Setting Up the Application

These topics help you set up and configure the application:

Viewing Switch Parameters

For WS-SVC-NAM-1, WS-SVC-NAM-2, and WS-X6380-NAM Platforms

Step 1 Click **Setup**.

Step 2 Click Switch Parameters.

The Switch System Information Table (Table 3-1) is displayed.

Table 3-1 Switch System Information Table

Field	Description
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-Write Community String	Enter the SNMP community string configured on the switch.
Verify String	Verify the SNMP community string.

Viewing Router Parameters

For NM-NAM Devices

Step 1 Click **Setup**.

Step 2 Click Router Parameters.

The Router System Information Table (Table 3-2) is displayed.

Table 3-2 Router System Information Table

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 Community String	Name of the SNMP community string configured on the router.
Verify String	Verify the SNMP community string.

Testing SNMP on the Switch or Router

To test SNMP communication on the switch or router, click **Test**.

The Switch/Router Community String Test window is displayed with the results of the test. Click **Close** to close the window.

Setting Up Data Sources

The NAM currently has four versions:

- WS-X6380-NAM
- WS-SVC-NAM-1
- WS-SVC-NAM-2
- NM-NAM

The NM-NAM devices have two FastEthernet data sources—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. For more information on setting up the data sources for the NM-NAM device, skip to the "Managing NetFlow Devices" section on page 3-19.

The following information descibes how to set up NetFlow and SPAN sessions for the WS-X6380-NAM, WS-SVC-NAM-1, and WS-SVC-NAM 2 devices.

The WS-X6380-NAM and WS-SVC-NAM-1 devices can have only one active SPAN session. You can select a switch port, VLAN, EtherChannel, or NetFlow Data Export (NDE) as the SPAN source; however, you may select only one SPAN type. WS-SVC-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 3-3).

Table 3-3 Methods of Directing Traffic

Method	Usage Notes
Switch SPAN	You can direct a set of physical ports, a set of VLANs, or a set of EtherChannels to the NAM. Selecting an EtherChannel as a SPAN source it is the same as selecting all physical ports comprising the EtherChannel as the SPAN source. **Note** This method does not apply to NM-NAM devices.

Table 3-3 Methods of Directing Traffic (continued)

Method	Usage Notes
Switch Remote SPAN (RSPAN)	You can monitor packet streams from remote switches, assuming that all traffic from a remote switch arrives at the local switch on a designated RSPAN VLAN. Use the RSPAN VLAN as the SPAN source for the NAM. **Note** This method does not apply to NM-NAM devices.
NetFlow Data Export (NDE)	You can monitor NDE records directly from remote switches or routers. You must configure the NDE source to the NAM from a local switch or remote router, using the switch CLI. SPAN and NDE sources can be in effect simultaneously.

The SPAN Sources Table (Table 3-4) describes the streams of traffic you can use as SPAN sources.

Table 3-4 SPAN Sources Table

SPAN Source	One of the following:
Any set of physical ports	• NAM Traffic Analyzer • Switch CLI • Supervisor portCopyTable (SNMP)
Any EtherChannel	• NAM Traffic Analyzer • Switch CLI • Supervisor portCopyTable (SNMP)

Table 3-4 SPAN Sources Table (continued)

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

You can also use locally generated NDE records (the NDE source) as a packet stream to populate NAM collections. You can activate only a subset of the NAM collection types defined in the NDE Collection Types Table (Table 3-5) 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 3-5 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.
DiffServ apps	DSMON applications table.
DiffServ hosts	DSMON host table. **Note** Only for remote switches and routers.

Creating a SPAN Session

Note This section does not apply to NM-NAM devices.

Creating a SPAN session on a switch running Catalyst OS software and a switch running Cisco IOS software are different. Unless otherwise stated, the following steps apply to switches running both Catalyst OS and Cisco IOS software.

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

The Active SPAN Sessions Dialog Box (Table 3-6) is displayed. The SPAN session directed to the NAM is selected by default, otherwise the first radio button is selected.

Table 3-6 Active SPAN Sessions Dialog Box

Column	Description
Monitor Session	Monitor session of the SPAN. **Note** For switches running Cisco IOS software only.
Type	Type of SPAN source.
Source - Direction	Source of the SPAN session and direction of the SPAN traffic. **Note** For switches running Cisco IOS software only.
Source	Source of the SPAN session. For port SPAN types, the source displays the port name and source status *after* you SPAN it—down, testing, or dormant. **Note** When creating a SPAN session, you can select all ports regardless of their state.
Dest. Port	The destination port of the SPAN session.
Dest. Module	The destination module of the SPAN session.

