CHAPTER 2

Setting Up The Cisco NAM

This chapter provides information about functions that will begin automatically, and other setup tasks you will need to perform for the Cisco NAM 5.1. For an overview of the setup for the NAM, which includes tasks not necessarily in the order in which you need to perform them, and many optional features, see Table 1-3 on page 1-18.

This chapter contains the following sections:

- Configuration Overview, page 2-2
- Default Functions, page 2-5
- Traffic, page 2-6
- Alarms, page 2-43
- Data Export, page 2-56
- Managed Device, page 2-62
- Network, page 2-65
- Classification, page 2-73
- Monitoring, page 2-80

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

Table 2-1, “Configuration Overview” leads you through the basic configuration steps you can follow for the Cisco NAM 5.1.

These are not necessarily in the order in which you need to perform them, and many are optional features.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>GUI Location</th>
<th>User Guide Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the NAM (upgrade is supported for platforms supported in NAM 5.0)</td>
<td>--</td>
<td>--</td>
<td>Platform-specific Installation and Configuration Guides (<a href="http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html</a>)</td>
</tr>
<tr>
<td>Configure the Managed Device Information</td>
<td>Traffic will populate on the dashboards if you have configured the managed device.</td>
<td>Setup &gt; Managed Device &gt; Device Information</td>
<td>See Managed Device, page 2-62.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Does not apply to the NAM-1 and NAM-2 blades.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up the System Time</td>
<td>You will need to set up the System Time correctly; if you do not have the time synchronized, then you will see either incorrect data or no data.</td>
<td>Administration &gt; System &gt; System Time</td>
<td>See System Time, page 5-5.</td>
</tr>
<tr>
<td>Verify that traffic has started</td>
<td>Traffic usage statistics for applications, hosts, conversations, VLANs, and DSCP are available on the Traffic Summary Dashboard. This will start automatically after the NAM is turned on and the system time is synched correctly.</td>
<td>Home (Traffic Summary Dashboard) or Monitor &gt; Overview &gt; Traffic Summary</td>
<td>See Traffic Analysis, page 2-5.</td>
</tr>
<tr>
<td>Verify that Application Response Time Metrics are being gathered</td>
<td>The NAM software provides response time measurements and various user-experience-related metrics, which are computed by monitoring and time-stamping packets sent from the user to the server providing services. This will start automatically after the NAM is turned on and the system time is synched correctly.</td>
<td>Analyze &gt; Response Time. You can view response times for applications, networks, servers, and clients.</td>
<td>See Application Response Time Metrics, page 2-5</td>
</tr>
</tbody>
</table>
## Chapter 2  Setting Up The Cisco NAM

### Configuration Overview

#### Verify that Voice/RTP Stream Traffic is being gathered
After the NAM is started, Voice/RTP stream traffic will automatically start being monitored. The NAM enables you to monitor all RTP stream traffic among all SPANed traffic, without having to know the signalling traffic used in negotiating the RTP channels.

This will start automatically after you turn on the NAM.

**GUI Location**
Analyze > Media > RTP Streams or Analyze > Media > Voice Call Statistics.

**User Guide Location**

#### Configure NDE Data Export
The NAM as a producer of NDE (NetFlow Data Export) packets was a new feature for NAM 5.0.

The NAM sends out NDE packets only in NDE v9 format.

**GUI Location**
Setup > Data Export > NetFlow

**User Guide Location**
See NetFlow, page 2-56.

#### Configure sites
A site is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems.

If you want to limit the view of your network data to a specific city, a specific building, or even a specific floor of a building, you can use the Sites function.

We recommend that sites are configured using prefix-based subnets instead of based on data source.

**GUI Location**
Setup > Network > Sites

**User Guide Location**
See Sites, page 2-65.

#### Define Alarms and Thresholds
Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose for what types of events you want the NAM to notify you, and how you want to be notified.

Alarms that will be used for Thresholds should be created first, then the Thresholds created second.

