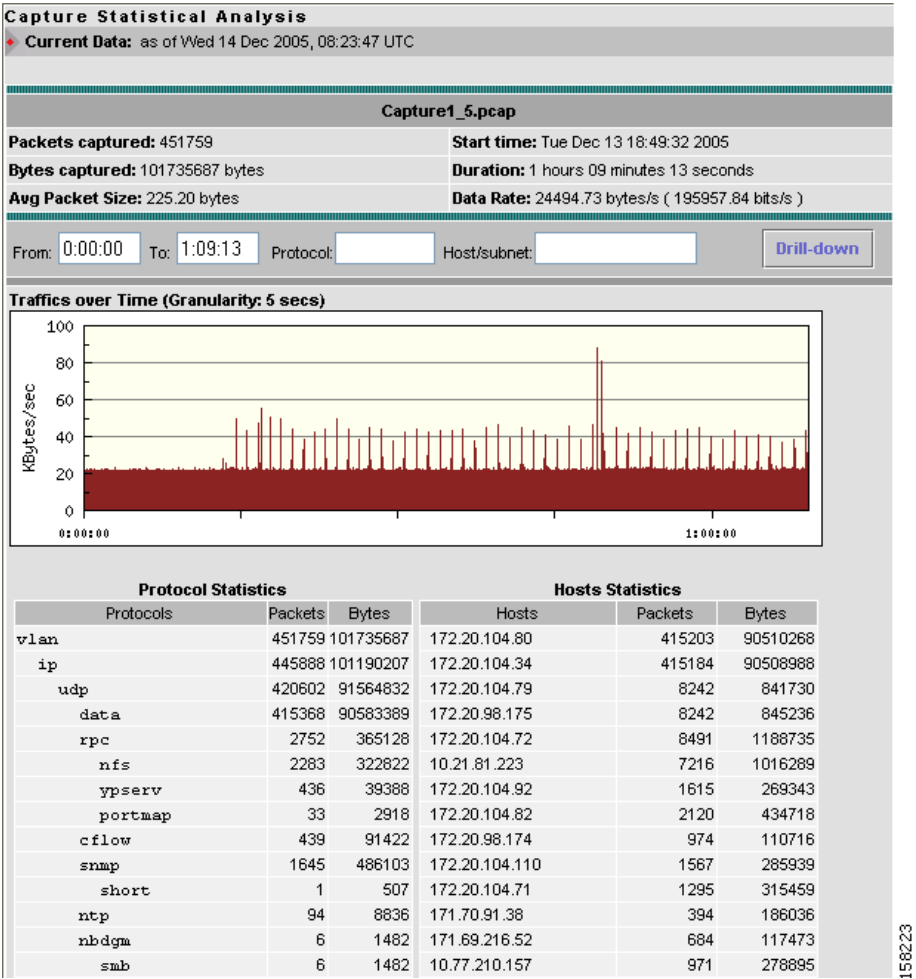


Table 6-11 describes the different areas of the capture analysis window.

**Table 6-11** Capture Analysis Window Fields

| Field               | Description                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capture Overview    | Provides a summary of the displayed capture including number of packets captured, bytes captured, average packet size, capture start time, duration of capture, and data transfer rate (both bytes and bits per second) |
| Traffic over Time   | Displays a graphic image of network traffic (KB/second)                                                                                                                                                                 |
| Protocol Statistics | Displays packets and bytes transferred for each protocol                                                                                                                                                                |
| Hosts Statistics    | Displays packets and bytes transferred for each host address                                                                                                                                                            |

## Decoding Capture Files

Decoding capture files is described in section [Viewing Packet Decode Information](#), page 6-11.

## Renaming or Merging Capture Files

Use the **Rename/Merge** button to rename a single capture file or merge multiple capture files into one file.

**Note**

On NAM 2200 Series appliances, this button is labeled **Convert/Rename/Merge**.

### Renaming Capture Files

To rename a capture file:

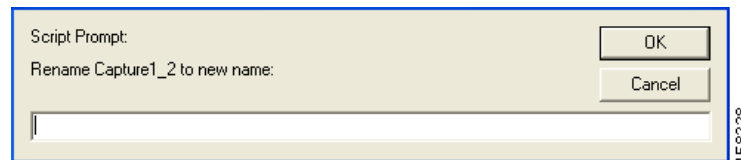
**Step 1** Choose **Capture > Files**.

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

**Step 3** Click **Convert/Rename/Merge**.

A dialog box displays and asks you to enter the new name for the selected capture file.

**Figure 6-10** *Rename Capture File Dialog Box*



**Step 4** Enter a new name for the capture file and click **OK**.

### Merging Capture Files

To merge multiple capture files into one capture file:

**Step 1** Choose **Capture > Files**.

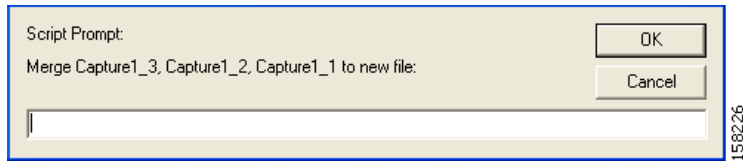
**Step 2** Choose two or more capture files from the list of captures.

**Step 3** Click **Convert/Rename/Merge**.

A dialog box displays and asks you to enter the new name for the merged capture files.

**Note**

Merged files cannot exceed 2 GB.

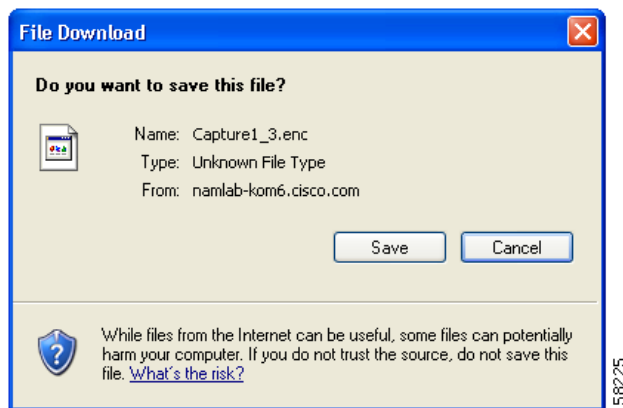
**Figure 6-11 Merging Capture Files Dialog Box**

- Step 4** Enter a name for the merged capture files and click **OK**.  
The capture files are merged in timestamp order from oldest to most recent.

## Downloading Capture Files

The following procedure describes how to download a capture file to your computer. You can only download one capture file at a time.

- Step 1** Choose **Capture > Files**.  
**Step 2** Choose a capture file from the list of captures.  
**Step 3** Click **Download**.  
 A **File Download** dialog box displays and asks “Do you want to save this file?”

**Figure 6-12 Download Capture File Dialog Box**

- Step 4** Click **Save**.  
A **Save As** dialog box opens and provides a way for you to rename and save the file at a location of your choice.

## Deleting a Capture File

To delete a capture file:

- 
- Step 1** Choose **Capture > Files**.
- Step 2** Choose a capture file from the list of captures.
- 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 or **Cancel** to allow the file to remain.
- 

## Deleting All Capture Files

To delete all capture files at once:

- 
- Step 1** Choose **Capture > Files**.
- Step 2** Choose a capture file from the list of captures.
- Step 3** Click **Delete All**.  
A dialog box displays and asks “**Delete all capture file(s)?**”
- Step 4** Click **OK** to delete all the files or **Cancel** to allow them to remain.
- 

## Custom Capture Filters

You can use custom capture filters to create and save specialized filters to disregard everything except the information you are interested in when you capture data.

For more information about using custom filters when capturing data, see the [“Capturing Using a Custom Filter” section on page 6-10](#).

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

- [Creating Custom Capture Filters, page 6-27](#)
- [Editing Custom Capture Filters, page 6-30](#)
- [Deleting Custom Capture Filters, page 6-30](#)

## Creating Custom Capture Filters

To create a custom capture filter:

- 
- Step 1** Choose **Capture > Custom Filters**.  
The Custom Capture Filters dialog box is displayed.
- Step 2** Click **Create**.  
The [Custom Capture Filter Dialog Box \(Table 6-12\)](#) displays.
- Step 3** Enter information in each of the fields as appropriate.

**Table 6-12 Custom Capture Filter Dialog Box**

| Field         | Description and Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter Name   | Enter a name of the new filter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description   | Brief description of the filter.<br>Enter a description from 1 to 35 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Protocol      | The protocol to match with the packet.<br>Choose the encapsulation from the drop-down list, then select the protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Data          | The data pattern to be matched with the packet. Use the Offset field to specify the starting location for the data to be checked.<br><br>Enter <i>hh hh hh . . .</i> , where <i>hh</i> represents hexadecimal numbers from 0 to 9 or a to f.<br><br>For example, to designate the decimal value 15, use the hexadecimal value 0f. For the decimal value 255, use the hexadecimal value ff. For the decimal value 16, use the hexadecimal value 10. See <a href="#">Tips for Creating Custom Capture Filter Expressions, page 6-29</a> , for more examples.<br><br>Leave blank if not applicable.<br><br>If the packet is too short and does not have enough data to match, the packet match fails.                                                              |
| Data Mask     | The mask applied to the data matching.<br><br>Enter <i>hh hh hh . . .</i> , where <i>hh</i> represents hexadecimal numbers from 0 to 9 or a to f.<br><br>Leave blank if all data bits are relevant.<br><br>If a bit in the Data Mask is set to 1, the corresponding bit in the packet is relevant in the matching algorithm.<br><br>If a bit in the Data Mask is set to 0, the corresponding bit in the packet is ignored.<br><br>If you do not specify the Data Mask, or if it is shorter than the Data field, the Data Mask is padded with “1” bits up to the length of the Data field. For example, if you enter a four-byte value in the Data field and leave the Data Mask field blank, that is the same as specifying a Data Mask of <i>ff ff ff ff</i> . |
| Data Not Mask | The mask applied to reverse data matching.<br><br>Enter <i>hh hh hh . . .</i> , where <i>hh</i> represents hexadecimal numbers from 0 to 9 or a to f.<br><br>Leave blank for no reverse data matching.<br><br>For those bits in the Data Not Mask that are set to 0 (or not specified), the relevant bits in the packet must match the corresponding bit in the Data field.<br><br>For those bits in the Data Not Mask that are set to 1, at least one relevant bit in the packet must be different than the corresponding bit in the Data field.<br><br>If you do not specify the Data Not Mask, or if it is shorter than the Data field, the Data Not Mask is padded with “0” bits up to the length of the Data field.                                        |
| Offset        | Enter a decimal number, the offset (in bytes, from the Base) where packet data-matching begins.<br><br>This offset applies to the Data, Data Mask, and Data Not Mask fields.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 6-12** Custom Capture Filter Dialog Box (continued)

| Field           | Description and Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base            | <p>Choose absolute or a protocol, the base from which the offset is calculated.</p> <p>If you select absolute, the offset is calculated from the absolute beginning of the packet (the beginning of the Ethernet frame). You must account for an 802.1q header when calculating an offset for NAM-1 and NAM-2 devices.</p> <p>If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match.</p>                                                              |
| Status          | <p>The status to match with the packet.</p> <p>Enter a number from 0 to 65535; leave blank if not applicable.</p> <p>For Ethernet packet captures, the status bits are:</p> <p>Bit 0—Packet is longer than 1518 octets.</p> <p>Bit 1—Packet is shorter than 64 octets.</p> <p>Bit 2—CRC or alignment error.</p> <p>For example, an Ethernet fragment has a status value of 6 (bits 1 and 2 set).</p>                                                                                                                                                                                |
| Status Mask     | <p>The mask applied to the status matching. Enter a number from 0 to 65535; leave blank if all status bits are relevant.</p> <p>If a Status Mask bit is set to 1, the corresponding bit in the packet status is relevant in the matching algorithm.</p> <p>If a Status Mask bit is set to 0, the corresponding bit in the packet status is ignored.</p> <p>If you do not specify a Status Mask, or if it is shorter than the Status field, the Status Mask is padded with “1” bits up to the length of the Status field.</p>                                                        |
| Status Not Mask | <p>Enter a number from 0 to 65535, the mask applied to reverse status matching.</p> <p>Leave blank for no reverse status matching.</p> <p>For those bits in the Status Not Mask that are set to 0 (or not specified), the relevant status bits of the packet must match the corresponding bit in the Status field.</p> <p>For those bits in the Status Not Mask that are set to 1, at least one relevant bit of the status packet must be different than the corresponding bit in the Status field.</p> <p>If you do not specify a Status Not Mask, it is padded with “0” bits.</p> |

**Step 4** Click **Apply** to create the filter, or click **Reset** to cancel the changes.

## Tips for Creating Custom Capture Filter Expressions

The TOS value is stored in byte 1 (the second byte) in the IP header. To match the IP packet with a TOS value of 16 (0x10), enter:

Data—10  
Offset—1  
Base—IP

With nothing in the Data Mask, its effective value is *ff*.

The source address of an IP packet is stored in bytes 12 to 15 in the IP header. To match IP packets with a source address of 15.16.17.18, enter:

Data—0f 10 11 12  
Offset—12  
Base—IP

To match IP packets with a source address of 15.\*.\*.18 (where \* is any number from 0 to 255), enter:

Data—0f 00 00 12  
Data Mask—ff 00 00 ff  
Offset—12  
Base—IP

To match IP packets with a source address of 15.16.17.18 and a destination address different than 15.16.17.19, enter:

Data—0f 10 11 12 0f 10 11 13  
Data Mask—ff ff ff ff ff ff ff  
Data Not Mask—00 00 00 00 00 00 00 00  
Offset—12  
Base—IP

## Editing Custom Capture Filters

To edit custom capture filters:

- 
- Step 1** Choose **Capture > Custom Filters**.  
The Custom Capture Filters dialog box is displayed.
- Step 2** Choose the filter to edit, then click **Edit**.  
The Custom Capture Filter dialog box (see [Table 6-12 on page 6-28](#)) 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 **Apply**.
  - To cancel the changes, click **Reset**.
- 

## Deleting Custom Capture Filters

To delete custom capture filters:

- 
- Step 1** Choose **Capture > Custom Filters**.  
The Custom Capture Filters dialog box is displayed.
- 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**.

## 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 6-31](#)
- [Editing Custom Display Filters, page 6-35](#)
- [Deleting Custom Display Filters, page 6-35](#)

## Creating Custom Display Filters

To create custom display filters:

- 
- Step 1** Choose **Capture > Custom Filters**.
- Step 2** In the contents, click **Display Filters**.  
The Custom Display Filters dialog box is displayed.
- Step 3** Click **Create**.  
The Custom Decode Filter Dialog Box, [Table 6-13](#), displays.
- Step 4** Enter information in each of the fields as appropriate.