Table 3-6 Active SPAN Sessions Dialog Box (continued)

Column	Description
Direction	The direction of the SPAN traffic.
Status	Status of the SPAN session.

Step 3 Click **Create**.

The Create SPAN Session Dialog Box (Table 3-7) is displayed. Switch Port is the default for the SPAN Type.

Step 4 Select the appropriate information.

Table 3-7 Create SPAN Session Dialog Box

Field	Description
Monitor Session	Monitor session of the SPAN. **Note** For switches running Cisco IOS software only.
SPAN Type	• SwitchPort. • VLAN. • EtherChannel. • RSPAN VLAN. **Note** You can have only one RSPAN VLAN source per SPAN session.
Switch Module List	Lists all modules on the switch other than NAMs and Switch Fabric Modules.
SPAN Destination Interface	The NAM interface you want to send data to. **Note** WS-SVC-NAM-2 devices only.
SPAN Traffic Direction	• Rx. • Tx. • Both. **Note** Not applicable to RSPAN VLAN SPAN types.
Available Sources	SPAN sources that are available for the selected SPAN type.
Add	Adds the selected SPAN source.

Table 3-7 Create SPAN Session Dialog Box (continued)

Field	Description
Remove	Removes the selected SPAN source.
Remove All	Removes all the SPAN sources.
Selected Sources	SPAN sources selected.
Submit button	Creates the SPAN configuration.

Step 5 To submit the SPAN session, click **Submit**.

The Active SPAN Sessions dialog box is displayed and the SPAN session is saved for switches running Catalyst OS software only.

Step 6 To save the SPAN session and save the running-configuration to the startup-configuration for switches running Cisco IOS software only, select the radio button and click **Save SPAN**.

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

Step 7 Click **Ok** to confirm.

Editing a SPAN Session

Note This section does not apply to NM-NAM devices.

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

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

The Active SPAN Sessions dialog box is displayed.

Step 3 Select the SPAN session to edit, then click **Edit**.

The Edit SPAN Session Dialog Box (Table 3-8) is displayed.

Step 4 Make the appropriate changes.

Table 3-8 Edit SPAN Session Dialog Box

Field	Description
Monitor Session	Monitor session of the SPAN. **Note** For switches running Cisco IOS software only. You cannot edit this value.
SPAN Type	Type of SPAN session. **Note** You cannot edit the SPAN type on switches running Catalyst OS software.
Switch Module List	Lists all modules on the switch other than NAMs and Switch Fabric Modules.
SPAN Traffic Direction	Direction of the SPAN traffic. **Note** You cannot edit the SPAN direction on switches running Catalyst OS software. For such switches, all SPAN sources in a SPAN session must be in only one direction.
Available Sources	SPAN sources available for the selected SPAN type.
Add	Adds the selected SPAN source
Remove	Removes the selected SPAN source.
Remove All	Removes all the SPAN sources.
Selected Sources	SPAN sources selected.
Submit button	Saves changes.
Reset button	Clears all changes.

Deleting a SPAN Session

Note This section does not apply to NM-NAM devices.

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

Understanding NetFlow Interfaces

To use a remote device as an NDE data source for the NAM, you must configure the remote 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 remote 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 remote 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 an input 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 an output 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 a bidirectional interface in another flow path for the same conceptual data source.

Understanding NetFlow Flow Records

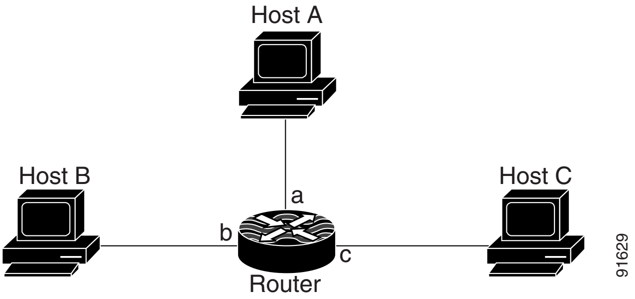
An NDE packet contains multiple flow records. Each flow record has two fields:

- 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 4-6.

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 3-1) shows a sample network configuration with a NetFlow router.

Figure 3-1 Sample NetFlow Network



The Reporting Flow Records table (Table 3-9) lists the reported flows if NetFlow is enabled on interface a.

Table 3-9 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>
```

Step 2 Enable NetFlow on the interface.