**GUI Location**
Setup > Alarms > Actions and Setup > Alarms > Thresholds

**User Guide Location**
See Alarm Actions, page 2-44. See Thresholds, page 2-46.

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

**GUI Location**
Capture > Packet Capture/Decode

**User Guide Location**
See Chapter 4, “Capturing and Decoding Packet Data.”
Chapter 2      Setting Up The Cisco NAM

### Configuration Overview

Some of the Cisco NAM 5.1 features require configuration of sites. A **site** is a collection of hosts, or network endpoints, partitioned into views that help you monitor traffic and troubleshoot problems (see *Sites, page 2-65* for more detailed information). These features include those in which the NAM provides measurements of application performance on networks where WAAS devices are deployed, and dashboards that show traffic levels between sites and alarms levels per site. All other NAM features can still be used without defining any sites (the default configuration).

If you have set up sites, you will be able to select a particular site to view in the Interactive Report and view data relevant to that site only. In some cases, you can select both a Client Site and a Server Site to view data pertaining to interaction between hosts at different sites.

### Configuring and Viewing Data

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Scheduled Export</td>
<td>You can set up scheduled jobs that will generate a daily report at a specified time, in the specified interval, and then e-mail it to a specified e-mail address.</td>
</tr>
<tr>
<td><em>GUI Location</em></td>
<td>In the Interactive Report (left side of the dashboard), click the <strong>Export</strong> button.</td>
</tr>
<tr>
<td><em>User Guide Location</em></td>
<td>See <a href="#">Scheduled Exports, page 2-60</a>.</td>
</tr>
<tr>
<td>Set up Northbound API</td>
<td>NBI (Northbound Interface), also referred to as API (Application Programming Interface), enables partners and customers to provision the NAM and extract performance data. You can write your own scripts based on the NAM Northbound API, but there is setup in the NAM GUI needed.</td>
</tr>
<tr>
<td><em>GUI Location</em></td>
<td>For application developers who want to use the NAM APIs to provision network services and leverage data, see the <em>Cisco Network Analysis Module API Programmer’s Guide, 5.1</em>.</td>
</tr>
<tr>
<td>Set up TACACS+ server</td>
<td>TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization. When a user logs into the NAM, TACACS+ determines if the username and password are valid and what the access privileges are.</td>
</tr>
<tr>
<td><em>GUI Location</em></td>
<td>Administration &gt; Users &gt; TACACS+</td>
</tr>
<tr>
<td><em>User Guide Location</em></td>
<td>See <a href="#">Configuring a TACACS+ Server to Support NAM Authentication and Authorization, page 5-20</a>.</td>
</tr>
<tr>
<td>Change System Preferences</td>
<td>You can change many preferences, such as refresh interval, Top N Entries, Data Displayed, and enabling Audit Trail, as needed.</td>
</tr>
<tr>
<td><em>GUI Location</em></td>
<td>Administration &gt; System &gt; Preferences</td>
</tr>
<tr>
<td><em>User Guide Location</em></td>
<td>See Chapter 5, “User and System Administration.”</td>
</tr>
</tbody>
</table>

---

Some of the Cisco NAM 5.1 features require configuration of sites. A **site** is a collection of hosts, or network endpoints, partitioned into views that help you monitor traffic and troubleshoot problems (see *Sites, page 2-65* for more detailed information). These features include those in which the NAM provides measurements of application performance on networks where WAAS devices are deployed, and dashboards that show traffic levels between sites and alarms levels per site. All other NAM features can still be used without defining any sites (the default configuration).

If you have set up sites, you will be able to select a particular site to view in the Interactive Report and view data relevant to that site only. In some cases, you can select both a Client Site and a Server Site to view data pertaining to interaction between hosts at different sites.
Cisco WAAS NAM Virtual Service Blade

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

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

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

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

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

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

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

### Default Functions

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

- Traffic Analysis, page 2-5
- Application Response Time Metrics, page 2-5
- Voice Signaling/RTP Stream Monitoring, page 2-6
- Traffic Usage Statistics, page 2-6

### Traffic Analysis

Traffic usage statistics for applications, hosts, conversations, VLANs, and DSCP will begin populating on the Traffic Summary dashboard (Monitor > Overview > Traffic Summary).

### Application Response Time Metrics

The NAM software provides response time measurements and various user-experience-related metrics, which are computed by monitoring and time-stamping packets sent from the user to the server providing services.