**Table 6-13** Custom Decode Filter Dialog Box

| Field               | Description                                                            | Usage Notes                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter Name         | The name of the capture filter.                                        | Enter the name of the filter to be created.                                                                                                                                                                                                                |
| Description         | The description of the capture filter.                                 | Enter a description of the filter.                                                                                                                                                                                                                         |
| Protocol            | The protocol to match with the packet.                                 | Choose a protocol from the list. (Select <b>All</b> to match all packets regardless of protocol.)                                                                                                                                                          |
| Address (MAC or IP) | Indicates whether to filter by MAC or IP address.                      | Choose MAC to filter using the source/destination MAC address of the packets.<br>Choose IP to filter using the source/destination addresses of the packets.                                                                                                |
| Both Directions     | Indicates whether the filter is applied to traffic in both directions. | If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A.<br>If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A. |

**Table 6-13** Custom Decode Filter Dialog Box (continued)

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                     | Usage Notes                                                                                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source      | Source address of the packets.                                                                                                                                                                                                                                                                                                                                                                  | For IP address, enter <i>n.n.n.n</i> , where <i>n</i> is 0 to 255 or <i>n.n.n.n/s</i> where <i>s</i> is the subnet mask (0 to 32).<br>For MAC address, enter <i>hh hh hh . . .</i> , where <i>hh</i> are hexadecimal numbers from 0 to 9 or a to f. |
| Destination | Destination address of the packets.                                                                                                                                                                                                                                                                                                                                                             | For IP address, enter <i>n.n.n.n</i> , where <i>n</i> is 0 to 255 or <i>n.n.n.n/s</i> where <i>s</i> is the subnet mask (0 to 32).<br>For MAC address, enter <i>hh hh hh hh hh hh</i> , where <i>hh</i> are hexadecimal numbers from 0-9 or a-f.    |
| Offset      | The offset (in bytes) from the Base where packet data-matching begins.                                                                                                                                                                                                                                                                                                                          | Enter a decimal number.                                                                                                                                                                                                                             |
| Base        | The base from which the offset is calculated.<br><br>If you select absolute, the offset is calculated from the absolute beginning of the packet (for example, the beginning of the Ethernet frame).<br><br>If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match. | Choose <b>absolute</b> or a protocol.                                                                                                                                                                                                               |

**Table 6-13** Custom Decode Filter Dialog Box (continued)

| Field             | Description                                                                                                                                                                                                                                                            | Usage Notes                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Data Pattern      | The data to be matched with the packet.                                                                                                                                                                                                                                | Enter <i>hh hh hh . . .</i> , where <i>hh</i> are hexadecimal numbers from 0-9 or a-f.<br><br>Leave blank if not applicable. |
| Filter Expression | An advanced feature to set up complex filter conditions.<br><br>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 <b>ipx</b> . | See the “ <a href="#">Tips for Creating Custom Decode Filter Expressions</a> ” section on page 6-33.                         |

- Step 5** Do one of the following:
- To create the filter, click **Apply**.
  - To cancel the changes, click **Reset**.

## Tips for Creating Custom Decode Filter Expressions

You can construct custom decode filter expressions using the following logical and comparison operators listed in [Table 6-14](#).

**Table 6-14** Logical and Comparison Operators

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

You can also group subexpressions within parentheses. You can use the following fields in filter expressions:

| Field                          | Filter By   | Format                                                                                             |
|--------------------------------|-------------|----------------------------------------------------------------------------------------------------|
| eth.addr<br>eth.src<br>eth.dst | MAC address | <i>hh : hh : hh : hh : hh : hh</i> , where <i>h</i> is a hexadecimal number from 0 to 9 or a to f. |

| Field                                    | Filter By             | Format                                                                                                                                                                                                                                                      |
|------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip.addr<br>ip.src<br>ip.dst              | IP address            | <i>n.n.n.n</i> or <i>n.n.n.n/s</i> , where n is a number from 0 to 255 and s is a 0-32 hostname that does not contain a hyphen.                                                                                                                             |
| tcp.port<br>tcp.srcport<br>tcp.dstport   | TCP port number       | A decimal number from 0 to 65535.                                                                                                                                                                                                                           |
| udp.port<br>udp.srcport<br>udp.dstport   | UDP port number       | A decimal number from 0 to 65535.                                                                                                                                                                                                                           |
| <i>protocol</i>                          | Protocol              | Click the Protocol list in the Custom Decode Filter dialog box to see the list of protocols on which you can filter.                                                                                                                                        |
| <i>protocol</i> [ <i>offset:length</i> ] | Protocol data pattern | <i>hh:hh:hh:hh...</i> , where hh is a hexadecimal number from 0 to 9 or a to f.<br><br><i>offset</i> and <i>length</i> are decimal numbers.<br><br><i>offset</i> starts at 0 and is relative to the beginning of the <i>protocol</i> portion of the packet. |
| frame.pkt_len                            | Packet length         | A decimal number that represents the packet length, not the truncated capture packet length.                                                                                                                                                                |

#### Examples of Custom Decode Filter Expressions

- To match SNMP packets from 111.122.133.144, enter:  
`snmp and (ip.src == 111.122.133.144)`
- To match IP packets from the 111.122 Class B network, enter:  
`ip.addr == 111.122.0.0/16`
- To match TCP packets to and from port 80, enter:  
`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:  
`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:  
`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 > Custom Filters**.
- Step 2** In the contents, click **Display Filters**.  
The Custom Display Filters dialog box is displayed.
- Step 3** Choose the filter to edit, then click **Edit**.
- Step 4** Change the information in each of the fields as appropriate.
- Step 5** Do one of the following:
- To apply the changes, click **Apply**.
  - To cancel the changes, click **Reset**.
- 

## Deleting Custom Display Filters

To delete custom display filters:

- 
- Step 1** Choose **Capture > Custom Filters**.
- Step 2** In the contents, click **Display Filters**.  
The Custom Display Filters dialog box is displayed.
- Step 3** Choose the filter to delete, then click **Delete**.
- Step 4** In the confirmation dialog box, do one of the following:
- To delete the filter, click **OK**.
  - To cancel, click **Cancel**.
-





# CHAPTER 7

## Viewing Alarms

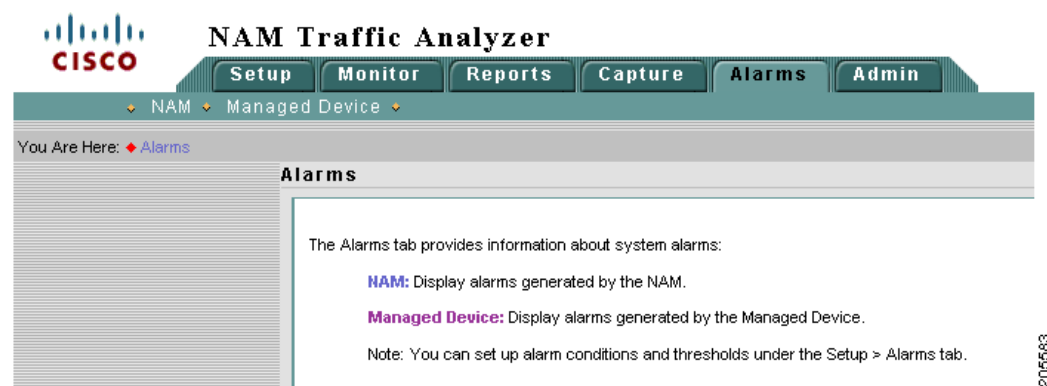
Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation and be alerted to potential problems.



**Note**

NAM 4.0 supports IPv6 for all alarm functionality.

**Figure 7-1**      **Alarms Window**



**Note**

NAM-1 and NAM-2 devices list *Chassis* as the second option instead of *Managed Device* and provide alarms generated by Catalyst 6000 Series Switches, Catalyst 6500 Series Switches, and Cisco 7600 Series Routers.

You can set up the following:

- Alarm events based on an SNMP trap community string  
See [Setting Up Alarm Events, page 3-82](#) for more detailed information.
- Alarm thresholds based on parameters you specify from a list of pre-selected variables  
See [Setting Alarm Thresholds, page 3-84](#) for more detailed information.
- Voice/Video stream thresholds  
See [Setting Up Voice/Video Stream Thresholds, page 3-88](#) for more detailed information.

**Note**

You can use an external SNMP manager to set up thresholds for NAM MIB variables by configuring the alarm and event tables in the NAM. However, you can set up thresholds for voice-monitoring variables only with the Catalyst 6500 NAM Traffic Analyzer.

Syslog messages are created for MIB threshold events, voice threshold events, or systems alerts. You can view two alarm logs:

- [Viewing NAM Threshold Alarms, page 7-2.](#)
- [Viewing Chassis Threshold Alarms, page 7-2.](#)

**Note**

The Switch Log does not apply to NM-NAM or NME-NAM devices, nor does it apply to the Cisco 2200 Series NAM appliances.

## Viewing NAM Threshold Alarms

The NAM Threshold Alarms window displays all threshold-crossing events for NAM MIB thresholds and NAM voice-monitoring thresholds.

**Step 1** Choose **Alarms > NAM**.

**Step 2** The [NAM Threshold Alarms](#) window, [Table 7-1](#), displays.

**Table 7-1 NAM Threshold Alarms**

| Field       | Description                        |
|-------------|------------------------------------|
| Date        | Date the alarm occurred.           |
| Time        | Time the alarm occurred.           |
| Description | Description of the alarm.          |
| Variable    | Alarm variable that was triggered. |
| Alarm Value | Value of the alarm.                |
| Message     | Alarm message.                     |

**Step 3** To clear the screen, click **Clear**.

**Tip**

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

## Viewing Chassis Threshold Alarms

**Note**

This section does not apply to NM-NAM or NME-NAM devices.



The switch log displays the RMON log table from the switch mini-RMON MIB.

You can set up switch thresholds from the application using the switch CLI or by an external SNMP manager configuring the switch mini-RMON MIB.

For information on using the application to set up switch thresholds, see the [“Creating Chassis or Managed Device Thresholds” section on page 3-91](#).

For information on using the switch CLI, see *Catalyst 6000 Content Switching Module Installation and Configuration Note*.

---

**Step 1** Choose **Alarms > Switch**.

The [Switch Threshold Alarms](#) window ([Table 7-2](#)) displays.

**Table 7-2 Switch Threshold Alarms**

| Field       | Description               |
|-------------|---------------------------|
| Date        | The date the alarm.       |
| Time        | Time the alarm occurred.  |
| Description | Description of the alarm. |



**Tip**

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

---





# APPENDIX A

## Troubleshooting

---

This appendix addresses some common issues you might encounter while using the NAM Traffic Analyzer.

- [Username and Password Issues, page A-2](#)
- [Login Issues, page A-3](#)
- [Packet Capturing Issues, page A-6](#)
- [Alarm and Interface/Port Stats Issues, page A-8](#)
- [SPAN Related Issues, page A-5](#)
- [NetFlow and NBAR Monitoring Problems, page A-8](#)
- [Report Problems, page A-12](#)
- [Image Upgrade and Patch Issues, page A-13](#)
- [Web Browser Response Time and Display Issues, page A-13](#)
- [NAM Switch Date and Time Synchronization Issues, page A-14](#)
- [Diagnostic Error Message Issues, page A-14](#)
- [Hostname Resolution Issues, page A-15](#)
- [Data Mismatch Issues, page A-16](#)
- [HTTPS/Security Certificate Issues, page A-16](#)
- [SNMP Issues, page A-17](#)
- [Protocol Support Issues, page A-18](#)
- [Voice Monitoring Issues, page A-19](#)
- [WAAS Application Response Time Issues, page A-20](#)

## 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*)

## CPU Usage Percentage

- Q. The NAM output of **show tech-support** command shows CPU usage that exceeds 100% for a process. Is there a problem with that process?
- A. No; the value shown is the sum of all current CPU usage for this process. In the following example, PID 1925 shows 305% CPU usage. This means that the total usage percentage of all of the NAMs CPUs totaled 305%.

| PID  | USER | PR | NI | VIRT  | RES  | SHR  | S | %CPU | %MEM | TIME+   | COMMAND |
|------|------|----|----|-------|------|------|---|------|------|---------|---------|
| 1925 | root | 15 | 0  | 3266m | 1.4g | 5804 | S | 305  | 8.9  | 3569:25 | mond    |
| 9626 | root | 20 | 0  | 10516 | 1172 | 784  | R | 2    | 0.0  | 0:00.01 | top     |
| 1    | root | 15 | 0  | 3676  | 568  | 476  | S | 0    | 0.0  | 0:03.87 | init    |

Using a NAM with only one CPU, the CPU usage percentage will never exceed 100%, while using a NAM with two CPUs, the CPU usage percentage would never exceed 200%. Using a Cisco NAM 2220 appliance with eight CPUs, the CPU usage percentage can exceed 200% or more. The value shown represents the sum of all current CPUs used by this process, not the over the length of process run time.

A high individual CPU usage percentage value for NAMs with multiple CPUs is a different case, but not unexpected. A software change in NAM 4.0 provides improved performance but can show high CPU usage percentage, even when the NAM is not busy, as the NAM polls incoming packets. When more packets arrive, the time used for packet polling shifts to real packet processing.

To see current CPU usage percentages, including individual and average for all, click **Admin > System** to view the System Resources window as described in section [System Resources, page 2-11](#).

## Username and Password Issues

- Q. Can I use my CLI username (root or guest) and password to log into the NAM Traffic Analyzer? Or, can I use my NAM Traffic Analyzer username and password to log into the NAM CLI?
- A. No. Web and CLI users are administered separately. You can create web users with a local database or using TACACS+. You can create a web user with the same username and password as used on the CLI. However, you must still make password changes in both places.
- Q. If I use TACACS+, must I still have web users defined in my local database?
- A. No. You can use TACACS+ either in addition to a local database or instead of a local database. (The local database is always checked first.) To use only TACACS+, you can eliminate the local database users by either of these methods:
- Use the NAM CLI **rmwebusers** command to remove only local users, not TACACS+ users, as they are administered separately on the TACACS+ server.

- From the Admin tab, click **Users**, then delete all local database users individually.

**Caution**

Do not delete all local database web users until you have verified that you can log into the NAM Traffic Analyzer as a TACACS+ user.

Q. How can I recover the local web admin user password?

A. You can recover the password in situations where you have forgotten the local web admin user password, or when another user with Account permission logged in and changed the local web admin user password.

To recover the local web admin user password:

**Step 1** Access the NAM CLI.

**Step 2** Enter the following commands:

```
web-user
user name <name>
exit
```

**Step 3** At the prompt, enter the new password.

**Step 4** Enter **Y** to confirm the new password.

Q. How can I recover when I mixed up the TACACS+ configuration between my NAM and TACACS+ server, and I do not have a local database user account to fix my TACACS+ configuration on my NAM?