```
Prompt(config-if)#ip route-cache flow
```

Step 3 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 v8 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 v8 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 UPD 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 UPD port 3000 of the NAM

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

For NAMs Located in a Device Slot

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

Step 1 Select the version of NDE

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

Step 2 Select NDE flow mask to be full.

```
Prompt>(enable) sel mls nde full
```

Step 3 Enable NDE export.

```
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 of 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.

Note VACL data analysis is not supported for WS-X6380-NAM devices.

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)#map 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 3-13 or your accompanying device documentation. The following topics help you set up and manage the devices used for NetFlow monitoring:

- Creating Devices, page 3-19
- Editing Devices, page 3-20
- Deleting Devices, page 3-21
- Testing Devices, page 3-21
- Creating Custom Data Sources, page 3-22
- Using the Listening Mode, page 3-25

Creating Devices

Once you create 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 3-25.

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

The Active SPAN Sessions table is displayed.

Note For NM-NAM devices, the Netflow Devices table is displayed.

Step 3 In the contents, click **Devices**.

The NetFlow Devices table is displayed.

Step 4 Click **Create**.

The New Device dialog box appears.

Step 5 Enter the device name and community string, then do one of the following:

- To save the changes, click **OK**.
- To clear the entries in the dialog box, click **Reset**,
- To leave the entries unchanged, click **Cancel**.

Editing Devices

Note You cannot edit the local switch.

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

The Active SPAN Sessions table is displayed.

Step 3 In the contents, click **Devices**.

The NetFlow Devices table is displayed.

Step 4 Select the device you wish to edit from the table and click **Edit**.

The Edit Device window appears.

Step 5 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 Devices

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

The Active SPAN Sessions table is displayed.

Step 3 In the contents, click **Devices**.

The NetFlow Devices table is displayed.

Step 4 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 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 3-10) is displayed.

Table 3-10 Device System Information Dialog Box

Field	Description
Name	Name of the device.
Hardware	Hardware description of the device.
Supervisor Software Version	The current software version running on the Supervisor.
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 switch only.

Table 3-10 Device System Information Dialog Box (continued)

Field	Description
SNMP write from device	SNMP write test result. For the local switch only.
NetFlow on device	Verification if NetFlow is configured for this device.
Mini-RMON on device	Verification if mini-RMON is available for this device. For the local switch only.
VLAN Traffic Statistics on device	Verification if VLAN traffic statistics are available for this device. For the local switch only.

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 "Creating Devices" section on page 3-19. This option allows you to create custom data sources on NetFlow devices with specific interface information.

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**.

Step 3 From the contents, select **Custom Data Sources**.

The NetFlow Data Sources table is displayed.

Step 4 Click **Create**.

The following table shows the wizard used to create or edit a NetFlow data source.

	Wizard Page	References
Step 1	Device Selection	"Selecting a NetFlow Device" section on page 3-23
Step 2	Interface Selection	"Selecting the Interfaces" section on page 3-23
Step 3	Summary	"Verifying NetFlow Data Source Information" section on page 3-24

Selecting 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

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

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

Step 1 Click the Setup tab.

Step 2 Click **Data Sources**

Step 3 Click **Custom Data Sources**.

The NetFlow Data Sources table is displayed.

Step 4 Select the data source you wish to edit, then click **Edit**.

The wizard used to edit NetFlow data sources is displayed.

Step 5 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.

Step 1 Click the Setup tab.

Step 2 Click **Data Sources.**

Step 3 In the contents click **Listening Mode.**

The NetFlow Listening Mode Table (Table 3-11) is displayed.

Table 3-11 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 4 Click **Start**.

Step 5 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 3-12) is displayed.

Table 3-12 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.

Adding a Device To Monitor

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

The New Device Window is displayed.

Step 2 Enter the device information and click OK.

The new device is added to the NetFlow Devices table.

Testing the Switch/Router Community Strings

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

The switch automatically sends the read and write community strings to the NAM. If the device is running the Catalyst OS, you can enter the switch SNMP community strings manually. For NM-NAM devices, 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 switch/router, use the switch or router CLI. For information on using the CLI, see the documentation that accompanied your device.

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

Step 1 Click the Setup tab.

Step 2 Click **Switch Parameters**.

For NM-NAM devices, click **Router Parameters**.

The Switch/Router Parameters dialog box is displayed.

Note WS-SVC-NAM-1 and WS-SVC-NAM-2 devices automatically match the read-write community strings with the Supervisor on the switch.

Step 3 Click **Test**.

The Switch/Router Community String Test dialog box is displayed.

Setting Up Data Collections

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 for:

- Monitoring Core Data
- Monitoring Voice Data
- Monitoring Response Time Data
- Monitoring DiffServ Data

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 screens.
- 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.