These Application Response Time Metrics are available to view under the menu Analyze > Response Time. You can view response times for applications, networks, servers, and clients.

After the NAM is started, these metrics will begin to populate.
Voice Signaling/RTP Stream Monitoring

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

Note

This is not supported on the NAM on Nexus 1010.

When RTP Stream Monitoring is enabled, the NAM:

- Identifies all RTP streams among the SPANed traffic
- Monitors the identified RTP traffic
- Sends syslog, trap, e-mail, and trigger captures for RTP streams that violate stream statistics thresholds on the following metrics:
  - Number of Consecutive Packet Loss
    Each RTP packet has an RTP header that contains a sequence number. The sequence number increments by one for each RTP packet received in the same RTP stream. A gap in the sequence numbers identifies a packet loss. If the gap in sequence numbers jump is more than the threshold, the NAM raises an alarm condition.
  - Packet Loss percent
    There are two types of percent packet loss percent: Adjusted Packet Loss and Actual Packet Loss. Actual Packet Loss indicates expected packets that never appear in the NAM. Adjusted Packet Loss includes actual packets lost and packets that arrive with large delay beyond the expected buffer capacity of the endpoint.
  - Jitter: Packets delay compare to the expected receiving time
  - Concealment Seconds: Seconds in which there is one or more packet lost
  - Severe Concealment Seconds: Seconds in which there is more than 5% of packet lost

You can set up thresholds at Setup > Alarms > Thresholds.

You can define filter entries to narrow down to the subset of RTP streams so the NAM monitors only those RTP streams matching the filter criteria.

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

Traffic Usage Statistics

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

Traffic

The NAM 5.1 menu selections for setting up Traffic are:
SPAN

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic.

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

- **About SPAN Sessions, page 2-7**
- **Creating a SPAN Session, page 2-10**
- **Editing a SPAN Session, page 2-11**
- **Deleting a SPAN Session, page 2-12**

**Note**

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

**About SPAN Sessions**

**Note**

This does not apply to the NAM Virtual Service Blades.

Depending on the IOS running on the Supervisor, port names are displayed differently. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the VSS, a port name might be displayed as Gi1/2/1 to represent a Gigabit port on switch 1, 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.

WS-SVC-NAM-1 devices can have only one active SPAN session. You can select a switch port or EtherChannel as the SPAN source; however, you may select only one SPAN type. 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 Table 2-2, Methods of Directing Traffic.
Table 2-2  Methods of Directing Traffic

<table>
<thead>
<tr>
<th>Method</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch SPAN</td>
<td>You can direct a set of physical ports, a set of VLANs, or a set of EtherChannels to the NAM.</td>
</tr>
<tr>
<td></td>
<td>Selecting an EtherChannel as a SPAN source is the same as selecting all physical ports comprising the EtherChannel as the SPAN source.</td>
</tr>
<tr>
<td>Switch Remote SPAN (RSPAN)</td>
<td>You can monitor packet streams from remote switches, assuming that all traffic from a remote switch arrives at the local switch on a designated RSPAN VLAN. Use the RSPAN VLAN as the SPAN source for the NAM.</td>
</tr>
</tbody>
</table>
| 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. For received NDE traffic, a default site will be created including all interfaces from that device. See Sites, page 2-65.

SPAN and NDE sources can be in effect simultaneously.

Note: Starting with NAM release 5.0, in addition to being a consumer of NDE records, the NAM is also a producer of NDE data packets.

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

Table 2-3  SPAN Sources

<table>
<thead>
<tr>
<th>SPAN Source</th>
<th>Configured with one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any set of physical ports</td>
<td>• NAM (the NAM GUI)</td>
</tr>
<tr>
<td></td>
<td>• Switch CLI</td>
</tr>
<tr>
<td></td>
<td>• Supervisor portCopyTable (SNMP)</td>
</tr>
<tr>
<td>Any EtherChannel</td>
<td>• NAM (the NAM GUI)</td>
</tr>
<tr>
<td></td>
<td>• Switch CLI</td>
</tr>
<tr>
<td></td>
<td>• Supervisor portCopyTable (SNMP)</td>
</tr>
<tr>
<td>Any set of VLANs configured on the local switch</td>
<td>• NAM (the NAM GUI)</td>
</tr>
<tr>
<td></td>
<td>• Switch CLI</td>
</tr>
<tr>
<td></td>
<td>• Supervisor portCopyTable (SNMP)</td>
</tr>
</tbody>
</table>