A. If you cannot fix this problem from the TACACS+ server, go to the NAM CLI and enter **ip http tacacs+ enable** to reconfigure the TACACS+ settings.

Q. Are there restrictions on using passwords when performing upgrades or applying patches?

A. Yes. Do not include the password as an argument in upgrade and patch commands. Use command syntax of this form:

```
patch ftp://user@host/full-patch/filename
```

Enter the password when prompted.

## Login Issues

Q. Why does my login session time out?

A. Your login session automatically times out after approximately 1 hour of inactivity, then logs you out of the NAM Traffic Analyzer.

**Note**

If you are viewing a window in which the autorefresh feature is enabled, your login session does not time out.

Q. Why do users remain logged in after their user accounts are deleted?

A. 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.

Q. Why am I unable to log into the NAM Traffic Analyzer with TACACS+ configured?

A. Verify that you entered the correct TACACS+ server name and secret key and that you are using the same the secret key as the one configured in the TACACS+ server. If you use a generic TACACS+ server, make sure that it supports Password Authentication Protocol (PAP) and that PAP is selected.

You can also check system alerts for any TACACS+-related messages.

- 
- Step 1** Log into the NAM Traffic Analyzer as a local user.
- Step 2** Choose **Admin > Diagnostics**.
- Step 3** In the contents, click **Tech Support**.
- Step 4** Scroll down to the **/var/log/messages** section.
- Step 5** Look for messages similar to the following, then take the appropriate action.
- 

| Message                                                                                                                                                                                                              | Likely Cause and Action                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ...PAM-tacplus[612]:auth failed:<br>Login incorrect                                                                                                                                                                  | <p>The username and password do not match any usernames and passwords in the TACACS+ server.</p> <ol style="list-style-type: none"> <li>1. Log into the TACACS+ server.</li> <li>2. Configure the server to authenticate and authorize NAM users.</li> </ol> <p>(See the <a href="#">“Establishing TACACS+ Authentication and Authorization”</a> section on page 2-6.)</p>                                         |
| ... httpd: tac_authen_pap_read: error<br>reading PAP authen header, read -1 of 12:<br>Connection reset by peer<br><br>... PAM-tacplus[10455]: auth failed:<br>Authentication error, please contact<br>administrator. | <p>The NAM has not been added to the NAS (AAA client) list of the ACS/TACACS+ server.</p> <ol style="list-style-type: none"> <li>1. Log into the TACACS+ server.</li> <li>2. Make sure that the NAM is in the NAS (AAA client) list and TACACS+ is selected as the authentication method.</li> </ol> <p>(See the <a href="#">“Establishing TACACS+ Authentication and Authorization”</a> section on page 2-6.)</p> |
| ...httpd:tac_authen_pap_read:<br>invalid reply content, incorrect key?<br>...PAM-tacplus[616]:auth failed:<br>Authentication error, please contact<br>administrator.                                                 | <p>The TACACS+ secret key configured in the NAM does not match the secret key of the TACACS+ server.</p> <ol style="list-style-type: none"> <li>1. Choose <b>Admin &gt; Users</b>.</li> <li>2. In the contents, click <b>TACACS+</b>.</li> <li>3. Enter the correct secret key in the Secret Key and Repeat Secret Key fields.</li> <li>4. Click <b>Apply</b>.</li> </ol>                                          |

| Message                                                                                                                                                                                                                                                           | Likely Cause and Action                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>..httpd:tac_connect:connection to 172.20.122.183 failed:Connection timed out ...httpd:tac_connect:all possible TACACS+ servers failed ...PAM-tacplus[613]:connection failed srv 0: Connection timed out ...PAM-tacplus[613]:no more servers to connect</pre> | <p>An incorrect TACACS+ server IP address is configured on the NAM.</p> <ol style="list-style-type: none"> <li>1. Click <b>Admin</b>.</li> <li>2. Click <b>Users</b>.</li> <li>3. In the contents, click <b>TACACS+</b>.</li> <li>4. Enter the correct TACACS+ server address.</li> <li>5. Click <b>Apply</b>.</li> </ol> |
| <p>Not authorized...<br/>(when accessing NAM Traffic Analyzer)</p>                                                                                                                                                                                                | <p>The user does not have the necessary access rights.</p> <ol style="list-style-type: none"> <li>1. Log into the TACACS+ server.</li> <li>2. Grant the appropriate rights to the user.</li> </ol> <p>(See the <a href="#">“Adding a NAM User or User Group”</a> section on page 2-8.)</p>                                |

## SPAN Related Issues



### Note

This section applies to NAM-1 and NAM-2 only.

Q. What if the SPAN session does not show up in the Active SPAN window?

A. If you have a switch that is running Catalyst OS, a SPAN session will become inactive if the module that contains the destination port is removed from the switch chassis. In this case, the NAM will not see the SPAN session because the SPAN configuration has been removed from the SNMP agent by the Supervisor engine module.

Q. Why does my create SPAN session fail on a switch running Cisco IOS?

A. For switches running Cisco IOS, a SPAN session can be partially defined with either a source type or destination port only. The NAM will not see this partial SPAN session. However, the partially configured SPAN session may cause the create SPAN request to fail if there is a conflict with either the source type or destination port.

Q. How do I change the SPAN session so it only spans in one direction—or, change the SPAN session type from switch port to VLAN or VLAN to switch port?

A. You cannot edit these characteristics using the NAM Traffic Analyzer after creating the SPAN session. Instead, you must delete the SPAN session and create a new one with the desired characteristics.

You can also simply click **Create** (without deleting the SPAN session) to overwrite the current SPAN.



### Note

You can only add or delete VLANs (if the current SPAN session is already VLAN) in a SPAN session in the Setup SPAN Sources dialog box. You cannot change the SPAN traffic type (such as changing VLAN to ports or changing the traffic direction).

- Q. Why do I sometimes see the message, `Failed to create SPAN session for...`, when I create or edit a SPAN session in the Setup SPAN Sources dialog box?
- A. This usually happens because you reached the SPAN limit on the switch. To determine the applicable limits, see the appropriate Catalyst OS or Cisco IOS documentation. The simplest solution is to delete the SPAN (or RSPAN, if applicable) session and try to edit or create a new one.

## Packet Capturing Issues

- Q. Why is the capture buffer locked and why are no packets being captured in the Capture Settings dialog box?

- A. This happens because you selected **Lock when full**, which prevents the capture process from overwriting the contents when the buffer fills.

To restart a locked capture, you first have to clear it. You might want to save the capture buffer to a file before clearing it.



### Note

- You can also select **Wrap when full** so the newly arriving packets overwrite the oldest packets when the capture buffer is full.

- Q. Why am I having problems capturing packets, even after I configured the capture settings in the Capture Settings dialog box and clicked **Start**?

- A. This might happen for several reasons.

Verify that the data source you selected in the **Capture packets from** list is spanned to the NAM.



### Tip

The NAM automatically learns VLANs from the switch, but does not automatically SPAN them—you must still SPAN them using the Active SPAN Sources window.

To verify that your SPAN session is working:

- Step 1** Choose **Setup > Data Sources**.
- Step 2** Verify that packet traffic is spanned from the appropriate source.
- Step 3** If not, click **Create** or **Edit**, to add the desired SPAN sources.
- Step 4** Click **Submit**.
- Step 5** Choose **Capture > Settings**.
- Step 6** Click **Start**.

You should also verify that you selected filters carefully in the Capture Settings dialog box. The filter you created might be too restrictive. (For more information, see [Chapter 6, “Capturing and Decoding Packet Data.”](#))

If you still cannot capture packets, try to remove all capture filters:

- Step 1** Choose **Capture > Buffers**.



- Step 2** Select the capture buffer and click **Settings**.
  - Step 3** Deselect the Address, Protocol, Port, and Custom check boxes.
  - Step 4** To restart the capture, click **Start**.
- 

You might also have selected a filter based on a protocol that has been deleted from the NAM protocol directory (by an SNMP manager or another web user).

To see the protocols available for filtering, do the following:

---

- Step 1** Choose **Setup > Monitor**.
  - Step 2** In the contents, click **Protocol Directory**.
- 

Capture might fail to start because no memory is available for capture buffers. To find out about NAM capture memory usage, choose **Capture > Buffers**. Clear or delete old buffers to free up capture memory.

Q. Why do I see duplicate captured packets?

- A. When packets appear twice in the Capture Decode dialog box, it might be because you are spanning in both directions (transmit and receive).

Q. Why does the automatic capture trigger not stop or start?

- A. The alarm associated with the automatic capture might have not occurred yet. Go to **Alarms > NAM** to see the list of past alarm occurrences. In addition, for start capture triggers, the capture buffer should initially be in a paused state.

If the buffer is cleared or running, a start capture trigger does not work. For stop capture triggers, the capture buffer should be running initially. If the buffer is paused or cleared, a stop trigger does not work. For more information, see the [“Configuring Capture Settings” section on page 6-3](#).

Q. Why am I unable to start a capture from the Monitor window?

- A. When the buffer has been completely allocated to other capture processes and the available buffer is 0 MB, the capture process will not start. To solve this problem, clear an existing capture process to free up the buffer so new processes can be started.

Q. Why does the layer two information in packets captured on an internal port of the NM-NAM look wrong.

- A. The router copies the packets to the NM-NAM in the CEF path. At that time the layer two has been stripped off. A special layer two header is used to send the packet to the NM-NAM

Q. Why do I see additional traffic on the NM-NAM internal port besides what I configured to be monitored.

- A. Besides the traffic copied to the NM-NAM by the analysis-module monitoring feature, management traffic might also be directed to the NM-NAM that is captured.

## Alarm and Interface/Port Stats Issues

- Q. Why does one of the alarms in the Setup/Alarm/NAM MIB Thresholds window show the Data Source as Collection Deleted?
- A. Data Sources are mapped to a table collection index. When you delete the collection from the Setup/Monitor/Core window, the table index is deleted. Because the alarm data source can no longer map to a table index, you must delete the alarm and recreate it.
- Q. Why am I unable to create threshold alarms or view interface or port statistics?
- A. Two typical reasons might be because there is no connectivity between the switch and the NAM, or that mini-RMON is not enabled on the switch.

### For WS-SVC-NAM-1 and WS-SVC-NAM-2 devices

To verify that there is connectivity, go to **Setup > Chassis Parameters > Chassis Information** and view the SNMP read from switch and SNMP write to switch results. For more information on the Switch Information table, see the [“Viewing the Switch Information” section on page 3-2](#).

To verify that Mini-RMON is enabled on the switch, go to **Setup > Chassis Parameters > Port Stats (Mini-RMON)** and view the Current Status in the table. For more information on enabling Mini-RMON, see the [“Enabling Mini-RMON Collection” section on page 3-56](#).

### For NM-NAM or NME-NAM Devices

To verify that there is connectivity, check that the community strings are configured. You can also go to **Setup > Router Parameters** and click the **Test** button to verify that the community string is correct. For more information on testing the router community strings, see the [“Testing the Router Community Strings” section on page 3-33](#).

- Q. Why do I see negative values on the Alarms window?
- A. The alarm counters wrapped back to zero between the last poll and the current poll.
- Q. Why does the Cumulative Data table for port/interface statistics take a long time to load?
- A. This might be because of poor or nonexistent connectivity. To check your connectivity, go to **Setup > Chassis Parameters** and click **Test**.



**Note** For NM-NAM or NME-NAM devices, go to **Setup > Router Parameters**.

## NetFlow and NBAR Monitoring Problems

- Q. Why is there no data for the default NetFlow data source of the device?
- A. Select **Setup > Data Sources > NetFlow > Listening Mode** and click **Start**. If the device is displayed in the table, see the [“Why is there no data in collections even though the Listening Mode table shows that the NAM is receiving NDE packets from the device?” question on page A-9](#). If the device is not displayed in the table after three refresh cycles, the NAM is not seeing NetFlow packets from the device. There is either a network problem or the device is not configured properly.

To verify that a NetFlow device is configured to send NetFlow packets to UDP port 3000 of the NAM, use the following command:

```
prompt#show ip flow export
```

or

```
prompt#show mls nde
```

Displayed information shows whether NetFlow export is enabled or disabled, to what IP address and port NetFlow packets are being exported, and the number of NDE packets that were sent to the NAM. For more information on configuring your NetFlow device, see the [“Configuring NetFlow on Devices” section on page 3-22](#) or your accompanying device documentation.

- Q. Why is there no data in collections even though the Listening Mode table shows that the NAM is receiving NDE packets from the device?
- A. Verify that you have data for the collections in the **Monitor > Hosts**, **Monitor > Apps** and **Monitor > Conversations** pages. If there is NetFlow data on the Monitor pages, then the auto refresh interval might be too fast. For more information on troubleshooting the auto refresh interval, see the [“Why are the Monitor > Hosts, Monitor > Apps and Monitor > Conversations pages showing data only every two \(or more\) auto refresh cycles?” question on page A-9](#) and the [“Why does the Network Conversations table on the Monitor>Conversations page have 0.0.0.0 for all entries in the source column?” question on page A-11](#).

If there is *no* NetFlow data on the Monitor pages, then you might be using an incompatible version of NDE. Make sure that the NDE version is 1, 5, 6, 7, or 8. For more information, see the [“Why do the Monitor>Hosts and Monitor>Conversations pages have no active flow data?” question on page A-10](#).




---

**Note** NDE version v8-AS-Aggregation is not supported.

---

- Q. Why are the **Monitor > Hosts**, **Monitor > Apps** and **Monitor > Conversations** pages showing data only every two (or more) auto refresh cycles?
- A. This is caused by the implementation of the NDE source device. Entries in the NetFlow cache expire after a certain level of inactivity, if the end of a connection is detected, or if an expiration time is reached. The expired flow will still be exported to the destination. If the aging time is longer than the NAM refresh interval, no NetFlow packets will appear in one refresh interval of the NAM.

To solve this problem, choose **Setup > Preferences** and increase the auto refresh interval on the NAM, or change the aging time of the NetFlow entries. Before you change the aging time on the NDE source device, consult your NDE usage guidelines.

For devices running Cisco IOS, use the following commands to specify the aging time.

```
Prompt(config)#ip flow-cache timeout <active || inactive> <seconds>
```

or

```
Prompt(config)#mls aging <fast time || long || normal> <seconds>
```

For devices running Catalyst OS, use the following command to specify the aging time.

```
Prompt>(enable) set mls agingtime <long-duration || fast || ip>
```

Where:

- long-duration—Sets the aging time for flows that are long active.

- fast—Sets the aging time for flows that do not exceed packet thresholds.
- ip—Sets aging time for IP flows.

Q. Why are there no collections for a custom NetFlow data source?

A. Verify that the data source is setup on an interface with an Input direction. Output and Both directions are recommended only for special cases. They might require you to enable NetFlow on all interfaces to get comprehensive output direction flow data. For more information on NetFlow flow records, see the [“Understanding NetFlow Flow Records” section on page 3-21](#).