Note MAC and VLAN collections are not available onNM-NAM devices.

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

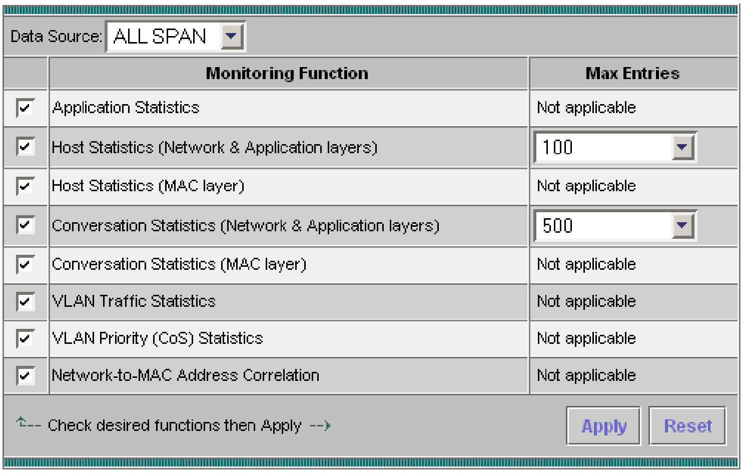
Note You must disable all reports for the collections you want to turn off. If you turn off collections that have reports running on them, the collections will automatically be turned on. For more information on disabling reports, see the "Enabling and Disabling Reports" section on page 5-3.

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions Dialog Box (Figure 3-2) is displayed.

Figure 3-2 Core Monitoring Functions Dialog Box



Data Source: ALL SPAN

	Monitoring Function	Max Entries
☑	Application Statistics	Not applicable
☑	Host Statistics (Network & Application layers)	100
☑	Host Statistics (MAC layer)	Not applicable
☑	Conversation Statistics (Network & Application layers)	500
☑	Conversation Statistics (MAC layer)	Not applicable
☑	VLAN Traffic Statistics	Not applicable
☑	VLAN Priority (CoS) Statistics	Not applicable
☑	Network-to-MAC Address Correlation	Not applicable

Step 3 Select the collection data source from the Data Source list.

Step 4 Select the check boxes to enable specific core monitoring functions.

Step 5 Select the maximum number entries from the Max Entries lists.

Step 6 Do one of the following:

- To save the changes, click **Apply**.
- To leave the configuration unchanged, click **Reset**.

Enabling Mini-RMON Collection

Note This section does not apply to NM-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.

Note The Catalyst 6000 and 6500 Series NAMs do not require the purchase of an RMON agent license.

Monitoring Voice Data

When you enable monitoring for voice data, the results are exclusively available through the NAM Traffic Analyzer. You can use the Monitor tab to view the collected voice data. For more information on viewing the voice data, see the "Viewing Voice Data" section on page 4-19.

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

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents, click **Voice Monitoring**.

The Voice Monitor Setup Dialog Box(Table 3-13) is displayed.

Step 4 Select the appropriate information.

Table 3-13 Voice Monitor Setup Dialog Box

Field	Description	Usage Notes
Monitoring Enabled	—	Select the check box to monitor the protocol.
Number of phone table rows	The maximum number of phone records that can be monitored.	Enter a number from 10 to 1000.
Number of call table rows	The maximum number of active calls that can be monitored.	Enter a number from 10 to 1000.
Number of top packet jitter rows	The number of Top N phone calls with the worst jitter.	Enter a number from 1 to 20.
Number of top packet loss rows	The number of Top N phone calls with the worst packet loss.	Enter a number from 1 to 20.
Debug	Allows the application to display calls that are still in the setup state.	Click to turn on the debug option.

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

Step 5 Do one of the following:

- To save the changes, click **Apply**.
- To leave the configuration unchanged, click **Reset**.

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:

- Creating Response Time Data Collections, page 3-33
- Editing Response Time Data Collections, page 3-34
- Deleting Response Time Data Collections, page 3-35

Creating Response Time Data Collections

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents, click **Response Time Monitoring**.

The Response Time Monitoring Setup table is displayed.

Step 4 Click **Create**.

The Response Time Monitoring Setup, Collection Configuration Dialog Box (Table 3-14) is displayed.

Step 5 Select the appropriate information.