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

Table 2-4  Active SPAN Sessions Dialog

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>Monitor session ID of the SPAN.</td>
</tr>
<tr>
<td>Note</td>
<td>For switches running Cisco IOS software only.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of SPAN source</td>
</tr>
</tbody>
</table>
Table 2-4 Active SPAN Sessions Dialog (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td>Source of the SPAN session. When creating a SPAN session, you can select all ports regardless of their state. See Table 2-5, Possible SPAN States for a description of the possible SPAN states.</td>
</tr>
<tr>
<td><strong>Dest. Port</strong></td>
<td>Destination port of the SPAN session.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>Direction of the SPAN traffic.</td>
</tr>
</tbody>
</table>
| **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**     | 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** | Add NAM Port 1 to the selected SPAN session as a SPAN destination. This button is labeled Add Dest. Port on the WS-SVC-NAM-1. |
| **Add Dest. Port 2** | Add NAM Port 2 to the selected SPAN session as a SPAN destination. This option is not available on the WS-SVC-NAM-1. |
| **Edit**       | Edit the selected SPAN session.                                              |
| **Delete**     | Delete the selected SPAN session.                                            |
| **Refresh**    | Update the SPAN session information.                                         |

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

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

To create a SPAN session on a switch:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**. The SPAN window displays as shown in **Figure 2-1**.

**Figure 2-1  SPAN Sessions**

<table>
<thead>
<tr>
<th>Monitor Session</th>
<th>Type</th>
<th>Source</th>
<th>Dest. Port</th>
<th>Direction</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>port</td>
<td>Te3/1</td>
<td>Te3/5</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>port</td>
<td>Te3/1</td>
<td>GE1/1</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>3</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>4</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>5</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>6</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>7</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
<tr>
<td>8</td>
<td>port</td>
<td>Te3/1</td>
<td>GbE/S2</td>
<td>Both</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

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

**Step 3** Select the appropriate information.
**Table 2-6 Create SPAN Session Dialog**

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

**Step 4** To create the SPAN session, click Submit. The Active Sessions window displays.

**Step 5** To save the current active SPAN session in the running-configuration to the startup-configuration for switches running Cisco IOS software only, click Save in the active SPAN session window.

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

**Step 6** To verify the SPAN session was created and to view the data, go to the Top N charts on the Traffic Analysis dashboard (Monitor > Overview > Traffic Summary).

**Editing a SPAN Session**

You can only edit SPAN sessions that have been directed to the NAM.
Note: Editing an existing SPAN session that has multiple SPAN destinations will affect all destinations.

To edit a SPAN session:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**. The Active SPAN Sessions dialog box displays.

**Step 2** Select the SPAN session to edit, then click **Edit**. The Edit SPAN Session Dialog Box displays. The fields are described in Table 2-7, *Edit SPAN Session Dialog Box*.

**Step 3** Make the appropriate changes.

### Table 2-7 Edit SPAN Session Dialog Box

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

**Deleting a SPAN Session**

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

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

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

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

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

Note

If you have configured sites (see Sites, page 2-65), you can assign data sources to that particular site. If you do this, and you also configure data sources, the two could overlap since sites can also be a primary “view” into data sources. If there is a mismatch between the two, you will not see any data.

Note

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

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

- SPAN, page 2-14
- ERSPAN, page 2-14
- VACL, page 2-21
- NetFlow, page 2-22
- WAAS, page 2-32
- Performance Agent, page 2-39

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

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

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

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure up to two SPAN sessions in a Catalyst 6500 or 7600 Routers chassis.

