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

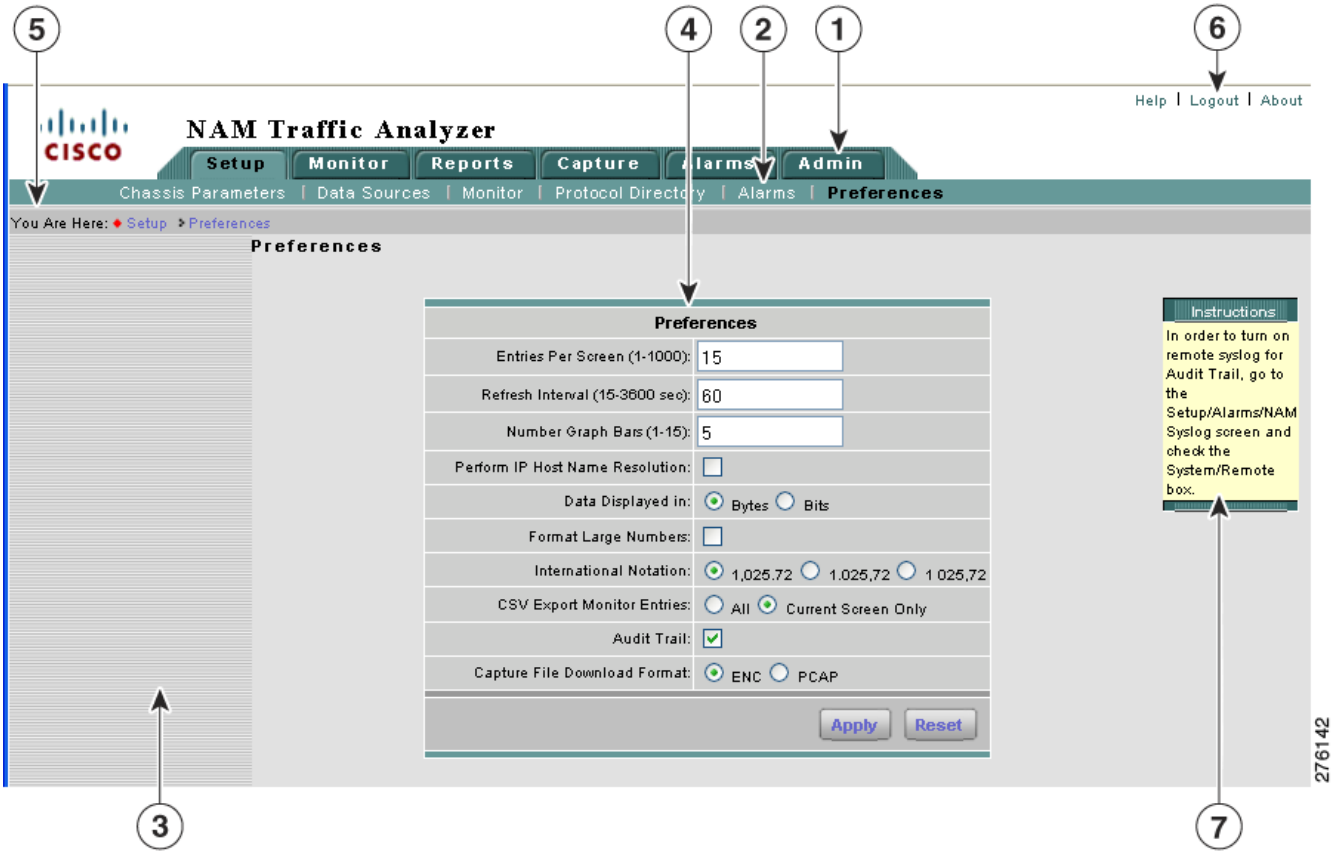
The Cisco Network Analysis Module (NAM) Traffic Analyzer software enables network managers to understand, manage, and improve how applications and services are delivered to end-users. The NAM offers flow-based traffic analysis of applications, hosts, and conversations, performance-based measurements 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

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

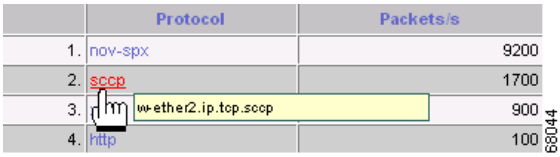
Element	Description
Start	Starts an action.
Stop	Stops an action, such as the active capturing of packets.
Pause	Temporarily suspends an action.
Create	Creates a new record, user, capture, filter, and so on.
Delete	Deletes a record, user, capture, filter, and so on.
Edit	Edits a record, user, capture,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

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

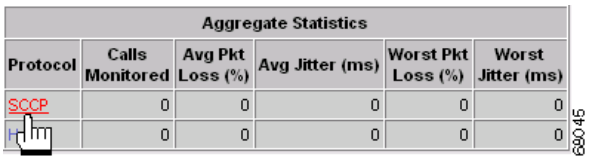
Element	Description
Real-Time	Displays real-time statistics for the selected variable.
Capture	Captures the packets to the buffer.
	Exports the data on the screen to a **.csv** text file. If you want to export more data, you must increase the rows per page setting for the table. The default setting is 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:

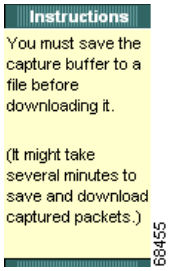
Pop-up help—To expand abbreviated protocol encapsulation information in some links, move your mouse over the link. The full protocol encapsulation name is displayed.



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.



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



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.

After configuring the VACL, you do not need to go to **Setup > Data Sources**, as the GUI will not show the VACL or WAN Interface as a Data Source.

You will need to:

- Go to **Setup > Monitor > Core Monitoring**
- Select the data port that you configured on the switch CLI as VACL CAPTURE (for example, Dataport1)
- Check the required Monitoring Functions for whatever you want the NAM to monitor (for example, Application Statistics, Host Statistics, Conversation Statistics).
- Go to the Monitor, Reports, or Capture Tab and configure as required to use the Dataport that you configured on the switch CLI (for example, Dataport1).

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**.