Table 3-14 Response Time Monitoring Setup, Collection Configuration Dialog Box

Field	Description	Usage Notes
Data Source List	List of available data sources.	Select the data source from the list.
Report Interval (sec)	Number of seconds between reports.	Enter a number in seconds. The default is 1800.
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 15.
RspTime3 (msec)	Upper response time limit for the third bucket.	Enter a number in milliseconds. The default is 50.

Table 3-14 Response Time Monitoring Setup, Collection Configuration Dialog Box (continued)

Field	Description	Usage Notes
RspTime4 (msec)	Upper response time limit for the fourth bucket.	Enter a number in milliseconds. The default is 100.
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 3000.
Maximum Entries in Tables	The maximum number of rows in the report.	The default is 500.

Step 6 Do one of the following:

- To save the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Editing Response Time Data Collections

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents, click **Response Time Monitoring**.

The Response Time Monitoring Setup table is displayed.

Step 4 Select the data source to edit, then click **Edit**.

The Response Time Monitoring Setup, Collection Configuration Dialog Box(Table 3-14) is displayed.

Step 5 Make the necessary changes, then do one of the following:

- To accept the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Deleting Response Time Data Collections

To delete one or more response time data collections, simply select the data collections from the Response Time Monitoring Setup table, 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 3-37.

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents under DiffServ, click **Monitoring**.

The DiffServ Monitor Setup Dialog Box(Table 3-15) is displayed.

Step 4 Select the appropriate information.

Table 3-15 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.
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 5 Do one of the following:

- To accept the changes, click **Apply**.
- To leave the configuration unchanged, click **Reset**.

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 3-35.

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

- Creating a DiffServ Profile, page 3-37
- Editing a DiffServ Profile, page 3-38
- Deleting a DiffServ Profile, page 3-38

Creating a DiffServ Profile

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents under DiffServ, click **Profile**.

The DiffServ Monitor Profile Dialog Box is displayed.

Step 4 Click **Create**.

The DiffServ Profile Setup Dialog Box (Table 3-16) is displayed.

Step 5 Select the appropriate information.

Table 3-16 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.
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 6 Do one of the following:

- To save the changes, click **Submit**.
- To clear all the changes, click **Reset**.

Editing a DiffServ Profile

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents under DiffServ, click **Profile**.

The DiffServ Monitor Profile Table is displayed.

Step 4 Select the profile to edit, then click **Edit**.

The DiffServ Profile Setup Dialog Box (Table 3-16) is displayed.

Step 5 Make the necessary changes, then do one of the following:

- To save the changes, click **Submit**.
- To clear all the changes, click **Reset**.

Deleting a DiffServ Profile

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

Setting Up the 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 help you manage the protocol directory:

- Creating a Protocol, page 3-39
- Editing a Protocol, page 3-41
- Deleting a Protocol, page 3-42

Creating a Protocol

Step 1 Click the Setup tab.

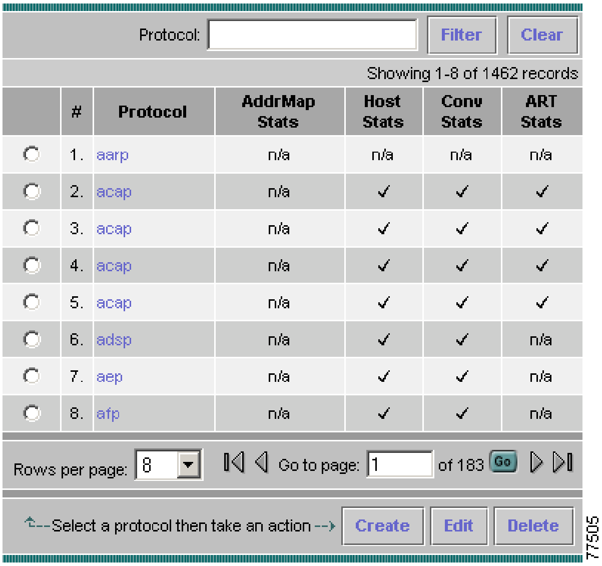
Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents, click **Protocol Directory**.

Protocol Directory Table (Figure 3-3) is displayed.

Figure 3-3 Protocol Directory Table



Protocol: Filter Clear

Showing 1-8 of 1462 records

	#	Protocol	AddrMap Stats	Host Stats	Conv Stats	ART Stats
○	1.	aarp	n/a	n/a	n/a	n/a
○	2.	acap	n/a	✓	✓	✓
○	3.	acap	n/a	✓	✓	✓
○	4.	acap	n/a	✓	✓	✓
○	5.	acap	n/a	✓	✓	✓
○	6.	adsp	n/a	✓	✓	n/a
○	7.	aep	n/a	✓	✓	n/a
○	8.	afp	n/a	✓	✓	n/a

Rows per page: 8 Go to page: 1 of 183

Select a protocol then take an action

Step 4 Click **Create**.