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

ERSPAN

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

As an ERSPAN consumer, the NAM can receive ERSPAN packets on its management port from devices such as Cisco routers and switches. Those packets are analyzed as if that traffic had appeared on one of the NAM data ports. The NAM supports ERSPAN versions 1 and 3. Incoming ERSPAN data is parsed by the NAM, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

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

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

- Enabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 2-14
- Enabling Autocreation of ERSPAN Data Sources Using the CLI, page 2-15
- Disabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 2-15
- Disabling Autocreation of ERSPAN Data Sources Using the CLI, page 2-15
- Creating ERSPAN Data Sources Using the Web GUI, page 2-16
- Creating ERSPAN Data Sources Using the CLI, page 2-16
- Deleting ERSPAN Data Sources Using the Web GUI, page 2-18
- Deleting ERSPAN Data Sources Using the CLI, page 2-18
- Configuring ERSPAN on Devices, page 2-19

Enabling Autocreation of ERSPAN Data Sources Using the Web GUI

There is a convenient “autocreate” feature for data sources, which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device that sends ERSPAN traffic to the NAM, after the first packet is received. Manual creation of ERSPAN data sources using the NAM GUI or the CLI is typically not necessary. When manually creating a data source, you may specify any name you want for the data source. A data source entry must exist on the NAM in order for it to accept ERSPAN packets from an external device.

Autocreated ERSPAN data sources will be assigned a name in the format ERSPAN-<IP Address>-ID-<Integer>, where IP Address is the IP address of the sending device, and Integer is the Session-ID of the ERSPAN session on that device. For example, device 192.168.0.1 sending ERSPAN packets with the Session ID field set to 12 would be named “ERSPAN-192.168.0.1-ID-12.” You can edit these autocreated data sources and change the name if desired.
One device can be configured to send multiple separate ERSPAN sessions to the same NAM. Each session will have a unique Session ID. The NAM can either group all sessions from the same device into one data source, or have a different data source for each Session ID. When data sources are autocreated, they will be associated with one particular Session ID. When manually created, you can instruct the NAM to group all traffic from the same device into one data source. If you check the Session check box, and enter a Session ID in the Value field, the data source will only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

To configure the NAM to automatically create data sources when it receives ERSPAN packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

| Step 1 | Choose Setup > Traffic > NAM Data Sources. |
| Step 2 | Click the Auto Create button on the bottom left of the window. |
| Step 3 | Check the ERSPAN check box to toggle autocreation of ERSPAN data sources to “on”. |
| Step 4 | Click the Submit button. |

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

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

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

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

The NAM will now automatically create a ERSPAN data source for each device that sends ERSPAN packets to it. The data source will have the specific Session ID that is populated by the device in the ERSPAN packets sent to the NAM. If the same device happens to send ERSPAN packets to the NAM with different Session ID values, a separate data source will be created for each unique Session ID sent from the device.

**Disabling Autocreation of ERSPAN Data Sources Using the Web GUI**

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

**Disabling Autocreation of ERSPAN Data Sources Using the CLI**

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

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

To manually configure a ERSPAN data source on the NAM using the GUI, for example if the autocreation feature is turned off, use the following steps:

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

**Step 2** Click the Create button along the bottom of the window.

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

**Step 4** Enter the IP address of the device that will export ERSPAN to the NAM.

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

**Step 6** (Optional) Check the Session check box and enter an Session ID into the Value field if the data source should only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

Devices can be configured with multiple ERSPAN Sessions. The packets exported may have the same source IP address, but the Session ID exported will be a different for each session. If you want to include only one Session in the data source, you must check the “Session” box and provide the value of that Session ID.

**Step 7** Click the Submit button.

Creating ERSPAN Data Sources Using the CLI

To manually configure a ERSPAN data source on the NAM using the CLI (for example if the autocreation feature is turned off), use the following steps. Note that when using the CLI, there are two separate phases involved: First, you must create a “device” entry on the NAM and remember the device ID, and then you must create a data source entry using this device ID. In the NAM GUI, these two phases for creating ERSPAN data sources are combined together.

