

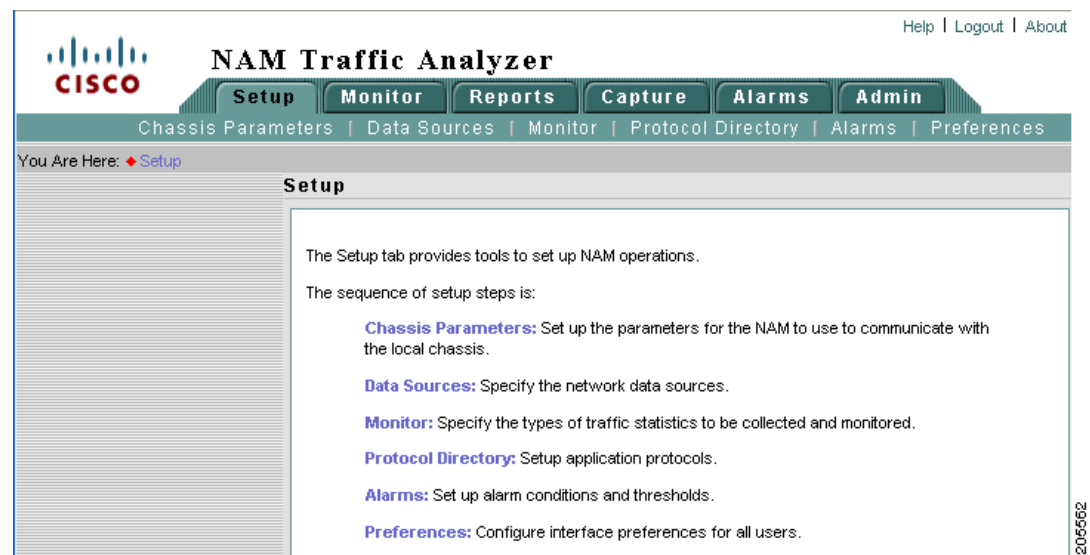


# CHAPTER 3

## 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 3-95](#)

# 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.  <b>Note</b> Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.

**Table 3-1**      **Switch Information (continued)**

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

## 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
<input checked="" type="checkbox"/>	Fa0/0	FastEthernet0/0
<input type="checkbox"/>	Se0/0	Serial0/0
<input checked="" type="checkbox"/>	Fa0/1	FastEthernet0/1
<input type="checkbox"/>	An1/0	Analysis-Module1/0
<input checked="" type="checkbox"/>	Fa2/0	FastEthernet2/0
<input checked="" type="checkbox"/>	Fa2/1	FastEthernet2/1
<input type="checkbox"/>	Fa2/2	FastEthernet2/2
<input type="checkbox"/>	Fa2/3	FastEthernet2/3
<input type="checkbox"/>	Fa2/4	FastEthernet2/4
<input type="checkbox"/>	Fa2/5	FastEthernet2/5
<input type="checkbox"/>	Fa2/6	FastEthernet2/6
<input type="checkbox"/>	Fa2/7	FastEthernet2/7
<input type="checkbox"/>	Fa2/8	FastEthernet2/8
<input type="checkbox"/>	Fa2/9	FastEthernet2/9
<input type="checkbox"/>	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	<p>Name of the interface.</p> <p>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.</p> <p>Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1.</p> <p>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.</p>
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:

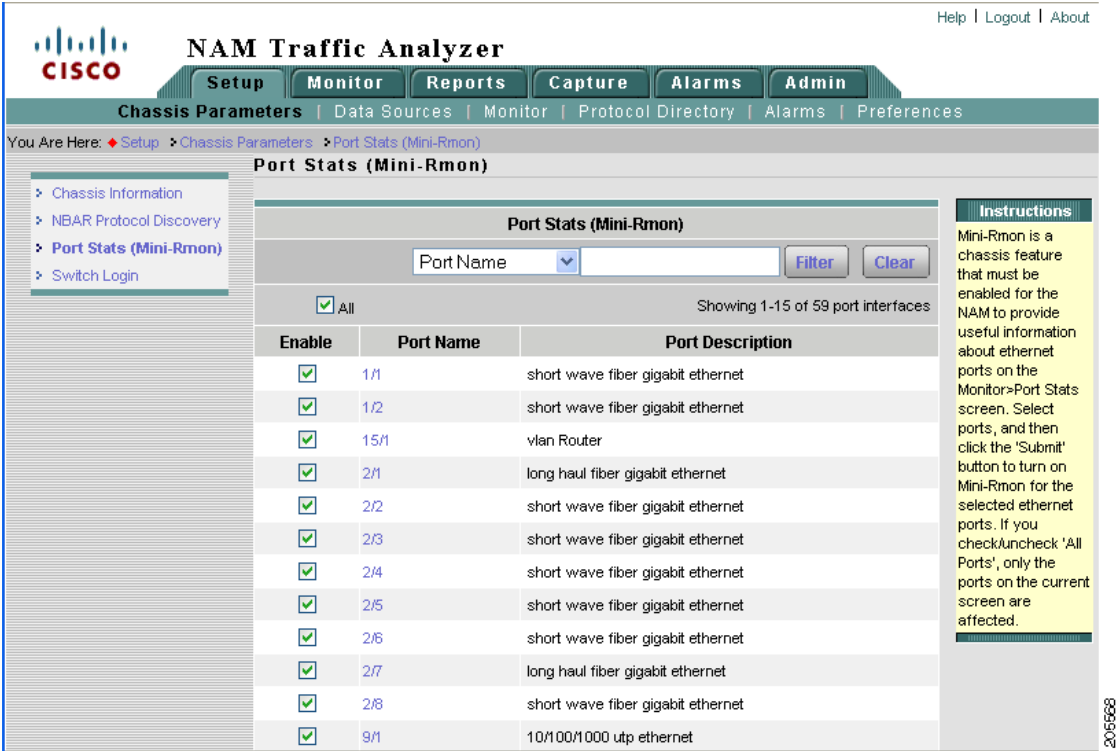
- Step 1

Click **Setup > Chassis Parameters**.
- 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 Gi1/2/1 to represent a Gigabit port on switch 1, module 2, 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, module 2, 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	<p>You can direct a set of physical ports, a set of VLANs, or a set of EtherChannels to the NAM.</p> <p>Selecting an EtherChannel as a SPAN source it is the same as selecting all physical ports comprising the EtherChannel as the SPAN source.</p> <p>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.</p> <p><b>Note</b> This method does not apply to NME-NAM devices.</p>
Switch Remote SPAN (RSPAN)	<p>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.</p> <p>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.</p> <p><b>Note</b> This method does not apply to NME-NAM devices.</p>
NetFlow Data Export (NDE)	<p>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.</p> <p>SPAN and NDE sources can be in effect simultaneously.</p>

## 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	<ul style="list-style-type: none"> <li>NAM Traffic Analyzer</li> <li>Switch CLI</li> <li>Supervisor portCopyTable (SNMP)</li> </ul>
Any EtherChannel	<ul style="list-style-type: none"> <li>NAM Traffic Analyzer</li> <li>Switch CLI</li> <li>Supervisor portCopyTable (SNMP)</li> </ul>
Any set of VLANs configured on the local switch	<ul style="list-style-type: none"> <li>NAM Traffic Analyzer</li> <li>Switch CLI</li> <li>Supervisor portCopyTable (SNMP)</li> </ul>
Packets from a remote switch arriving via RSPAN <b>Note</b> You can select only one RSPAN VLAN as a SPAN source.	<ul style="list-style-type: none"> <li>NAM Traffic Analyzer</li> <li>Switch CLI</li> <li>Supervisor portCopyTable (SNMP)</li> <li><i>and</i></li> <li>Configuration on remote switch</li> </ul>

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. <b>Note</b> 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 <a href="#">Table 3-10</a> for a description of the possible SPAN states. <b>Note</b> 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. <b>Note</b> This button is labeled <b>Add Dest. Port</b> on the NAM-1.
Add Dest. Port 2	Click to add NAM Port 2 to the selected SPAN session as a SPAN destination. <b>Note</b> 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.  <b>Note</b> For switches running Cisco IOS or Catalyst OS 8.4 (and later) software only.
SPAN Type	<ul style="list-style-type: none"> <li>SwitchPort</li> <li>VLAN</li> <li>EtherChannel</li> <li>RSPAN VLAN</li> </ul> <b>Note</b> 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	<ul style="list-style-type: none"> <li>Rx</li> <li>Tx</li> <li>Both</li> </ul> <b>Note</b> Not applicable to RSPAN VLAN SPAN types.
Available Sources	SPAN sources that are available for the selected SPAN type.
<b>Add</b>	Adds the selected SPAN source.
<b>Remove</b>	Removes the selected SPAN source.
<b>Remove All</b>	Removes all the SPAN sources.
Selected Sources	SPAN sources selected.
<b>Refresh</b>	Causes the NAM to update the switch configuration information with current configuration.
<b>Submit</b>	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. <b>Note</b> 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.
<b>Refresh</b>	Causes the NAM to update the switch configuration information with current configuration.
<b>Submit</b>	Saves changes.
<b>Reset</b>	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
<input checked="" type="checkbox"/>	VLAN 1	default (1)	Operational
<input checked="" type="checkbox"/>	VLAN 2	probe_vlan (2)	Operational
<input checked="" type="checkbox"/>	VLAN 3	ixLoadServerTraffic (3)	Operational
<input checked="" type="checkbox"/>	VLAN 4	ixLoadClientTraffic (4)	Operational
<input checked="" type="checkbox"/>	VLAN 10	3845_Crash_Test (10)	Operational
<input type="checkbox"/>	VLAN 35	connect_to_gateway (35)	Operational
<input type="checkbox"/>	VLAN 36	VLAN0036 (36)	Operational
<input type="checkbox"/>	VLAN 37	VLAN0037 (37)	Operational
<input type="checkbox"/>	VLAN 38	VLAN0038 (38)	Operational
<input type="checkbox"/>	VLAN 39	VLAN0039 (39)	Operational
<input type="checkbox"/>	VLAN 40	VLAN0040 (40)	Operational
<input type="checkbox"/>	VLAN 150	VLAN0150 (150)	Operational
<input type="checkbox"/>	VLAN 600	VLAN0600 (600)	Operational
<input type="checkbox"/>	VLAN 890	VLAN0890 (890)	Operational
<input type="checkbox"/>	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:

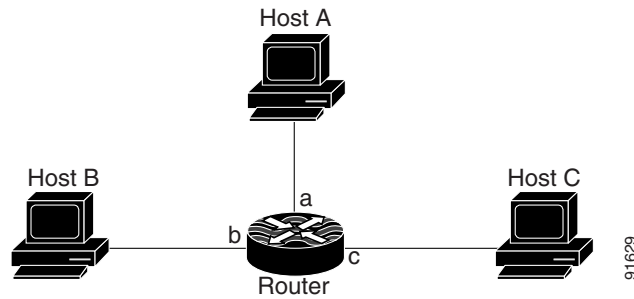
- Input SNMP ifIndex
- Output SNMP ifIndex



### 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**

| V9 Template for 172.20.98.129 |                                           |                |
|-------------------------------|-------------------------------------------|----------------|
| 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*

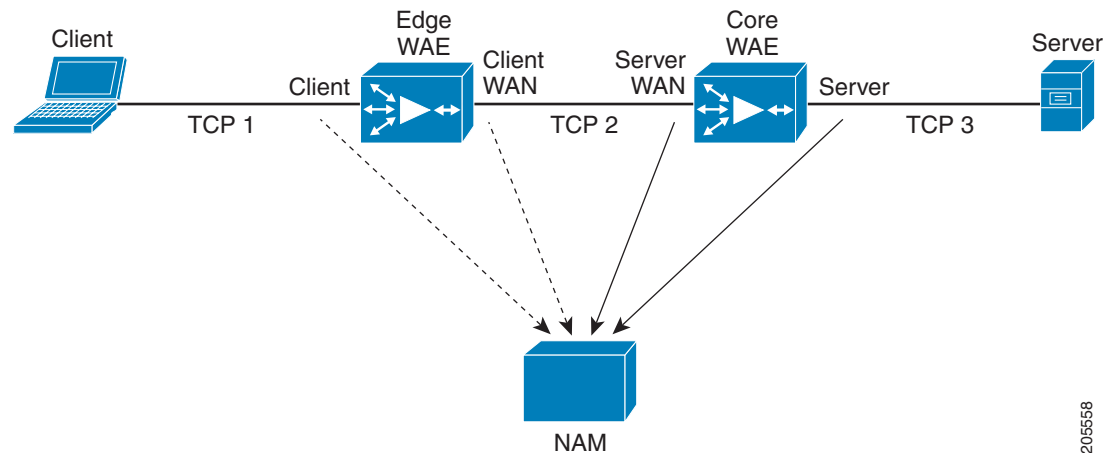
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/waas/v4019/configuration/guide/waas4cfg.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html)

## 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**

**New Device**

WAAS Device IP Addr:

**Monitor WAAS segment(s):**

☐ Client

☐ Client WAN

☐ Server WAN

☐ Server

☐ Export Passthru Response Time

206584

**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 --> Add Delete

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**

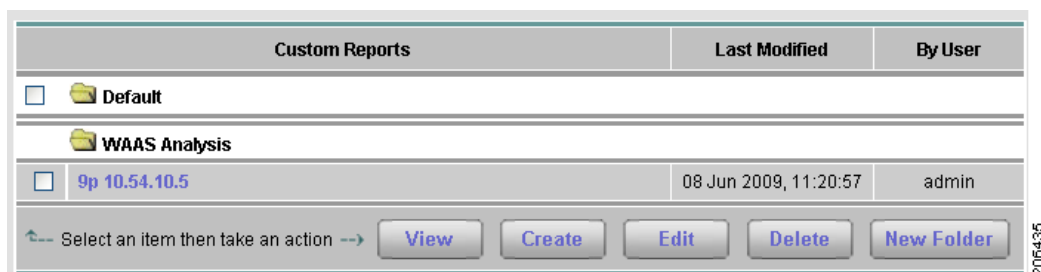
- Step 3** Choose a Branch WAE from the Select Branch WAE pull-down menu.
- If no WAE devices listed, use WAE CLI command **flow monitor** to enable flow exports to the NAM.

- 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:

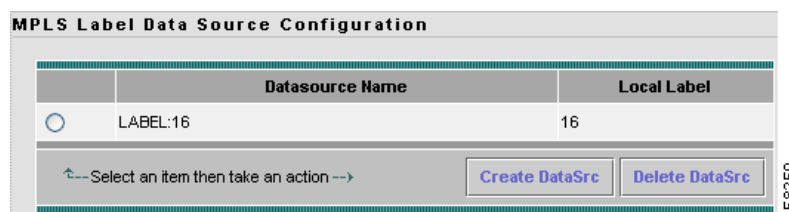
**Step 1** Choose **Setup > Data Sources**.

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**



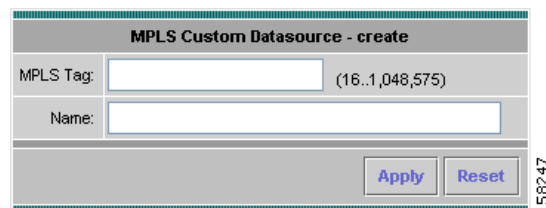
**Step 3** Click **Create DataSrc**.