The Create New Protocol dialog box is displayed.

Step 5 Select an encapsulation method, then click **Submit**.

The New Protocol Parameters Dialog Box (Table 3-17) is displayed.

Step 6 Select the appropriate information.

Table 3-17 New Protocol Parameters Dialog Box

Field	Description	Usage Notes
Protocol Identification Value, such as: • IP Protocol • TCP Port • UDP Port	Numeric value used to identify the new protocol.	—
Name	Full name of the protocol.	—
Affected Stats	• Address Map • Host • Conversations • ART	Select the statistics the protocol should collect.

Step 7 Do one of the following:

- Click **Submit** to accept the changes.
- Click **Cancel** to leave the configuration unchanged.

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

Note 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 such as NetScout nGenius Real-Time Monitor. However, advanced users might want to monitor proprietary protocols or alter the normal settings for well-known protocols.

Step 1 Click the Setup tab.

Step 2 Click **Monitor**.

The Core Monitoring Functions table is displayed.

Step 3 In the contents, click **Protocol Directory**.

The Protocol Directory table is displayed.

Step 4 Select the protocol to edit, then click **Edit**.

The Edit Protocol Dialog Box (Table 3-18) is displayed.

Step 5 Make the necessary changes.

Table 3-18 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.	—
Encapsulation	Protocol encapsulation type.	—
Affected Stats	The statistics that can be collected for the protocol: • Address Map • Hosts • Conversations • ART	A statistic is grayed out if it is not available for the protocol.

Step 6 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 Alarm Thresholds

You can set up alarm thresholds on the NAM 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 NM-NAM devices.

These topics help you set up and manage alarm threshold settings:

- Setting NAM MIB Thresholds, page 3-43
- Setting Voice Thresholds, page 3-48
- Setting Up the Syslog, page 3-49
- Setting Switch Thresholds, page 3-50
- Setting NAM Trap Destinations, page 3-53

Setting NAM MIB Thresholds

NAM MIB thresholds are values you set that trigger alarms. Thresholds can be set on network hosts, MAC-layer hosts, network conversations, and MAC-layer conversations.

Note MAC-layer hosts and conversations are not available on NM-NAM devices.

	Wizard Page	Reference
Step 1	Select a Variable	"Selecting NAM MIB Variables" section on page 3-44
Step 2	Select Parameters	"Selecting NAM MIB Parameters" section on page 3-44

Selecting NAM MIB Variables

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

Step 3 The Thresholds Table is displayed.

Step 4 Click Create.

Step 5 The Alarms wizard is displayed. The following table shows the steps used to create NAM MIB thresholds.

	Wizard Page	Reference
Step 1	Select a Variable	"Selecting NAM MIB Variables" section on page 3-44
Step 2	Select Parameters	"Selecting NAM MIB Parameters" section on page 3-44

Selecting NAM MIB Parameters

Step 1 Select the alarm variables from the Variable list. The Variable list displays the MIB variables for which thresholds can be configured.

Step 2 Select the network protocol from the Network Protocol list, then click **Submit**.

The New Alarm Dialog Box (Table 3-19) is displayed.

Step 3 Select the appropriate information.

Table 3-19 New Alarm Dialog Box

Field	Description	Usage Notes
Data Source	Available data sources on the NAM.	Select the data source from the list.
Aggregate Group	Aggregate group of the selected DiffServ profile.	For DiffServ variables only.
Network Protocol	Selected protocol to be monitored.	This variable comes from Step 1 of the wizard.
Application Protocol	Application protocol to be monitored.	Select the application protocol from the list. For server and server-client response time variables only.
Variable	Selected variable to be monitored.	This variable comes from Step 1 of the wizard.
Server Address	Network address of the server.	For server and server-client response time variables only.
Client Address	Network address of the client.	For server-client response time variables only.
Network Address	Network address of host.	For network-layer host variables only.
MAC Address	MAC address of host.	For MAC-layer host variables only. **Note** MAC variables are not available on NM-NAMdevices.
Dst Address	Destination IP or MAC address of the host.	For MAC- or network-layer conversation variables only. **Note** MAC variables are not available on NM-NAM devices.
Src Address	Source IP or MAC address of the host.	For MAC- or network-layer conversation variables only. **Note** MAC variables are not available on NM-NAM devices.
Interval	Interval in seconds for the sampling period to last.	Enter a decimal value.
Description	Description of the alarm.	Must not exceed 128 characters.