**Step 1** Enter the command `device erspan`. You will now be in erspan device subcommand mode as shown here:

```plaintext
root@172-20-104-107.cisco.com# device erspan

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

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

**Step 2** Enter `?` to see all the command options available, as in the example below:

```plaintext
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                        - display help
address                  - device IP address (*)
cancel                   - discard changes and exit from subcommand mode
exit                     - create device and exit from sub-command mode
help                     - display help
show                     - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.
```
Step 3  Enter the IP address of the device as shown in this example (required):
root@172-20-104-107.cisco.com(sub-device-erspan)# address 192.168.0.1

Step 4  Type show to look at the device configuration that will be applied and verify that it is correct:
root@172-20-104-107.cisco.com(sub-device-erspan)# show
DEVICE TYPE : ERSPAN (Encapsulated Remote SPAN)
DEVICE ADDRESS : 192.168.0.1

Step 5  Type exit to come out of the subcommand mode and create the device. Remember the ID value that was assigned to the new device (you will need it to create the data source).
root@172-20-104-107.cisco.com(sub-device-erspan)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#

Step 6  Enter the command data-source erspan. You will now be in erspan data source subcommand mode as shown here:
root@172-20-104-107.cisco.com# data-source erspan

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

Step 7  Enter ? to see all the command options available, as in the example below:
root@172-20-104-107.cisco.com(sub-data-source-erspan)# ?
?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - erspan device ID (*)
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
session-id                - erspan Session ID
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

Step 8  Enter the device ID from Step 4.
root@172-20-104-107.cisco.com(sub-data-source-erspan)# device-id 1

Step 9  Enter the name you would like for the data source (required):
root@172-20-104-107.cisco.com(sub-data-source-erspan)# name MyFirstErspanDataSource

Step 10 If desired, supply the specific Session ID for this ERSPAN data source (optional):
root@172-20-104-107.cisco.com(sub-data-source-erspan)# session-id 123

Step 11 Enter show to look at the data source configuration that will be applied and verify that it is correct:
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show
DATA SOURCE NAME : MyFirstErspanDataSource
DATA SOURCE TYPE : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID : 1
DEVICE ADDRESS : 192.168.0.1
SESSION ID : 123

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

Step 12 Enter exit to come out of the subcommand mode and create the data source:
root@172-20-104-107.cisco.com(sub-data-source-erspan)# exit
Data source created successfully, ID = 3

The data source is now created, and ERSPAN records from the device will be received and accepted by the NAM as they arrive.

Deleting ERSPAN Data Sources Using the Web GUI

To delete an existing ERSPAN data source, use the following steps. Note that if the autocreation feature is turned on, and the device continues to send ERSPAN packets to the NAM, the data source will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

Step 1 Choose Setup > Traffic > NAM Data Sources.
Step 2 Choose the data source you would like to delete.
Step 3 Click the Delete button along the bottom of the window.

Deleting ERSPAN Data Sources Using the CLI

To delete an ERSPAN data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.

Step 1 Show all data sources so you can find the ID of the one you want to delete:
root@172-20-104-107.cisco.com# show data-source

DATA SOURCE ID : 1
DATA SOURCE NAME : DATA PORT 1
TYPE : Data Port
PORT NUMBER : 1
---------

DATA SOURCE ID : 2
DATA SOURCE NAME : DATA PORT 2
TYPE : Data Port
PORT NUMBER : 2
---------
DATA SOURCE ID : 3
DATA SOURCE NAME : MyFirstErspanDataSource
TYPE            : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID       : 2
DEVICE ADDRESS  : 192.168.0.1
ENGINE ID       : 123

-------------

root@172-20-104-107.cisco.com#

Step 2 Use the no data-source command to delete the data source:

root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#

Step 3 Show all devices so you can find the ID of the one you want to delete:

root@172-20-104-107.cisco.com# show device

DEVICE ID            : 1
DEVICE TYPE          : ERSPAN (Encapsulated Remote SPAN)
IP ADDRESS           : 192.168.0.1
INFORMATION          : No packets received
STATUS               : Inactive
-------

root@172-20-104-107.cisco.com#

Step 4 Use the no device command to delete the device:

root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#

Note that if the autocreation mode is on, and the device continues to send ERSPAN packets to the NAM, the data source (and device entry) will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

Configuring ERSPAN on Devices

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