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. |

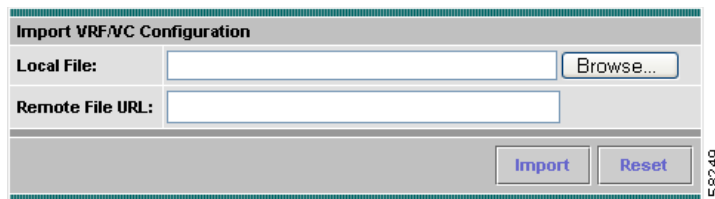
The following is an example of the VRF/VC configuration file:

```
# 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**

The screenshot shows the 'RTP Stream Monitor Setup' window. It includes a configuration section with the following details:

- Enabled:** ☒
- Max RTP Streams: (1-4000):** 4000
- Report Interval:** 60 seconds
- Buttons:** Apply, Reset

Below this is a **Filter Table** with the following structure:

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

At the bottom of the window, there is a status bar that says 'Check desired functions then Apply' and buttons for 'Create', 'Edit', and 'Delete'.

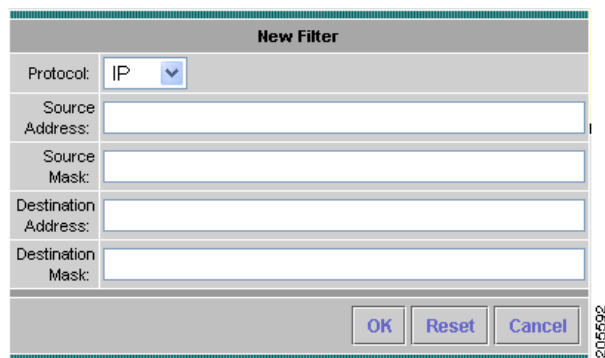
**Step 3** Click the Enabled check box to enable RTP stream monitoring.

**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. |

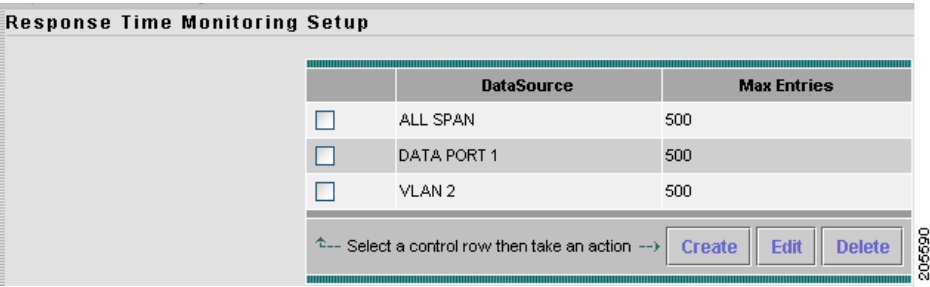
- Step 3**    Accept the default settings or change the settings to the values you want to monitor. Click **Submit** to save your changes, or click **Reset** to cancel.

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 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 | ART 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:

---

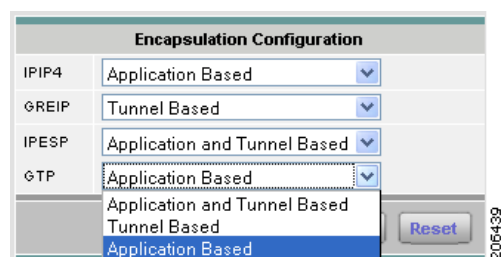
**Step 1** Choose **Setup > Protocol Directory**.

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><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

Autolearned Protocols Preferences

Enable Autolearned Protocols:

☒

Maximum Autolearned Protocols (100-500):

100

Maximum TCP Port (0-65535):

65535

Maximum UDP Port (0-65535):

65535

TCP Exclusion Port Range (0 Disables) (1-65535):

Start: 0 End: 0

UDP Exclusion Port Range (0 Disables) (1-65535):

Start: 0 End: 0

Apply

Reset

129519

- 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.



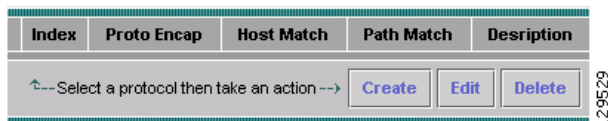
### Note

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.<br>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:<br>application/octet-stream,<br>text/html, or image/gif |
| Protocol Description | Name of the URL based application                                                              | For example:<br><b>url-match-domain-com.</b>                         |

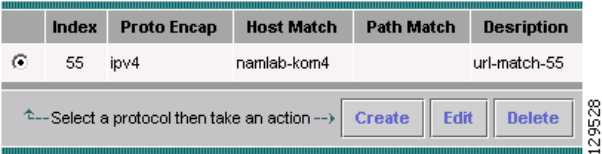
**Step 5**      Click **Apply** to save your changes, or click **Reset** to cancel.

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

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          |
|-------|-------------|------------|------------|----------------------|
| 55    | ipv4        | domain.com | /intro?id  | url-match-domain.com |

**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 3-91](#)
- [Setting NAM Trap Destinations, page 3-94](#)
- [Setting NAM Alarm Mail, page 3-95](#)

## 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**

- 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:

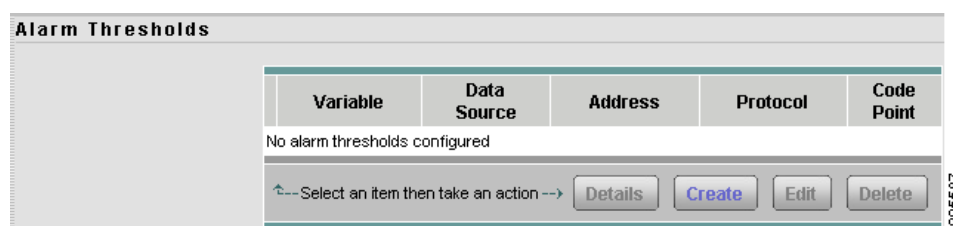
**Step 1** Click **Setup > Alarms**.

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 <button>Details</button> <span style="color: blue;">Create</span> <button>Edit</button> <button>Delete</button> |             |         |          |            |

**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**

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**

| 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                            |
|                          | 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): |
| <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                              |

Defaults Apply Reset

[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.

If logging on a remote host, in most Unix-based systems, the syslog collector that handles the incoming syslog messages uses the facility field to determine what file to write the message to, and it will use a facility called "local2." Check the syslog collector configuration to ensure that "local2" is handled properly.

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 3-93](#)
- [Deleting Chassis or Managed Device Thresholds, page 3-94](#)

### 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> | —                                                                                                                                                                                                                                     |
| 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.                                                                                                                                                                                                       |

**Table 3-35**      ***New Chassis Alarm Dialog Box (continued)***

| Field        | Description                                     | Usage Notes                                                                                                                                                                                                                                            |
|--------------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 3-94](#)
- [Editing a NAM Trap Destination, page 3-94](#)
- [Deleting a NAM Trap Destination, page 3-95](#)

## 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><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.                                                               |
| 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                                                                                                                                                                   |



**Table 3-37**      **Preferences Dialog Box (continued)**

| Field                        | Description                                                                                                                              | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                          | <p>Enables the recording of critical user activities to an internal log file. By default, the audit trail is enabled.</p> <p>See also:</p> <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.