You can verify the interface direction by clicking the Detail button on the NetFlow Listening Mode table. For more information on using the NetFlow Listening Mode, see the [“Using the Listening Mode” section on page 3-30](#).

The custom NetFlow data source might also be collecting data on a wrong interface ifIndex. This is due to ifIndices in the remote NetFlow devices not being persisted after device reboots. It is recommended you use the ifIndex persist feature for any supported devices. For devices running Cisco IOS, the ifIndex can be persisted per interface or globally for all ifIndices.

For example:

- snmp ifindex persist
- snmp-server ifindex persist

For devices running Catalyst OS, ifIndices are always persisted.

Q. Why do the Monitor>Hosts and Monitor>Conversations pages have no active flow data?

A. Either the active flow has not expired, the device has an NDE filter, or the cache is full and new entries cannot be inserted into the cache. In any of these cases, the active flow is not in the NetFlow packets that are being exported to the NAM.

To solve this problem make sure there is no NDE filter on the device, check for long aging times, and check for dropped flow packets.

To check for long aging times to see if the active flow has expired, enter one of the following commands:

```
Prompt>(enable)show ip cache flow
```

```
Prompt>(enable)show mls netflow aging
```

```
Prompt>(enable)show mls
```

Active flows that have an active time *below* the long duration aging time are not yet expired and have not been exported to the NAM. You can set the aging time to a lower value. For information on how to do this, refer to the user documentation for the NDE device.

Q. Why is there no data for a NetFlow data source configured for specific interfaces, but there is data for the default NetFlow data source?

A. There might be no NetFlow record that has the specific interface information. Use the Listening Mode to find out what interfaces have NetFlow records.

---

**Step 1** Choose **Setup > Data Sources > NetFlow > Listening Mode**.

**Step 2** Click **Start**.

**Step 3** Wait until the device table has more than three MDE packet counts.

**Step 4** Select the device in interest.

**Step 5** Click **Details**.

If the interfaces are not in the Details window, you must configure the NetFlow source device manually.

**For Devices Running Cisco IOS**

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

**For Devices Running Catalyst OS**

```
Prompt>(enable) set mls nde destination-ifindex enable
Prompt>(enable) set mls nde source-ifindex enable
```

Make sure the flow mask is set to full or interface-full.

- Q. Why is only the local device address appearing in the drop-down list when I create a NetFlow data source from the **Setup > Data Sources > NetFlow > Custom Data Sources** page?
- A. First you must add the device in the **Setup > Data Sources > NetFlow > Devices** page. A default NetFlow data source for the device is displayed on the **Setup > Data Sources > NetFlow > Custom Data Sources** page. The drop down list now contains the devices.

- Q. Why is there no available interfaces list when I create a NetFlow data source?
- A. Make sure the community string is correct. Use the Test button on the NetFlow Devices table on the **Setup > Data Sources > NetFlow > Devices** page. For more information, see the [“Testing NetFlow Devices” section on page 3-27](#).

If there is an error, the community string might not be correct. Select the device from the NetFlow Devices table, click **Edit**, and enter the correct community string. Also make sure that the remote device accepts SNMP connections.

- Q. Why does the Network Conversations table on the Monitor>Conversations page have 0.0.0.0 for all entries in the source column?
- A. This is because the NDE device has the flow mask set to destination. To set the flow mask to full, interface-destination-source, or interface-full, use the following commands.

**For Devices Running Cisco IOS**

```
Prompt(config)#mls flow ip <full || interface-full>
```

**For Devices Running Catalyst OS**

```
Prompt>(enable) set mls flow full
```



**Note** The NAM supports NDE versions 1, 5, 6, 7, 8, and 9 source-prefix, destination-prefix, prefix, and protocol-port aggregations.

For more information on flow masks and the Monitor pages, see the [“NDE Flow Masks and V8 Aggregation Caches” section on page 4-5](#).

- Q. Why is NBAR not available on switches?
- A. Although NBAR can be configured using the command line on the Catalyst 6500 switches, currently the switches do not provide the MIBs to configure and monitor NBAR.

## Report Problems

- Q. Why does my report not show any data for some or all of the time periods?
- A. This could be for several reasons:
- The report might have been created recently and no data has been collected yet. It takes at least two polling intervals for the first data point to show up.
  - The applicable traffic data source is not being sent to the NAM. For example, the SPAN session might have been configured improperly and it does not contain applicable traffic for the report. Go to **Setup > Data Source** to make sure that the data source for the report is properly configured.
  - The report is disabled.
  - The NAM was shut down or was not running during the time period.
  - The report target is inactive.
- Q. Why does the report status shows OK, but the report has no data during some or all of the time periods?
- A. There might be an error condition or exception. From the reports window, select the tabular report style and click **system events** to view the report error conditions and exceptions. For more information on report error conditions and exceptions, see [Table 5-15 on page 5-23](#).
- Q. Why is there no data in all of my PortStat reports?
- A. PortStat reports require the mini-RMON feature on the switch. Make sure that the switch supports mini-RMON and that it is enabled.
- Q. Why is there no data in all of my VLAN reports?
- A. Top N VLAN reports and target VLAN reports with the Supervisor engine module as a data source require the SMON feature in the switch Supervisor. Make sure that the Supervisor engine module supports the SMON feature and that it is enabled.
- Q. Why does the data in my Response Time reports stay constant for multiple time periods?
- A. You might have selected a reporting interval that is too long. Select **Setup > Monitor > Response Time Monitoring** and select a shorter report interval. It is recommended that you select the same polling interval as your Response Time reports. For example, if you select a 60 minute report interval and a 15 minute polling interval for your reports, the report data will be over-pollled and the same data will repeat for every four consecutive 15 minute intervals.
- Q. What happens to a report if I change the DNS resolution setting?
- A. The Monitor window will not be able to see the report. If you create a report with DNS turned on, the report will be set up with the DNS name as the host. If you then turn DNS off, the Monitor window will look for the IP address instead of the DNS name.

# Image Upgrade and Patch Issues

Q. How do I upgrade the application image of my NAM?

A. For NAM-1 and NAM-2 see the Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Installation and Configuration.



**Note**

For NME-NAM see the *Network Analysis Module (NM-NAM) Feature Guide*.

Q. Why am I having problems upgrading my NAM image?

A. Verify the following:

1. The NAM booted into the correct partition
  - To upgrade the NAM application image, you must boot the NAM into the maintenance partition.
  - To upgrade the NAM maintenance image, you must boot the NAM into the application partition.
2. The URL specifies the correct image location. If it does not, enter the correct URL.
3. The upgrade was not interrupted. If it was, reboot the NAM and start the upgrade again.



**Note**

For more information, see the *Network Analysis Module (NM-NAM) feature module*.

Q. Why am I having problems applying a patch?

A. Verify the following:

- Does the URL specify the correct image location? If not, enter the correct URL.
- Was the patch process interrupted? If so, start the process again.

Q. How can I verify which patches are installed on the NAM?

A. You can use the command-line **show patches** command or click **About** in the toolbar in the NAM Traffic Analyzer user interface.

# Web Browser Response Time and Display Issues

Q. Why do my browser windows (such as the Packet Decode window or those under the Monitor tab) sometimes refresh so slowly?

Q. Why is the Packet Decoder window so slow in displaying packets?

A. You might need to verify that your DNS name servers point to valid DNS servers.



**Tip**

- If the name servers point to nonexistent or misconfigured DNS servers, lookups time out after 20 to 30 seconds.
  - In an environment without DNS, no name servers should be configured.
- You also might need to turn off automatic hostname resolution:

- 
- Step 1** Choose **Setup > Preferences**.
- Step 2** Deselect the Perform IP Host Name Resolution check box.
- Step 3** Click **Apply**.
- 



**Note** For more information, see the [“Hostname Resolution Issues” section on page A-15](#).

---

The browser windows might also refresh slowly because of the amount of data to be sorted and displayed. Consider limiting your collection (such as the number of conversations) and reducing the maximum entries in the appropriate Monitoring window (in the Setup tab) to improve response time.

- Q. Why does the formatting of my browser window or popup windows sometime look incorrect?
- A. If browser displays are not formatted correctly, click your browser **Refresh** button. If popups are not formatted correctly, close and reopen the popup.

## NAM Switch Date and Time Synchronization Issues

- Q. Why are the NAM date and time different than the switch date and time?
- A. When you boot the NAM, the NAM date and time are synchronized with the date and time on the switch. However, if the dates and times do not match, go to **Admin > System > NAM System Time** to synchronize the NAM system time with the switch or an NTP server. For more information on using the NAM System Time, see the [“NAM System Time” section on page 2-16](#).
- Q. Why does the NAM display an incorrect time when I change the time synchronization method from NTP to switch?
- A. For Supervisors running Catalyst OS images earlier than 7.5(1), the NAM system time is synchronized with the switch only at startup. The NAM will not resynchronize time with the switch when you change from NTP time to switch time. To work around this problem, reset the NAM.

## Diagnostic Error Message Issues

- Q. What do these errors in the Diagnostics Tech Support window indicate?

```
Fri Nov 16 11:33:33 2001] [error] [client 172.20.9.52] File does not exist:
/usr/local/ apache/htdocs/scripts/..%2f../winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/MSADC/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/c/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/d/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/..%5c../winnt/system32/cmd.exe
```



- A. These errors might indicate a virus-infected client searching for the next system to infect. Some viruses look for vulnerabilities in a webserver running on port 80. Several remedies exist, including:
- Disinfecting clients (note their IP addresses).
  - Implementing access control lists (ACLs) to prevent access to the NAM.
  - Running the NAM webserver on a different port (because many virus attacks target only port 80.)

## Hostname Resolution Issues

Q. Why did my importing of a remote hosts file fail when I used the `ip hosts add ...` command?

A. This might happen because:

- The hosts file is not formatted correctly. For more information see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note*: [http://www.cisco.com/en/US/docs/net\\_mgmt/network\\_analysis\\_module\\_software/4.0/switch/configuration/guide/swconfig.html](http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html)
- The local hosts file is limited to 1000 entries. Verify that you are not trying to add more than 1000 entries. You can use the NAM CLI command **show tech-support**, then look for a line that reads:  
Total number of entries in hosts files: *nn*



### Tip

- To review the entries configured in the file, use the **show hosts** command.
- If you need to add more than 1000 hosts, use DNS or select the 1000 most critical hosts for local name resolution.

Q. Why are there long delays during remote Telnet sessions to the NAM?

A. The problem might be with the DNS server address. The DNS server address must be set to the IP address of an operational DNS server. When the NAM cannot reach the server because of an incorrect address, inability to connect to the server, or a non-operational server, you might experience long delays.

To resolve this problem, change the DNS server to the IP address of a working server, or eliminate the server:

- 
- Step 1** Choose **Admin > System**.
- Step 2** In the contents, click **Network Parameters**.
- Step 3** Change the parameters as needed.
- Step 4** Click **Apply**.
- 

You can also use the NAM CLI command `ip nameserver nameserver_addr` (to select a specific nameserver) or eliminate the nameserver completely with the command `ip nameserver disable`.

- Q. Why are there long delays while waiting for diagnostic tech support output?
- A. The problem might be with the DNS server address. To resolve this problem, change the DNS server to the IP address of a working server, or eliminate the server:

- 
- Step 1** Choose **Admin > System**.
- Step 2** In the contents, click **Network Parameters**.
- Step 3** Change the parameters as needed.
- Step 4** Click **Apply**.
- 

You can also use the NAM CLI command `ip nameserver nameserver_addr` (to select a specific nameserver) or eliminate the nameserver completely with the command `ip nameserver disable`.

- Q. Are there restrictions on adding or deleting certain IP addresses to my local hosts file using the `ip hosts add ...` and `ip hosts delete ...` commands?
- A. Yes. Do not add or delete host entries using the NAM IP address or IP addresses beginning with 127.x.x.x.

## Data Mismatch Issues

- Q. I clicked the Monitor tab, then **Hosts** or **Conversations**. The Network Host Table displayed. When I click a hostname, the data in the popup chart and tables sometimes do not match. Why does this happen?
- A. The sources of the data used for the chart and tables in the detail popups are independent and might age out at different intervals.

## HTTPS/Security Certificate Issues

- Q. Why do I see warning messages that my certificate has expired when I point my web browser to the NAM using https?
- A. This happens because your certificate has expired. To resolve this, you can either:
- Generate a self-signed certificate.
  - Generate a certificate-signing request. Send the request to the certification authority, then install the certificate you receive.
  - To do either of these, you use NAM CLI commands. For more information, see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note*:  
[http://www.cisco.com/en/US/docs/net\\_mgmt/network\\_analysis\\_module\\_software/4.0/switch/configuration/guide/swconfig.html](http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html)
- Q. What do I do when I see warning messages in my web browser that the name on the security certificate does not match the name of the site?

- A. To resolve this, you can either:
- Generate a self-signed certificate—When doing so, enter **no** when asked whether to re-use the certificate-signing request. This generates a new certificate-signing request, then a self-signed certificate. Enter your hostname when prompted for the Common Name.
  - Generate a certificate-signing request—Enter your hostname when prompted for the Common Name. Send the request to the certification authority, then install the certificate you receive.
  - To do either of these, you use NAM CLI commands. For more information, see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note*:  
[http://www.cisco.com/en/US/docs/net\\_mgmt/network\\_analysis\\_module\\_software/4.0/switch/configuration/guide/swconfig.html](http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html)
- If you have done the above and still see the warning message, try to enter the full host name of the NAM in the browser address window. For example, if the full host name of the NAM is nam1.cisco.com, enter https://nam1.cisco.com instead of https://nam1.
- Q. What do I do when I see warning messages in my browser that the security certificate was issued by a company I have not chosen to trust?
- A. View the certificate to determine whether you want to trust the certifying authority. You may see this message if the HTTPS certificate of the NAM is the factory (test) certificate, or a self-signed certificate. Click **Proceed**.

## SNMP Issues

- Q. Does the NAM support SNMPv3?
- A. The NAM supports only SNMPv1 and SNMPv2c, including both external SNMP managers interacting with the NAM and the NAM interacting with the switch for mini-RMON port statistics and switch-based alarms.
- Q. When I click **Test** on the Router Parameters dialog box, a window displays that SNMP read from the router failed.
- A. You must verify that the SNMP read-write community strings entered are the same SNMP read-write community strings defined for the *router*. If the community strings are correct, and the test fails, verify that the router has IP permit list enabled.

### For Switches Running Catalyst OS only

---

**Step 1** Log into the switch in enable mode

**Step 2** Enter **show IP permit**.

If IP permit list is enabled, verify that the internal address of the NAM is added to the list.