Table 3-19 New Alarm Dialog Box (continued)

Field	Description	Usage Notes
Sample Type	Type of sampling to be done.	• Click **Absolute** for an alarm to be triggered by an absolute value that is reached. • Click the **Delta** for an alarm to be triggered by a change in the data rate.
Rising Threshold	Number of packets/octets that triggers the alarm. For response time alarms, it is the number of msec.	Enter a decimal number.
Falling Threshold	Number of packets/octets that triggers the alarm. For response time alarms, it is the number of msec.	Enter a decimal number.
Alarm Action	Action to be taken when the alarm is triggered.	• Click **Log** to log the event and display it in the Alarms tab. • Click **Trap** to send the event to traps. • Click **Log and Trap** to log the event and send it to traps.
Community	SNMP community to which traps are sent.	This community string must match the traps community string set in NAM traps.
Capture Trigger	Starts or stops the capture when the alarm threshold is triggered.	• Click **None** to disable Capture Triggers. • Click **Start** to start the capture when the alarm threshold is triggered. • Click **Stop** to stop the capture when the alarm threshold is triggered.

Step 4 Do one of the following:

- To accept the changes, click **Finish**.
- To leave the configuration unchanged, click **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 3-20) is displayed.

Table 3-20 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.
Description	Description of the alarm.
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.

Editing a NAM MIB Threshold

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed.

Step 3 Select the alarm to edit, then click **Edit**.

The Edit Alarm dialog box is displayed.

Step 4 Make the necessary changes.

Step 5 Do one of the following:

- To save the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Deleting a NAM MIB Threshold

To delete a NAM MIB threshold, simply select it from the Alarms table, then click **Delete**.

Setting Voice Thresholds

Voice threshold events can be logged locally on the NAM or sent to remote syslog hosts. For information on setting up syslogs, see the "Setting Up the Syslog" section on page 3-49.

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed.

Step 3 In the content, click **NAM Voice Thresholds**.

The Voice Alarms Dialog Box (Table 3-21) is displayed.

Step 4 Select the appropriate information.

Table 3-21 Voice Alarms Dialog Box

Protocol	Condition	Threshold
SCCP	Jitter Threshold—Select to monitor jitter.	Enter the threshold in milliseconds.
	Pkt Loss Threshold—Select to monitor the number of packets lost.	Enter the threshold as a percentage of total packets lost per call.

Table 3-21 Voice Alarms Dialog Box (continued)

Protocol	Condition	Threshold
H.323	Jitter Threshold—Select to monitor jitter	Enter the threshold in milliseconds.
	Pkt Loss Threshold—Select to monitor the number of packets lost.	Enter the threshold as a percentage of total packets lost per call.
MGCP	Jitter Threshold—Select to monitor jitter	Enter the threshold in milliseconds.
	Pkt Loss Threshold—Select to monitor the number of packets lost.	Enter the threshold as a percentage of total packets lost per call.

Step 5 Do one of the following:

- To save the changes, click **Apply**.
- To leave the configuration unchanged, click **Reset**.

Setting Up the Syslog

Syslogs are created for MIB threshold events, voice threshold events, or system alerts. The NAM maintains two syslog files, one for logging RMON threshold events (for MIB and voice threshold events) and one for logging local NAM system alerts.

You can specify whether syslog messages should be logged locally on the NAM, on a remote host, or both. You can use the NAM Traffic Analyzer to view the local NAM syslogs.

For information on viewing the syslogs, see Chapter 7, "Viewing Alarms." You can use a standard text editor to view syslogs on remote hosts.

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed.

Step 3 In the content, click **NAM Syslog**.

The Syslog Dialog Box (Table 3-22) is displayed.

Step 4 Make the necessary changes.

Table 3-22 Syslog Dialog Box

Field	Usage Notes
MIB Thresholds	• Select **Local** to log messages on your local system. • Select **Remote** to log messages on a remote system.
Voice	• Select **Local** to log voice threshold syslogs on your local system. • Select **Remote** to log voice threshold syslogs on a remote system.
System	• Select **Local** to log system alert syslogs on your local system. • Select **Remote** to log system alert syslogs on a remote system. • Select **Debug** to log debug messages from the application to the syslog.
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 (MIBs, Voice, and System).

Step 5 Do one of the following:

- To save the changes, click **Apply**.
- To leave the configuration unchanged, click **Reset**.