**Note** To view the NAM internal IP address from Traffic Analyzer, click **Test** from the Switch Community String dialog box under **Setup > Chassis Parameters**. The Switch Community String Test dialog box is displayed.

---

Enter **set IP permit** *NAM ip address* **SNMP**.

---

Q. Must I enable the NAM SNMP agent when I use the NAM Traffic Analyzer?

A. No. You only need the SNMP agent to support SNMP communication from external SNMP managers. To disable SNMP on the NAM:

---

**Step 1** Choose **Admin > System**.

**Step 2** In the contents, click **NAM SNMP**.

**Step 3** In the NAM Community Strings pane, select and delete all NAM community strings.

---

Q. When I set the timing buckets and report interval of an ART collection using SNMP, why do the settings of other ART collections also change?

A. NAM supports a global setting for ART timing buckets and report interval. So any settings you make using SNMP will apply to all ART collections. See [Setting Up Response Time Configuration, page 3-61](#), for information about using the GUI to configure ART timing and report interval.



**Note** The method you use last overrides previous settings. So if you change the settings using SNMP, those settings will override the settings made using the GUI, and vice versa.

---

## Protocol Support Issues

Q. Why do some protocols (such as sunrpc) sometimes appear twice in the application statistics windows?

A. Only the highest-level protocols are displayed. In some cases, a higher-level protocol might run on more than one lower layer protocol. For example, sunrpc might run on TCP and UDP. The NAM Traffic Analyzer would display two line items so you can differentiate between the two. Hold your mouse over the protocol and a small popup displays the full protocol stack involved.

Q. When I click the Monitor tab, then **DiffServ**, then **Application Stats**, I sometimes see a protocol such as http with a larger number of packets (or bytes) per second than the lower-layer protocol TCP. Why does this happen?

A. The differentiated services monitoring (DiffServ) statistics counts the packets only in the highest-level protocol possible. Therefore, a ...tcp.http packet counts as only an http packet. Packets classified as TCP mean that was the highest level the NAM could process. This might happen because it was an unrecognized TCP port or a state-based protocol in which the NAM did not detect a preceding packet to classify it.

Q. Where can I find a list of all protocols that the NAM supports?

A. A list of all protocols the NAM monitors is displayed in the Protocol Directory table under **Setup > Monitor**. You can also retrieve and modify the protocols using an SNMP tool.

Q. If I do not see a protocol listed on the **Setup > Capture > Settings** page, does that mean the NAM does not recognize that protocol, and it therefore is not displayed in the Monitor displays?

- A. If the Protocols check box is selected and All is selected from the Protocols drop-down list, then all of the protocols the NAM can monitor will be listed in the selection box. You can use the Protocols drop-down list to select a more appropriate subset of protocols for your given environment.
- Q. Are all of the protocols that the NAM tracks for Monitor displays (such as Monitor Apps, Monitor Overview) available for decode in the Capture Decode dialog box?
- A. No. Decodes are available only for some of the protocols supported by the NAM. For additional decodes, you might consider using a third-party application. You can use the Capture Download feature to export your trace file to the third-party application.
- Q. What does the protocol entry labeled "others" signify on some of the NAM web windows?
- A. The protocol entry labeled "others" represents the sum of traffic for which the NAM was unable to identify the topmost application layer in the packet data. For example, these can be unrecognized TCP/UDP ports or dynamically assigned ports for which the NAM was not able to analyze the setup transactions. One way to gain more information is to use the capture capability of the NAM to capture packet data, then look for packets that cannot be fully decoded in the **Capture > Decode** window.

## Voice Monitoring Issues

- Q. Why are some columns blank in the detail windows that display VoIP phones and phone calls?
- A. The amount of detail the NAM can provide for IP telephony traffic depends on the physical placement of the NAM relative to the IP phones, Call Managers, H.323 gatekeepers, and MGCP gateways. It also depends on what subset of traffic in the switch or router is being spanned or copied to the NAM. The NAM sometimes cannot directly observe the call setup transactions for phones on remote networks. In general, all detailed phone and call information that the NAM can observe is populated into the fields of the web displays.
- Q. Why do some displays show that the phone protocol is SCCP (H.323 or MGCP) when it is really something else?
- A. The protocol associated with a phone denotes the protocol by which the NAM initially *learned* about the phone, not necessarily the protocol used by that phone.  
  
For example, if an SCCP phone calls an H.323 phone, and the NAM directly observes only the SCCP side of the call setup, it associates the SCCP protocol with both sides of the call because that is how the NAM learned about *both* phones.
- Q. Why don't I see quality statistics (jitter, packet loss) for my SCCP phone calls?
- A. For the NAM to report jitter and packet loss statistics for SCCP calls, Call Maintenance Records and Call Detail Records must be enabled on the Cisco Call Managers.  
  
To turn on CMR and CDR in Cisco Call Manager 3.1, follow these steps:

- 
- Step 1** Go to the Cisco CallManager Administration window.
  - Step 2** Choose **Service > Service Parameters**.
  - Step 3** Choose the IP address of your Cisco CallManager server.
  - Step 4** Click the **Next** button.
  - Step 5** Choose the Cisco CallManager service.

- Step 6** Choose **True** in the Parameter Value field for Call Diagnostics Enabled.
- Step 7** Scroll down to the CdrEnabled service parameter and choose **True** for the value.
- Step 8** Click the **Update** button.
- Step 9** Call detail records start logging immediately.



**Note** This procedure is only valid on CallManager version 3.1, but other versions have a very similar process.

- Q. What is the MGCP Endpoint in the **Monitor > Voice > Known Phones** window?
- A. An MGCP Endpoint entry represents a MGCP gateway trunk port that one or more IP phones use to communicate with phones in the PSTN.
- Q. Why do some MGCP Call Detail tables have Q.931 detail information?
- A. When Cisco Call Manager and Cisco MGCP gateway traffic is copied to the NAM, the phone number and phone alias information for the MGCP calls might be obtained from Q.931 traffic. When this happens, the MGCP Call Detail table will have separated Q.931 table above it with detail information.

## WAAS Application Response Time Issues

- Q. Why is there no data in the response time monitor screens?
- A. Response Time calculation requires that NAM sees traffic in both directions: from clients to servers and vice versa. If NAM sees traffic in one direction only, it will not be able to calculate and monitor response time. Check you SPAN configuration to make sure that NAM receives traffic in both directions. Also check if there is asymmetric routing in the network, in which returning traffic may follow a different path from originating traffic.
- Q. Why does the WAAS device status remain *Inactive*?
- A. Use the following WAAS CLI commands to enable the WAAS device to export flow data to the NAM for monitoring.

**flow monitor tcpstat-v1 host <NAM IP address>**

**enable**

- Q. Why is there no data for the WAAS data source?  
or  
Why does the WAAS device status remain *Pending* and not *Active*?
- A. Go to **Setup > Data Sources > WAAS > Monitored Servers** and make sure that you specify the correct application servers to be monitored (for example. web and FTP servers).



**Note** The monitored servers should be among the servers whose traffic is being optimized by WAAS.

Use the following WAAS CLI command to verify that you have configured the correct monitored servers:

**show statistics flow filters**

```

Number of Filters: 7
 Status: Enabled
 Capture Mode: FILTER

Flags:
CSN: Client-Side Non-Optimized (Edge), SSN: Server-Side Optimized (Edge)
CSO: Client-Side Optimized (Core), SSN: Server-Side Non-Optimized (Core)
PT: Pass Through (Edge/Core/Intermediate), IC: Internal Client

```

| Server         | Flow Hits | Flags   |
|----------------|-----------|---------|
| 172.20.107.123 | 120       | CSO SSN |
| 1.2.3.4        | 0         | CSO SSN |
| 10.96.1.2      | 0         | CSO SSN |
| 10.31.10.1     | 0         | CSO SSN |
| 10.31.10.2     | 0         | CSO SSN |

If the WAAS CLI command **show statistics flow filters** output shows **zero flow hits** for the servers, these servers have no traffic being optimized, and the WAAS device has no data to export to the NAM to be monitored. In this case, check your WAAS configuration to determine which servers are being optimized, and configure the NAM to monitor these servers.

Finally, make sure you configure the correct data sources for the WAAS devices. Typically, you should configure the Client data sources for wide-area edge (WAE) edge devices and configure Server and Server WAN data sources for WAE core devices. See the section [Configuring WAAS Data Sources, page 3-38](#), for more information.

For more information about WAAS and configuring the WAAS components, see the document:

[Cisco Wide Area Application Services Configuration Guide, OL-16376-01](#)

[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/waas/v4019/configuration/guide/waas4cfg.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html)







## APPENDIX B

# Supported MIB Objects

---

The NAM supports all of the following MIB groups:

- RMON
- RMON2
- DSMON
- High Capacity RMON—except the mediaIndependentGroup.
- SMON
- Application Response Time (ART) MIB

## Supported MIBs

[Table B-1](#) lists the RMON and RMON2 MIB objects supported by the supervisor engine and the NAM. The supervisor engine implements some objects from the RMON MIBs as specified in [Table B-1](#). The supervisor engine RMON implementation is completely independent of the NAM implementation, and no MIB objects are shared.

To collect etherStats from a physical interface on the switch, configure the etherStatTable on the supervisor engine instead of on the NAM. The etherStats are collected accurately on multiple physical interfaces simultaneously.

If you are interested in the etherStats for a specific VLAN, configure the etherStatsTable on the NAM. For the data source, use the ifIndex corresponding to that VLAN.

Any alarmVariable configured on the supervisor engine must reference a MIB object on the supervisor engine. An alarmVariable configured on the NAM must reference a MIB object on the NAM.



### Note

---

You cannot configure an alarmVariable on the NAM that references a MIB object on the supervisor engine or configure an alarmVariable on the supervisor engine that references a MIB object on the NAM.

---

**Table B-1 Supervisor Engine Module and NAM RMON Support**

| Module            | Object Identifier (OID) and Description                                                                                                                                                                                               | Source                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Supervisor Engine | ...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)<br>...mib-2(1).rmon(16).statistics(1).tokenRingMLStatsTable(2)...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)                                                        | RFC 2819 (RMON-MIB)<br>RFC 1513<br>(TOKEN-RING-RMON MIB)<br>RFC 1513<br>(TOKEN-RING-RMON MIB)                        |
|                   | Counters for packets, octets, broadcasts, errors, etc.                                                                                                                                                                                |                                                                                                                      |
| Supervisor Engine | ...mib-2(1).rmon(16).history(2).historyControlTable(1)<br>...mib-2(1).rmon(16).history(2).etherHistoryTable(2)<br>...mib-2(1).rmon(16).history(2).tokenRingMLHistoryTable(3)...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4) | RFC 2819 (RMON-MIB)<br>RFC 2819 (RMON-MIB)<br>RFC 1513<br>(TOKEN-RING-RMON MIB)<br>RFC 1513<br>(TOKEN-RING-RMON MIB) |
|                   | Periodically samples and saves statistics group counters for later retrieval.                                                                                                                                                         |                                                                                                                      |
| Supervisor Engine | ...mib-2(1).rmon(16).alarm(3)                                                                                                                                                                                                         | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | A threshold that can be set on critical RMON variables for network management.                                                                                                                                                        |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).alarm(3)                                                                                                                                                                                                         | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | A threshold that can be set on critical RMON variables for network management.                                                                                                                                                        |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).hosts(4)                                                                                                                                                                                                         | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | Maintains statistics on each host device on the segment or port.                                                                                                                                                                      |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).hostTopN(5)                                                                                                                                                                                                      | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | A user-defined subset report of the Hosts group, sorted by a statistical counter.                                                                                                                                                     |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)                                                                                                                                                                                 | RFC 2819 (RMON-MIB)                                                                                                  |
| Network Analysis  | ...mib-2(1).rmon(16).matrix(6)                                                                                                                                                                                                        | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | Maintains conversation statistics between hosts on a network.                                                                                                                                                                         |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).filter(7)                                                                                                                                                                                                        | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | A filter engine that generates a packet stream from frames that match a specified pattern.                                                                                                                                            |                                                                                                                      |
| Network Analysis  | ...mib-2(1).rmon(16).capture(8)                                                                                                                                                                                                       | RFC 2819 (RMON-MIB)                                                                                                  |
|                   | Manages buffers for packets captured by the Filter group for uploading to the management console.                                                                                                                                     |                                                                                                                      |

**Table B-1 Supervisor Engine Module and NAM RMON Support (continued)**

| Module            | Object Identifier (OID) and Description                                                       | Source                         |
|-------------------|-----------------------------------------------------------------------------------------------|--------------------------------|
| Supervisor Engine | ...mib-2(1).rmon(16).event(9)                                                                 | RFC 2819 (RMON-MIB)            |
|                   | Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.          |                                |
| Network Analysis  | ...mib-2(1).rmon(16).event(9)                                                                 | RFC 2819 (RMON-MIB)            |
|                   | Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.          |                                |
| Supervisor Engine | ...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1)                                 | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2)                                        | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3)                                   | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4)                           | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5)                                  | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)                                 | RFC 1513 (TOKEN-RING-RMON MIB) |
|                   | Aggregates detailed Token Ring statistics.                                                    |                                |
| Network Analysis  | ...mib-2(1).rmon(16).protocolDir(11)                                                          | RFC 2021 (RMON2-MIB)           |
|                   | A table of protocols for which the Network Analysis Module monitors and maintains statistics. |                                |
| Network Analysis  | ...mib-2(1).rmon(16).protocolDist(12)                                                         | RFC 2021 (RMON2-MIB)           |
|                   | A table of statistics for each protocol in protocolDir(11).                                   |                                |
| Network Analysis  | ...mib-2(1).rmon(16).addressMap(13)                                                           | RFC 2021 (RMON2-MIB)           |
|                   | List of MAC-to-network-layer address bindings.                                                |                                |
| Network Analysis  | ...mib-2(1).rmon(16).nlHost(14)                                                               | RFC 2021 (RMON2-MIB)           |
|                   | Statistics for each network layer address.                                                    |                                |
| Network Analysis  | ...mib-2(1).rmon(16).nlMatrix(15)                                                             | RFC 2021 (RMON2-MIB)           |
|                   | Traffic statistics for pairs of network layer addresses.                                      |                                |
| Network Analysis  | ...mib-2(1).rmon(16).alHost(16)                                                               | RFC 2021 (RMON2-MIB)           |
|                   | Statistics by application layer protocol for each network address.                            |                                |
| Network Analysis  | ...mib-2(1).rmon(16).alMatrix(17)                                                             | RFC 2021 (RMON2-MIB)           |
|                   | Traffic statistics by application layer protocol for pairs of network layer addresses.        |                                |

**Table B-1 Supervisor Engine Module and NAM RMON Support (continued)**

| Module            | Object Identifier (OID) and Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Source                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Network Analysis  | ...mib-2(1).rmon(16).usrHistory(18)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | RFC 2021 (RMON2-MIB)            |
|                   | Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                 |
| Supervisor Engine | ...mib-2(1).rmon(16).probeConfig(19).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | RFC 2021 (RMON2-MIB)            |
|                   | Displays a list of agent capabilities and configurations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                 |
| Network Analysis  | ...mib-2(1).rmon(16).switchRMON(22).smonMIB Objects(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | RFC 2613 (SMON-MIB)             |
|                   | dataSourceCaps(1).dataSourceCapsTable(1).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                 |
|                   | Maps physical entities and VLANs to ifEntries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                 |
| Network Analysis  | ...mib-2(1).rmon(16).switchRMON(22).smonMIB Objects(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | RFC 2613 (SMON-MIB)             |
|                   | smonStats(2).smonVlanStatsControlTable(1).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                 |
|                   | Traffic statistics by VLAN ID number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                 |
| Network Analysis  | ...mib-2(1).rmon(16).switchRMON(22).smonMIB Objects(1).smonStats(2).smonPrioStatsControlTable(3)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | RFC 2613 (SMON-MIB)             |
|                   | .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                 |
|                   | Traffic statistics by 802.1p user priority value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                 |
| Network Analysis  | ...frontier(141).mibdoc2(2).netscout2(1).art(5).art ControlTable(2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | draft-warth-rmon2-artmib-01.txt |
|                   | Application response time statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | (ART-MIB)                       |
| Network Analysis  | ...mib-2(1).rmon(16).mediaIndependentStats(21)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | RFC 3273 (HC-RMON-MIB)          |
|                   | Counters for packets, octets, broadcasts, errors, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                 |
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonMaxAggGroups(1)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggControlLocked(2)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggControlChanges(3)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggControlLastChangeTime(4)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggControlTable(5)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggProfileTable(6)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggGroupTable(7) | RFC 3287 (DSMON-MIB)            |
|                   | Aggregation or profile control variables and tables                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                 |

**Table B-1 Supervisor Engine Module and NAM RMON Support (continued)**

| Module            | Object Identifier (OID) and Description                                                                                                                                                                                                                                                                                                                                                                                   | Source                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2).dsmonStatsControlTable(1)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2).dsmonStatsTable(2)                                                                                                                                                                                                                                                             | RFC 3287 (DSMON-MIB)             |
|                   | Per-datasource statistics collection tables                                                                                                                                                                                                                                                                                                                                                                               |                                  |
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistCtlTable(1)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistStatsTable(2)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNCtlTable(3)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTopNTable(4)                                                                                       | RFC 3287 (DSMON-MIB)             |
|                   | Per-protocol statistics collection tables                                                                                                                                                                                                                                                                                                                                                                                 |                                  |
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostCtlTable(1)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTable(2)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTopNCtlTable(3)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4).dsmonHostTopNTable(4)                                                                                                    | RFC 3287 (DSMON-MIB)             |
|                   | Per-host statistics collection tables                                                                                                                                                                                                                                                                                                                                                                                     |                                  |
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5).dsmonCapabilities(1)                                                                                                                                                                                                                                                                                                                                                | RFC 3287 (DSMON-MIB)             |
|                   | DSMON capabilities variable                                                                                                                                                                                                                                                                                                                                                                                               |                                  |
|                   | rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixCtlTable(1)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixSDTable(2)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixDSTable(3)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNCtlTable(4)<br>rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNTable(5) | RFC 3287 (DSMON-MIB)             |
|                   | Matrix statistics collection tables                                                                                                                                                                                                                                                                                                                                                                                       |                                  |
| Supervisor Engine | ...ciscoMgmt(9).ciscoNbarProtocolDiscoveryMIB(244).cnpdMIBObjects(1).cnpdStatus(1)                                                                                                                                                                                                                                                                                                                                        | CISCO-NBAR-PROTOCOL-DISCOVER-MIB |
|                   | Indicates per interface whether nbar protocol discovery is enabled.                                                                                                                                                                                                                                                                                                                                                       |                                  |

**Table B-1 Supervisor Engine Module and NAM RMON Support (continued)**

| Module            | Object Identifier (OID) and Description                                                                           | Source                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Supervisor Engine | ...ciscoMgmt(9).ciscoNbarProtocolDiscoveryMIB(244).cnpdMIBObjects(1).cnpdAllStats(2)                              | CISCO-NBAR-PROTOCOL-DISCOVER-MIB |
|                   | Statistics per interface for nbar protocol discovery.                                                             |                                  |
| Network Analysis  | ...mib-2(1).entityMIB(47).entityMIBObjects(1).entityPhysical(1).entPhysicalTable(1)                               | RFC 2737 (ENTITY-MIB)            |
|                   | Entity physical description.                                                                                      |                                  |
| Network Analysis  | ...mib-2(1).entityMIB(47).entityMIBObjects(1).entityGeneral(4)                                                    | RFC 2737 (ENTITY-MIB)            |
| Network Analysis  | ...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpInterface(1)                                             | CISCO-CDP-MIB                    |
| Network Analysis  | ...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpCache(1)                                                 | CISCO-CDP-MIB                    |
| Network Analysis  | ...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpGlobal(3)                                                | CISCO-CDP-MIB                    |
| Supervisor Engine | ...ciscoMgmt(9).ciscoProcessMIB(109).ciscoProcessMIBObjects(1).cpmCPU(1).cpmCPUTotalTable(10).cpmCPUTotalEntry(1) | CISCO-PROCESS-MIB                |
|                   | CPU Statistics                                                                                                    |                                  |
| Supervisor Engine | ...cisco(9).workgroup(5).ciscoStackMib(1).systemGrp(1).sysTrafficPeak(19)                                         | CISCO-STACK-MIB                  |
|                   | Peak traffic meter value                                                                                          |                                  |
| Supervisor Engine | ..cisco(9).workgroup(5).ciscoStackMib(1).systemGrp(1).sysTrafficPeakTime(20)                                      | CISCO-STACK-MIB                  |
|                   | Time since last peak traffic meter value occurred.                                                                |                                  |
| Supervisor Engine | ...ciscoMgmt(9).ciscoMemoryPoolMIB(48).ciscoMemoryPoolEntry(1)                                                    | CISCO-MEMORY-POOL-MIB            |
|                   | Free and Largest block of contiguous memory                                                                       |                                  |
| Supervisor Engine | ...mgmt(20).mib-2(1).entityMIB(47).entityMIBObjects(1).entityPhysical(1)                                          | ENTITY-MIB                       |
|                   | Text description of physical entity.                                                                              |                                  |
| Supervisor Engine | ...ciscoMgmt(9).ciscoEnvMonMib(13).ciscoEnvMonObjects(10)                                                         | CISCO-ENVMON-MIB                 |
|                   | Power, Temperature and Fan Status                                                                                 |                                  |

**Table B-1 Supervisor Engine Module and NAM RMON Support (continued)**

| Module            | Object Identifier (OID) and Description                                                                                                           | Source                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Supervisor Engine | ...cisco(9).workgroup(5).ciscoStackMIB(1).ciscoStatckMIBConformance(31).ciscoStaticMIBGroups(20.chassisGroup(3)                                   | CISCO-STACK-MIB          |
|                   | Collection of objects providing information about the chassis of the device.                                                                      |                          |
| Supervisor Engine | ...ciscoMgmt(9).ciscoCat6kCrossbarMIB(217).ciscoCat6kXbarMIBObjects(1)                                                                            | CISCO-CAT6K-CROSSBAR-MIB |
|                   | Crossbar statistics.                                                                                                                              |                          |
| Supervisor Engine | ...ciscoMgmt(9).ciscoMIBObjects(1).cseMIBObjects(1).cseTcamUsage(9).cseTcamUsageTable(1).cseTcamUsageEntry(1)                                     | CISCO-SWITCH-ENGINE      |
|                   | Description of the resource type, total amount of TCAM allocated for that type as well as the amount of allocated resource that has been used up. |                          |







## INDEX

---

### A

- accounts in NAM Traffic Manager, managing [1-6](#)
- address filters, using to capture settings [6-8](#)
- administration (see system administration) [2-1](#)
- Alarm
  - EMail addresses [3-94](#)
- Alarm events
  - last sent [3-82](#)
- Alarm events table [3-82](#)
- alarms, viewing [7-1](#)
  - alarm logs, overview [7-1](#)
  - NAM log, viewing [7-2](#)
  - switch log, viewing [7-2](#)
- alarm thresholds, setting [3-81](#)
  - NAM MIB thresholds [3-84](#)
    - deleting [3-87](#)
    - editing [3-87](#)
  - switch thresholds [3-90](#)
    - creating [3-91](#)
    - deleting [3-93](#)
    - editing [3-92](#)
- syslog, setting up [3-90](#)
- All button [3-7](#)
- application data, viewing [4-14](#)
  - application protocols, capturing data for [4-11, 4-16](#)
    - detail
      - by protocol [4-10, 4-15](#)
      - cumulative [4-14](#)
    - packets and bytes collected
      - by protocol [4-9, 4-14](#)
      - cumulative [4-13, 4-17](#)
  - real-time data in graphical format [4-11, 4-16](#)

- reports

- Application report, creating [5-4](#)
  - Application table reports [4-11, 4-16](#)

- tables and charts useful in

- Applications Cumulative Data table [4-13, 4-17](#)
  - Applications Current Rates table [4-9, 4-14](#)
  - TopN Applications chart [4-11, 4-16](#)

- Application Response Time report

- creating [5-4](#)

- Applications Cumulative Data table, using [4-13, 4-17](#)

- details [4-14](#)

- packets and bytes collected [4-13, 4-17](#)

- Applications Current Rates table, using [4-9, 4-14](#)

- application protocol data, capturing [4-11, 4-16](#)

- details for specific protocol, viewing [4-10, 4-15](#)

- real-time data, viewing [4-11, 4-16](#)

- reports [4-11, 4-16](#)

- ART [4-72, 4-77, 4-88](#)

- Audit trail [2-26](#)

---

### B

- browser response time and display, troubleshooting [A-13](#)

---

### C

- Capture Analysis

- drill down [6-23](#)

- Capture buffer

- maximum buffer size [6-5](#)

- Capture data

- storage [2-19](#)

- Capture Files

- Analyze button [6-23](#)
- capturing data [1-10, 6-1](#)
  - application protocols [4-11, 4-16](#)
  - capture buffer
    - displaying data in [1-8](#)
    - downloading to a file [6-22](#)
  - capture settings, configuring [6-3](#)
    - using a custom filter [6-10](#)
    - using an address filter [6-8](#)
    - using a protocol filter [6-9](#)
  - client/server response time [4-86, 4-90](#)
  - custom capture filters, setting up [6-27](#)
    - creating [6-27](#)
    - deleting [6-30](#)
    - editing [6-30](#)
  - custom decode filters, setting up [6-31](#)
    - creating [6-31](#)
    - deleting [6-35](#)
    - editing [6-35](#)
  - host conversations [4-44](#)
  - network hosts current rates [4-36](#)
  - packet decode information, viewing [6-11](#)
  - protocol decode information, viewing [6-14](#)
  - response time [4-86, 4-90](#)
  - server detail [4-82](#)
  - server response time [4-82](#)
- cautions
  - regarding
    - local database web users, deleting all [A-3](#)
    - NAM community strings, deleting [2-15](#)
    - switch string and read-write community string matching [3-33](#)
- Client/Server Response Time table, using [4-84](#)
  - data, capturing [4-86, 4-90](#)
  - detail [4-86, 4-90](#)
  - reports [4-86, 4-90](#)
- Client/Server Response Time Top N chart, using [4-87](#)
- collection (see data collection, setting up) [1-6](#)
- collections
  - creating [1-11](#)
  - common navigation and control elements (table) [1-4](#)
  - community switch strings, setting and viewing [3-33](#)
  - configuring NAM Traffic Analyzer [3-1](#)
    - community switch strings, setting and viewing [3-33](#)
  - data collection, setting up [3-54](#)
    - core data, collecting [3-54](#)
    - DiffServe profile, setting up [3-65](#)
    - DSMON data, monitoring [3-64](#)
    - response time data, monitoring [3-60](#)
    - voice data, collecting [3-57](#)
  - data sources, setting up [3-10](#)
  - router parameters, viewing [3-8](#)
  - traffic, directing for spanning [3-10](#)
    - creating a SPAN session [3-14](#)
    - custom NetFlow data sources, creating [3-28](#)
    - deleting a SPAN session [3-16](#)
    - editing a SPAN session [3-15](#)
    - listening mode, using [3-30](#)
    - NDE collection types (table) [3-12](#)
    - NetFlow, configuring on devices [3-22](#)
    - NetFlow devices, managing [3-26](#)
    - NetFlow interfaces, understanding [3-21](#)
    - NetFlow records, understanding [3-21](#)
    - SPAN sources (table) [3-12](#)
    - traffic directing methods (table) [3-11](#)
    - VACL, configuring on LAN VLANs [3-25](#)
    - VACL, configuring on WAN interfaces [3-24](#)
- Consecutive Packets Loss threshold [3-59](#)
- Console
  - external reporting [2-25](#)
- Continuous capture [6-5, 6-18](#)
- conversations data, viewing [4-42](#)
  - cumulative data for each host conversation [4-46](#)
  - packets and bytes collected for MAC station conversations [4-49](#)
  - packets and bytes for each host conversation [4-43](#)
    - capturing data on [4-44](#)
    - detail [4-44](#)

- real-time traffic statistics in graphical format [4-44](#)
    - reports [4-45](#)
  - packets and bytes for top n host conversations [4-45](#)
  - tables and charts useful in
    - MAC Conversations Top N chart [4-49](#)
    - MAC Station Conversations Cumulative Data table [4-51](#)
    - Network Host Conversations Cumulative Data table [4-46](#)
    - Network Host Conversations Top N chart [4-45](#)
    - Viewing the Network Host Conversations Current Rates table [4-43](#)
  - core data, collecting [3-54](#)
  - Core monitoring
    - router [3-55](#)
    - switch [3-55](#)
  - Correlated data sources [4-92](#)
  - CPU usage [A-2](#)
    - percentage [A-2](#)
  - creating
    - basic reports [5-4](#)
    - custom capture filters [6-27](#)
    - custom decode filters [6-31](#)
    - custom NetFlow data sources [3-28](#)
      - data source, deleting [3-30](#)
      - data source information, verifying [3-30](#)
      - data sources, editing [3-30](#)
      - interfaces, selecting [3-29](#)
      - NetFlow device, selecting [3-29](#)
    - custom reports [5-26](#)
    - NAM Traffic Analyzer accounts [1-6](#)
    - NAM traps [3-93](#)
    - NetFlow devices [3-26](#)
    - protocol [3-70](#)
    - SPAN sessions [3-14](#)
    - switch thresholds [3-91](#)
  - Custom capture filter
    - creating [6-27](#)
  - custom capture filters
    - managing
      - creating [6-27](#)
      - deleting [6-30](#)
      - editing [6-30](#)
      - setting up [6-27](#)
    - using [6-10](#)
  - Custom captures [6-27](#)
  - custom decode filters, managing
    - creating [6-31](#)
    - deleting [6-35](#)
    - editing [6-35](#)
    - setting up [6-31](#)
  - Custom filters [6-27](#)
  - Custom report
    - editing [5-27](#)
  - Custom reports [5-25](#)
    - creating a new folder [5-26](#)
    - deleting [5-27](#)
    - moving to a different folder [5-27](#)
    - viewing [5-27](#)
- 
- ## D
- data collection
    - overview [4-2](#)
    - setting up [3-54](#)
      - core data collection [3-54](#)
      - DiffServe profile data [3-65](#)
      - DSMON data [3-64](#)
      - response time data [3-60](#)
      - voice data [3-57](#)
  - Data Expired [5-23](#)
  - data export [1-10](#)
  - data mismatches, troubleshooting [A-16](#)
  - Data Pending [5-23](#)
  - data-port collection
    - creating [1-11](#)
  - Data source
    - core monitoring [3-55](#)