Setting Switch Thresholds

Note This section does not apply to NM-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 Switch Thresholds, page 3-51
- Editing Switch Thresholds, page 3-53
- Deleting Switch Thresholds, page 3-53

Creating Switch Thresholds

Note This section does not apply to NM-NAM devices.

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed.

Step 3 In the contents, click **Switch Thresholds**.

The Switch Threshold Alarms dialog box is displayed.

Step 4 Click **Create**.

The New Switch Alarm Dialog Box(Table 3-23) is displayed.

Table 3-23 New Switch Alarm Dialog Box

Field	Description	Usage Notes
Data Source List	Data source from the switch.	—
Variable	MIB variable to be sampled.	—
Interval (seconds)	Length of time, in seconds, for the sampling period to last.	Enter a decimal number.
Description	Description of the alarm.	Must not exceed 128 characters.
Sample Type	Type of sampling to be done.	• Click **Absolute** for an alarm to be triggered by an absolute value that is reached. • Click **Delta** for an alarm to be triggered by a change in the data rate.

Table 3-23 New Switch Alarm Dialog Box (continued)

Field	Description	Usage Notes
Rising Threshold	Number of packets/octets that trigger the alarm.	Enter a decimal number.
Falling Threshold	Number of packets/octets that trigger the alarm.	Enter a decimal number.
Alarm Action	Action to be taken when the alarm is triggered.	• Click **Log** to log the event and display it in the Alarms tab. • Click **Trap** to send the event to traps. • Click **Log and Trap** to log the event and send it to traps.
Community	SNMP community where traps are sent.	This community string must match the traps community string set on the switch.

Step 5 Do one of the following:

- To save the changes, click **Submit.**
- To leave the configuration unchanged, click **Reset**.

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 Switch Thresholds

Note This section does not apply to NM-NAM devices.

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed.

Step 3 In the content, click **Switch Thresholds**.

The Switch Threshold Alarms dialog box is displayed.

Step 4 Select the alarm to edit, then click **Edit**.

The Edit Alarm dialog box is displayed.

Step 5 Make the necessary changes, then do one of the following:

- To save the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Deleting Switch Thresholds

Note This section does not apply to NM-NAM devices.

To delete an existing switch threshold alarm, simply select it from the Switch 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 3-54
- Editing a NAM Trap Destination, page 3-55
- Deleting a NAM Trap Destination, page 3-55

Creating a NAM Trap Destination

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed

Step 3 In the content, click **NAM Trap Destinations**.

The Traps dialog box is displayed.

Step 4 Click **Create**.

The Create Trap Dialog Box (Table 3-24) is displayed.

Step 5 Enter the appropriate information.

Table 3-24 Create Trap Dialog Box

Field	Description
Community	The community string of the *alarm* community string set in the NAM MIB Thresholds.
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 6 Do one of the following:

- To save the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Editing a NAM Trap Destination

Step 1 Click the Setup tab.

Step 2 Click **Alarms**.

The Thresholds table is displayed

Step 3 In the contents, click **NAM Traps**.

The Traps dialog box is displayed.

Step 4 Select the trap to edit, then click **Edit**.

The Edit Trap dialog box is displayed.

Step 5 Make the necessary changes.

Step 6 Do one of the following:

- To save the changes, click **Submit**.
- To leave the configuration unchanged, click **Reset**.

Deleting a NAM Trap Destination

To delete an existing trap, simply select it from the Traps table, then click **Delete**.

Setting Global Preferences for All Users

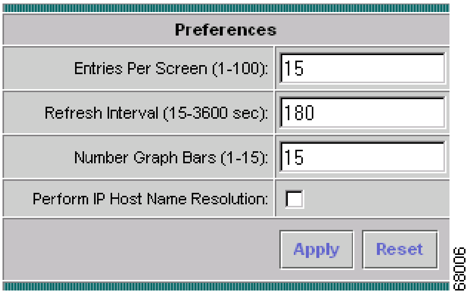
Global preferences settings apply to all users of the NAM and determine how data displays are formatted.

Step 1 Click the Setup tab.

Step 2 Click **Preferences**.

The Preferences Dialog Box (Figure 3-4) is displayed.

Figure 3-4 Preferences Dialog Box



Preferences

Entries Per Screen (1-100): 15

Refresh Interval (15-3600 sec): 180

Number Graph Bars (1-15): 15

Perform IP Host Name Resolution: □

Step 3 Enter or change the information described in the Preferences Dialog Box (Table 3-25).

Table 3-25 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. **Note** Enabling IP host name resolution without configuring nameservers might result in slow response times.

Step 4 Do one of the following:

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