- persistence [4-9](#)
- datasources
  - maximum supported [3-34](#)
- data sources, overview [4-2](#)
  - multiple collections, configuring [4-2](#)
  - NDE flow-masks, and V8 aggregation caches [4-5](#)
  - protocol autodiscovery [4-4](#)
- data sources, setting up [3-10](#)
- Data type
  - response time report parameters [5-14](#)
- deleting
  - basic reports [5-25](#)
  - custom capture filters [6-30](#)
  - custom decode filters [6-35](#)
  - custom NetFlow data sources [3-30](#)
  - custom reports [5-27](#)
  - DiffServe profiles [3-66, 3-76](#)
  - NAM MIB thresholds [3-87](#)
  - NAM Traffic Analyzer accounts [1-6](#)
  - NAM traps [3-94](#)
  - NetFlow devices [3-27](#)
  - protocols [3-73](#)
  - SPAN sessions [3-16](#)
  - switch thresholds [3-93](#)
- diagnostic error messages (see troubleshooting) [A-14](#)
- diagnostics, generating [2-25](#)
  - configuration information, monitoring and capturing [2-27](#)
  - system alerts, capturing [2-28](#)
  - system alerts, viewing [2-25](#)
- Diagnostics Tech Support window (illustration) [2-29](#)
- Differentiated Services report
  - creating [5-4](#)
- DiffServ Application Statistics Cumulative Data table, using [4-64](#)
- DiffServ Application Statistics Current Rates table, using [4-61](#)
  - application conversation details [4-62](#)
  - real-time statistics in graphical format [4-62](#)
  - reports [4-63](#)
- DiffServ Application Statistics Top N chart, using [4-63](#)
- DiffServ data, viewing [4-57](#)
  - application conversation details [4-62](#)
  - host conversation detail [4-66](#)
  - real-time data for specific hosts [4-66](#)
  - real-time traffic for specific aggregation groups [4-59](#)
  - real-time traffic for specific application protocols [4-62](#)
  - reports
    - application statistics [4-63](#)
    - host statistics [4-67](#)
    - traffic statistics [4-59](#)
- tables and charts useful in
  - DiffServ Application Statistics Cumulative Data table [4-64](#)
  - DiffServ Application Statistics Current Rates table [4-61](#)
  - DiffServ Application Statistics Top N chart [4-63](#)
  - DiffServ Host Statistics Cumulative Data table [4-68](#)
  - DiffServ Host Statistics Current Rates table [4-65](#)
  - DiffServ Host Statistics Top N chart [4-67](#)
  - DiffServ Traffic Statistics Cumulative Data table [4-60](#)
  - DiffServ Traffic Statistics Current Rates table [4-58](#)
  - DiffServ Traffic Top N chart [4-59](#)
- DiffServe profile, managing
  - creating [3-65, 3-75](#)
  - deleting [3-66, 3-76](#)
  - editing [3-66, 3-75](#)
  - setting up [3-65](#)
- DiffServ Host Statistics Cumulative Data table, using [4-68](#)
- DiffServ Host Statistics Current Rates table, using [4-65](#)
  - host conversation details [4-66](#)
  - real-time data in graphical format [4-66](#)
  - reports [4-67](#)
- DiffServ Host Statistics Top N chart, using [4-67](#)
- DiffServ Traffic Statistics Cumulative Data table, using [4-60](#)

- DiffServ Traffic Statistics Current Rates table, using [4-58](#)
- DiffServ Traffic Statistics table, using
  - real-time traffic statistics in graphical format [4-59](#)
  - reports [4-59](#)
- DiffServ Traffic Statistics Top N chart, using [4-59](#)
- directing traffic for spanning [3-10](#)
  - custom NetFlow data sources, creating [3-28](#)
    - data source, deleting [3-30](#)
    - data source, editing [3-30](#)
    - data sourcedeleting [3-30](#)
    - data source information, verifying [3-30](#)
    - interfaces, selecting [3-29](#)
    - NetFlow device, selecting [3-29](#)
  - listening mode, using [3-30](#)
  - methods (table) [3-11](#)
  - NDE collection types (table) [3-12](#)
  - NetFlow, configuring on devices [3-22](#)
    - devices running Catalyst OS [3-23](#)
    - devices running Cisco IOS [3-22](#)
    - devices supporting multi-layer switching cache [3-23](#)
    - devices supporting NDE export [3-24](#)
    - devices supporting NDE v8 aggregations [3-23](#)
    - devices supporting vi aggregations [3-23](#)
    - NAMs in a device slot [3-24](#)
  - NetFlow devices, managing [3-26](#)
    - creating [3-26](#)
    - deleting [3-27](#)
    - editing [3-27](#)
    - testing [3-27](#)
  - SPAN session
    - creating [3-14](#)
    - deleting [3-16](#)
    - editing [3-15](#)
  - SPAN sources (table) [3-12](#)
  - VACL, configuring on LAN VLANs [3-25](#)
  - VACL, configuring on WAN interfaces [3-24](#)
- displaying
  - alarms [1-9](#)

- capture buffer data [1-8](#)
- network traffic data [1-8](#)
- reports [1-8](#)

- Drill-Down button [6-23](#)

- DSMON data collection, setting up [3-64](#)

---

## E

- editing
  - custom capture filters [6-30](#)
  - custom decode filters [6-35](#)
  - custom reports [5-27](#)
  - DiffServe profiles [3-66, 3-75](#)
  - NAM MIB thresholds [3-87](#)
  - NAM Traffic Analyzer accounts [1-6](#)
  - NAM traps [3-94](#)
  - NetFlow devices [3-27](#)
  - protocols [3-72](#)
  - SPAN sessions [3-15](#)
  - switch thresholds [3-92](#)
- EMail alarms [3-94](#)
- Enabling
  - audit trail [3-96](#)
  - voice monitoring [3-57](#)
- Encapsulation [3-74](#)
- Encapsulation Configuration [3-74](#)
- Encapsulation configuration [3-74](#)
- Encapsulated Remote SPAN [1-11](#)
- error messages (see troubleshooting) [A-14](#)
- ERSPAN [3-53](#)
  - configuring as datasource [3-52](#)
  - encapsulated remote SPAN [1-11](#)
  - sending data directly to NAM [3-53](#)
  - SPAN [1-11](#)
- External reporting console [2-25](#)

---

**F**
**Filtering**

- audit trail [2-27](#)
- IP [6-20](#)
- IP and Payload Data [6-21](#)
- IP and TCP/UDP [6-20](#)
- IPv6 traffic [6-19](#)
- Payload data [6-21](#)
- VLAN [6-19](#)
- VLAN and IP [6-19](#)

Filter Response Time for all Data Sources by Monitored Servers [3-42](#)

folders, moving custom reports between [5-27](#)

---

**G**

generic routing encapsulation [1-11](#)

global preferences, setting [3-94](#)

GPRS (General Packet Radio Service) Tunneling Protocol [3-74](#)

**GRE**

- generic routing encapsulation [1-11](#)

GREIP [3-74](#)

GTP [3-74](#)

GUI for NAM Traffic Analyzer, navigating [1-2](#)

---

**H**

hardware, NAM installation, and

- Catalyst 6000 and 6500 series switches [1-1](#)
- Cisco 2600, 3660, and 3700 series routers [1-1](#)

Hardware assisted capture session [6-15](#)

Hardware filter [6-18](#)

**help**

- (see also troubleshooting) [A-1](#)
- diagnostics, generating for technical assistance [2-25](#)
  - configuration information, monitoring and capturing [2-27](#)

system alerts, capturing [2-28](#)

system alerts, viewing [2-25](#)

historical network traffic data, storing and retrieving [1-8](#)

host data, viewing [4-34](#)

cumulative data on each host [4-38](#)

cumulative MAC station data [4-41](#)

data for a specific host, capturing [4-36](#)

data on top n MAC stations [4-40](#)

detail [4-35](#)

Host Conversation report

creating [5-4](#)

network hosts table reports [4-37](#)

real-time statistics in graphical format [4-36](#)

tables and charts useful in

MAC Stations Current Rates table [4-39](#)

MAC Stations Top N chart [4-40](#)

Network Hosts Cumulative Data table [4-38](#)

Network Hosts Current Rates table [4-34](#)

Network Hosts Top N chart [4-37](#)

hostname resolution, troubleshooting [A-15](#)

HTTP/security certificates, troubleshooting [A-16](#)

---

**IGMP** [1-12](#)

image upgrades, troubleshooting [A-13](#)

Individual data sources [4-92](#)

interface data, viewing

detail [4-102](#)

Interface Stats Current Rates table, using [4-95, 4-111](#)

Interface Top N chart, using [4-99](#)

IPESP [3-74](#)

IP host name resolution, and slow response time, troubleshooting [3-95](#)

IPIP4 [3-74](#)

IP tunnel encapsulations [3-74](#)

---

**L**

Last Status [5-24](#)  
 listening mode (NAM), using [3-30](#)  
 Log  
     MPLS Import [3-52](#)  
 logins  
     troubleshooting [A-3](#)

---

**M**

MAC station conversations, monitoring  
     cumulative [4-51](#)  
     current rates [4-49](#)  
     top n [4-49](#)  
 MAC stations, monitoring data on  
     cumulative [4-41](#)  
     current rates [4-39](#)  
     top n [4-40](#)  
 management port  
     data source [1-11](#)  
 MGCP gateways, how represented [4-30](#)  
 Monitored servers filters [3-42](#)  
 Monitoring  
     Application response times [4-72, 4-77, 4-88](#)  
 monitoring  
     port traffic [1-12](#)  
     traffic [1-10](#)  
 monitoring data [4-1](#)  
     application [4-14](#)  
         packets and bytes for each application  
         protocol [4-9, 4-14](#)  
         real-time data in graphical format [4-11, 4-16](#)  
         reports [4-11, 4-16](#)  
     data collection, overview [4-2](#)  
     data sources, overview [4-2](#)  
         multiple collections, configuring [4-2](#)  
         NDE flow-masks, and V8 aggregation  
         caches [4-5](#)

    protocol autodiscovery [4-4](#)  
 DSMON [3-64](#)  
 host [4-34](#)  
     cumulative data on [4-38](#)  
     MAC stations [4-40](#)  
 Monitor Overview charts, viewing [4-6](#)  
 response time [3-60](#)  
     data collections, deleting [3-64](#)  
     data collections, editing [3-62](#)  
 voice [4-18](#)  
     active calls [4-32](#)  
     known phones [4-30](#)

Monitoring voice/video stream thresholds [3-88](#)  
 Monitor Overview charts, viewing [4-6](#)  
 MOS  
     codec [3-89](#)  
 MPLS Import log [3-52](#)  
 MPLS-tagged traffic [3-11](#)  
 MPLS traffic statistics [4-115](#)  
 Multiple WAAS segments  
     viewing response time [4-92](#)

---

**N**

NAM  
     community strings, working with [2-14](#)  
         creating [2-14](#)  
         deleting [2-15](#)  
     listening mode, using [3-30](#)  
     MIB alarm thresholds  
         deleting [3-87](#)  
         editing [3-87](#)  
         setting [3-84](#)  
     SNMP system groups, setting and viewing [2-13](#)  
     switch date/time synchronization, and,  
     troubleshooting [A-14](#)  
     system time, setting [2-16](#)  
         configuring with an NTP server [2-17](#)  
         synchronizing with switch or router [2-17](#)

- traps
    - creating [3-93](#)
    - deleting [3-94](#)
    - editing [3-94](#)
    - setting [3-93](#)
  - versions [3-10](#)
  - NAM-1 devices
    - default reports [5-3](#)
  - NAM-2 devices
    - default reports [5-3](#)
  - NAM appliances
    - default reports [5-4](#)
  - Nameservers, and slow response time, troubleshooting [3-95](#)
  - NAM RTP Stream Thresholds [3-59](#)
  - navigation and control elements [1-4](#)
  - NDE flow-masks, and V8 aggregation caches [4-5](#)
  - NetFlow [1-9](#)
    - configuring on devices [3-22](#)
      - Catalyst OS [3-23](#)
      - Cisco IOS [3-22](#)
      - multi-layer switching cache [3-23](#)
      - NAMs in a device slot [3-24](#)
      - NDE export [3-24](#)
      - NDE v8 aggregations [3-23](#)
    - data sources, managing
      - creating [3-28](#)
      - deleting [3-30](#)
      - editing [3-30](#)
      - interfaces, selecting [3-29](#)
      - NetFlow device, selecting [3-29](#)
      - source information, verifying [3-30](#)
    - devices, managing [3-26](#)
      - creating [3-26](#)
      - deleting [3-27](#)
      - editing [3-27](#)
      - testing [3-27](#)
    - exporting data [1-12](#)
    - interfaces, understanding [3-21](#)
    - monitoring problems, troubleshooting [A-8](#)
    - records, understanding [3-21](#)
  - NetFlow Data Export [3-11](#)
  - network host data charts and tables, using
    - Network Host Conversations Cumulative Data table, using [4-46](#)
    - Network Host Current Rates [4-37](#)
      - data for a specific host, capturing [4-36](#)
      - detail [4-35](#)
      - real-time statistics in graphical format [4-36](#)
    - Network Host Top N chart [4-37](#)
  - network parameters, setting and viewing [2-12](#)
  - network traffic data, storing and retrieving [1-8](#)
  - NFS Server
    - Configuring for capture data storage [2-20](#)
  - NME-NAM devices
    - default reports [5-4](#)
  - NM-NAM devices
    - NAM version supported [3-10](#)
    - Router Parameters option, and [1-6](#)
    - VLAN data, and [1-7](#)
  - No Activity [5-23](#)
  - Not Monitored [5-23](#)
- 
- ## O
- overview of NAM Traffic Analyzer [1-1](#)
    - alarm logs [7-1](#)
    - data collection [4-2](#)
    - data sources [4-2](#)
    - GUI [1-2](#)
    - navigation and control elements [1-4](#)
    - user interface components [1-3](#)
- 
- ## P
- packet captures, troubleshooting [A-6](#)
  - Packet Loss threshold [3-59](#)
  - passwords, recovering [2-2](#)



patches, troubleshooting [A-13](#)

## Period

report length [5-21](#)

Port Name [3-7](#)

Port names [3-5, 3-7, 3-10, 3-33, 4-94, 4-96, 4-100](#)

port statistics data, viewing [4-93, 4-103](#)

cumulative data [4-100, 4-113](#)

detail [4-96, 4-112](#)

real-time data in graphical format [4-96](#)

reports [4-97](#)

tables and charts useful in

Interface Stats Current Rates table [4-95, 4-111](#)

Port Stats Current Rates table [4-93](#)

Port Stats Top N chart [4-97, 4-112](#)

Top N Interface Stats chart [4-99](#)

port statistics issues, troubleshooting [A-8](#)

Port Stats Current Rates table, using [4-93](#)

detail [4-96, 4-112](#)

real-time data in graphical format [4-96](#)

reports [4-97](#)

Port Stats Top N chart, using [4-97, 4-112](#)

cumulative data [4-100, 4-113](#)

detail [4-102](#)

port traffic

monitoring [1-12](#)

## Process

CPU usage percentage [A-2](#)

protocol data, capturing

client/server data [4-86, 4-90](#)

server data [4-82](#)

protocol directory

managing

creating protocols [3-70](#)

deleting protocols [3-73](#)

editing protocols [3-72](#)

setting up [3-69](#)

protocol filters, in capturing settings [6-9](#)

protocol support, troubleshooting [A-18](#)

## R

real-time data displays, setting up [1-7](#)

recovering passwords [2-2](#)

Refresh button [3-7](#)

Creating SPAN session [3-15](#)

renaming a report [5-25](#)

Report details

viewing [5-21](#)

Report export

editing [5-30](#)

scheduling [5-28](#)

Reports

deleting [5-25](#)

disabling [5-25](#)

error conditions [5-22](#)

Last Status [5-24](#)

Top N [5-21](#)

reports

accessing [1-8](#)

creating [5-1](#)

basic [5-4](#)

custom [5-26](#)

custom

creating [5-26](#)

deleting [5-27](#)

editing [5-27](#)

moving between folders [5-27](#)

viewing [5-27](#)

deleting

basic [5-25](#)

custom [5-27](#)

managing basic report types [5-2](#)

creating [5-4](#)

deleting [5-25](#)

disabling [5-24](#)

enabling [5-24](#)

renaming [5-25](#)

table of, viewing [5-20](#)

- troubleshooting [A-12](#)
  - viewing [5-1](#)
    - custom reports [5-27](#)
  - Response time
    - multiple segments [4-92](#)
  - response time data, viewing [4-69](#)
    - detail
      - client/server [4-86, 4-90](#)
      - server [4-82](#)
    - reports
      - client/server [4-86, 4-90](#)
      - server [4-76, 4-79, 4-83](#)
    - tables and charts useful in
      - Client/Server Response Time table [4-84](#)
      - Client/Server Response Time Top N chart [4-87](#)
      - Server Response Time Top N chart [4-83](#)
  - response time data collections, managing
    - deleting [3-64](#)
    - editing [3-62](#)
    - setting up [3-60](#)
  - RMON
    - log table, viewing [7-2](#)
  - RMON extension [1-9](#)
  - router parameters viewing [3-8](#)
  - RTP Stream Monitoring [3-59](#)
- 
- ## S
- SCCP traffic [6-14](#)
  - Scheduled reports [5-28](#)
  - Server Response Time table, using
    - data, capturing [4-82](#)
    - detail [4-82](#)
    - reports [4-76, 4-79, 4-83](#)
  - Server Response Time Top N chart, using [4-83](#)
  - sessions
    - SPAN [1-10](#)
  - setting
    - alarm thresholds [3-81](#)
    - NAM MIB thresholds [3-84](#)
    - switch thresholds [3-90](#)
    - syslog [3-90](#)
    - community switch strings [3-33](#)
    - NAM SNMP system groups [2-13](#)
    - network parameters [2-12](#)
  - Setup Voice/Video Stream Thresholds window [3-88](#)
  - SNMP
    - troubleshooting [A-17](#)
  - Software filter [6-22](#)
  - SPAN
    - ERSPAN [1-11](#)
    - issues related to, troubleshooting [A-5](#)
    - sessions [1-10](#)
      - creating [3-14](#)
      - deleting [3-16](#)
      - editing [3-15](#)
  - spanning, directing traffic for [3-10](#)
    - custom NetFlow data sources, creating [3-28](#)
    - data source, deleting [3-30](#)
    - data source, editing [3-30](#)
    - data source information, verifying [3-30](#)
    - interfaces, selecting [3-29](#)
    - NetFlow device, selecting [3-29](#)
  - listening mode, using [3-30](#)
  - methods (table) [3-11](#)
  - NDE collection types (table) [3-12](#)
  - NetFlow, configuring on devices [3-22](#)
    - Catalyst OS [3-23](#)
    - Cisco IOS [3-22](#)
    - multi-layer switching cache [3-23](#)
    - NAMs in a device slot [3-24](#)
    - NDE export [3-24](#)
    - NDE v8 aggregations [3-23](#)
  - NetFlow devices, managing [3-26](#)
    - creating [3-26](#)
    - deleting [3-27](#)
    - editing [3-27](#)
    - testing [3-27](#)

- SPAN session
    - creating [3-14](#)
    - deleting [3-16](#)
    - editing [3-15](#)
  - SPAN sources (table) [3-12](#)
  - VACL, configuring
    - on LAN VLANs [3-25](#)
    - on WAN interfaces [3-24](#)
  - spanning, troubleshooting [A-6](#)
  - SPAN states [3-13](#)
  - Statistics
    - viewing VRF [4-115](#)
    - viewing VRF/VC [4-116](#)
  - Style [5-21](#)
  - switch
    - alarm and port statistics issues, troubleshooting [A-8](#)
    - alarm thresholds
      - creating [3-91](#)
      - deleting [3-93](#)
      - editing [3-92](#)
      - setting [3-90](#)
    - NAM date/time synchronization issues, and, troubleshooting [A-14](#)
  - Switch Port report
    - creating [5-4](#)
  - Switch Remote SPAN [3-11](#)
  - Switch SPAN [3-11](#)
  - syslog alarm threshold, setting up [3-90](#)
  - system administration [2-1](#)
    - diagnostics, generating for technical assistance [2-25](#)
    - overview of system administration tasks [2-10](#)
      - NAM community strings, working with [2-14](#)
      - NAM SNMP system group, setting and viewing [2-13](#)
      - NAM system time, setting [2-16](#)
      - network parameters, setting and viewing [2-12](#)
      - system resources, viewing [2-11](#)
    - overview of user administration tasks [2-2](#)
      - passwords, recovering [2-2](#)
      - predefined NAM user accounts, changing [2-3](#)
      - TACACS+ authentication and authorization, establishing [2-6](#)
      - TACACS+ server, configuring to support NAM [2-7](#)
      - user privileges (table) [2-2](#)
      - users, creating new [2-4](#)
      - users, deleting [2-6](#)
      - users, editing [2-5](#)
      - user sessions table, viewing [2-9](#)
      - system resources, viewing [2-11](#)
  - System alerts [2-25](#)
  - system alerts
    - capturing [2-28](#)
    - viewing [2-25](#)
  - System Config Log [5-23](#)
  - System event log
    - viewing [5-23](#)
  - System events [5-23](#)
- 
- ## T
- TAC (Technical Assistance Center)
    - (see also troubleshooting) [A-1](#)
  - TACACS+
    - authentication and authorization, establishing [2-6](#)
    - server, configuring to support NAM [2-7](#)
      - secret key, requirements for [2-8](#)
  - technical assistance, obtaining
    - (see also troubleshooting) [A-1](#)
    - diagnostics, generating for [2-25](#)
      - configuration information, monitoring and capturing [2-27](#)
      - system alerts, capturing [2-28](#)
      - system alerts, viewing [2-25](#)
  - testing NetFlow devices [3-27](#)
  - TopN Applications chart, using [4-11, 4-16](#)
  - TopN Chart
    - Server ART [4-83](#)

Top N report [5-21](#)

traffic analysis [1-10](#)

traffic sources

- monitoring [1-10](#)

troubleshooting [A-1](#)

- data mismatch issues [A-16](#)
- diagnostic error message issues [A-14](#)
- host name resolution issues [A-15](#)
- HTTPS/security certificate issues [A-16](#)
- image upgrade and patch issues [A-13](#)
- login issues [A-3](#)
- NAM and switch date/time synchronization issues [A-14](#)
- NetFlow monitoring problems [A-8](#)
- packet capturing and spanning issues [A-6](#)
- protocol support issues [A-18](#)
- reporting issues [A-12](#)
- slow response times [3-95](#)
- SNMP issues [A-17](#)
- SPAN-related issues [A-5](#)
- switch, cannot communicate with [3-33](#)
- switch alarm and port statistics issues [A-8](#)
- username and password issues [A-2](#)
  - caution regarding deleting all local database web users [A-3](#)
- voice monitoring issues [A-19](#)
- web browser response time and display issues [A-13](#)

---

## U

user

- administration (see system administration) [2-1](#)
- privileges (table) [2-2](#)
- sessions table, viewing [2-9](#)
- Users Table (illustration) [2-4](#)

username and password issues, troubleshooting [A-2](#)

---

## V

V8 aggregation caches, and NDE flow-masks [4-5](#)

VACL [1-11](#)

- VLAN access control list [1-10, 1-11](#)

VACL, configuring

- on LAN VLANs [3-25](#)
- on WAN interfaces [3-24](#)

VC statistics [4-116](#)

verifying NetFlow data source information [3-30](#)

versions of Catalyst 6500 NAM [3-10](#)

Viewing

- MPLS traffic statistics [4-117](#)

viewing

- active call data [4-32](#)
- application data [4-14](#)
  - capturing, for a specific protocol [4-11, 4-16](#)
  - detail for a specific protocol [4-14](#)
  - packets and bytes collected [4-13, 4-17](#)
  - real-time data in graphical format [4-11, 4-16](#)
  - reports [4-11, 4-16](#)
- community switch strings [3-33](#)
- conversations data [4-42](#)
  - packets and bytes for each host conversation [4-43](#)
- custom reports [5-27](#)
- DiffServ data [4-57](#)
  - host conversation details [4-66](#)
  - host statistics [4-67](#)
  - real-time data in graphical format [4-66](#)
  - real-time traffic statistics in graphical format [4-59](#)
  - reports [4-59](#)
- host data [4-34](#)
  - collected during last time interval [4-34](#)
  - cumulative MAC stations data [4-41](#)
  - for a specific host, capturing [4-36](#)
  - MAC stations current rates [4-39](#)
  - real-time statistics in graphical format [4-36](#)

- reports [4-37](#)
- Monitor Overview charts [4-6](#)
- NAM log [7-2](#)
- NAM MIB alarm details [3-87](#)
- NAM SNMP system groups [2-13](#)
- network parameters [2-12](#)
- packets and bytes collected for top n MAC station conversations [4-49](#)
- packets and bytes for each MAC station conversation [4-51](#)
- port statistics data [4-93, 4-103](#)
  - cumulative [4-100, 4-113](#)
  - detail [4-96, 4-112](#)
  - real-time data in graphical format [4-96](#)
  - reports [4-97](#)
- response time data [4-69](#)
  - client/server [4-86, 4-90](#)
  - client/server detail [4-86, 4-90](#)
  - server [4-76, 4-79, 4-83](#)
  - server detail [4-82](#)
- RMON log table [7-2](#)
- router parameters [3-8](#)
- switch
  - log [7-2](#)
- system alerts [2-25](#)
- system resources [2-11](#)
- user sessions table [2-9](#)
- VLAN data [4-51](#)
  - collected for the top n VLAN IDs, in graphical format [4-53](#)
  - cumulative data for each VLAN ID [4-54](#)
  - reports [4-53](#)
  - user priority distributions in graphical format [4-56](#)
  - user priority distributions per data source [4-55, 4-57](#)
- voice data [4-18](#)
  - active calls [4-32](#)
  - known phones [4-30](#)
- Viewing audit trail [2-26](#)
- Virtual circuits [3-47](#)
- Virtual Switch Software (VSS) [3-5](#)
- Virtual switch software (VSS) [4-94](#)
- VLAN access control list
  - VACL [1-10, 1-11](#)
- VLAN data, viewing [4-51](#)
  - cumulative data for each VLAN ID [4-54](#)
  - reports [4-53](#)
  - tables and charts useful in
    - VLAN Priority (COS) Statistics Cumulative Data table [4-57](#)
    - VLAN Priority (COS) Statistics Current Rates table [4-55](#)
    - VLAN Priority (COS) Statistics Top N chart [4-56](#)
    - VLAN Traffic Statistics Cumulative Data table [4-54](#)
    - VLAN Traffic Statistics Current Rates table [4-52](#)
    - VLAN Traffic Statistics Top N chart [4-53](#)
  - user priority distributions in graphical format [4-56](#)
  - user priority distributions per data source
    - cumulative [4-57](#)
    - current rates [4-55](#)
- VLAN Priority (COS) Statistics
  - Cumulative Data Table, using [4-57](#)
  - Current Rates table, using [4-55](#)
  - Top N chart, using [4-56](#)
- VLAN report
  - creating [5-4](#)
- VLAN Traffic Statistics
  - Cumulative Data table, using [4-54](#)
  - Current Rates table, using [4-52](#)
  - Top N chart, using [4-53](#)
- Voice/Video stream thresholds [3-88](#)
- Voice/Video Stream Thresholds Per Minute window [3-88](#)
- voice data
  - collecting [3-57](#)
  - viewing [4-18](#)
    - active calls [4-32](#)
    - known phones [4-30](#)

Voice monitoring [3-57](#)  
voice monitoring, troubleshooting [A-19](#)  
VPN routing/forwarding table [3-47](#)  
VRF statistics [4-115, 4-116](#)  
VSS  
    see Virtual Switch Software [3-7, 3-10, 3-33](#)

---

## W

WAAS data source  
    no data [A-20](#)  
WAAS data sources [4-92](#)  
WAAS device status  
    pending [A-20](#)  
WAN interfaces [3-34](#)  
WS-SVC-NAM-1 [3-10](#)  
WS-SVC-NAM-2 [3-10](#)