- Sending ERSPAN Data to Layer 3 Interface, page 2-19
- Sending ERSPAN Data Directly to the NAM Management Interface, page 2-20

Sending ERSPAN Data to Layer 3 Interface

To send the data to a layer 3 interface on the Switch housing the NAM, configure the ERSPAN source session. The ERSPAN destination session then sends the traffic to a NAM data-port. After performing this configuration, you can select the DATA PORT X data source to analyze the ERSPAN traffic.

Note This method causes the ERSPAN traffic to arrive on one of the NAM data ports, which is the most efficient method and will not have any adverse effect on the NAM’s IP connectivity. Therefore, we recommend this method.
Sample Configuration of ERSPAN Source

monitor session 1 type erspan-source
  no shut
source interface Fa 3/47
destination
  erspan-id N
    ip address aa.bb.cc.dd
    origin ip address ee.ff.gg.hh

Where:
- \textit{erspan-id N} is the ERSPAN ID
- \textit{aa.bb.cc.dd} is the IP address of the destination switch (loopback address or any routable IP address)
- \textit{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:
- \textit{erspan-id N} matches the ERSPAN ID at the source switch
- \textit{aa.bb.cc.dd} is the IP address defined at the destination

You can now connect to the NAM to monitor and capture traffic of the Data Port 2 data source.

Sending ERSPAN Data Directly to the NAM Management Interface

To send the data directly to the NAM management IP address (management-port), configure the ERSPAN source session. No ERSPAN destination session configuration is required. After performing this configuration on the Catalyst 6500 switch or Cisco 7600 series router, when ERSPAN packets are sent to the NAM, it will automatically create a data source for that packet stream. If the autocreate feature is not enabled, you will have to manually create the data source for this ERSPAN stream of traffic (see Creating ERSPAN Data Sources Using the Web GUI, page 2-16).

\textbf{Note}

This method causes the ERSPAN traffic to arrive on the NAM management port. If the traffic level is high, this could have negative impact on the NAM’s performance and IP connectivity.

Sample Configuration

monitor session 1 type erspan-source
  no shut
source interface Fa3/47
destination
  erspan-id Y
    ip address aa.bb.cc.dd
    origin ip address ee.ff.gg.hh

Where:
- Interface fa3/47 is a local interface on the erspan-source switch to be monitored
- \textit{Y} is any valid span session number
- \textit{aa.bb.cc.dd} is the management IP address of the NAM
• *ee.ff.gg.hh* is the source IP address of the ERSPAN traffic

**VACL**

A VLAN access control (VACL) list can forward traffic from either a WAN interface or VLANs to a data port on the NAM. A VACL provides an alternative to using SPAN; a VACL can provide access control based on Layer 3 addresses for IP and IPX protocols. The unsupported protocols are access controlled through the MAC addresses. A MAC VACL cannot be used to access control IP or IPX addresses.

**Configuring VACL on a WAN Interface**

Because WAN interfaces do not support the SPAN function, you must use the switch CLI to manually configure a VACL in order to monitor WAN traffic with the NAM. This feature only works for IP traffic over the WAN interface.

VACL can also be used 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.

The following example shows how to configure a VACL on an ATM WAN interface and forward both ingress and egress traffic to the NAM. These commands are for switches running Cisco IOS version 12.1(13)E1 or higher. For more information on using these features, see your accompanying switch documentation.

```plaintext
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:

```plaintext
Cat6509#show cwan vlan
```

After you have the VLAN ID, configure the NAM data port using the following command:

```plaintext
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:

```plaintext
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)#exit
Cat6509#(config)#vlan access-map lan 200
Cat6509#(config-access-map)#match ip address 100
Cat6509#(config-access-map)#action forward
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan filter lan vlan-list 1
Cat6509#(config)#analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509#(config)#analysis module 3 data-port 1 capture
Cat6509#(config)#exit
```

### NetFlow

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

As a consumer, the NAM can receive NetFlow packets on its management port from devices such as Cisco routers and switches. Those records are stored in its collection database as if that traffic had appeared on one of the NAM data ports. The NAM understands NetFlow v1, v5, v6, v7, v8, and v9. Incoming NetFlow data is parsed by the NAM, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

For the NAM to receive NetFlow packets from an external switch or router, that device must be configured by export flow records to the NAM’s IP address and the correct UDP port number. The default port number on which the NAM listens for NetFlow packets is port 3000. This can be modified using the NAM CLI, but the important point is that the same port must be configured on the NAM and the exporting device(s). Depending on the external device, you may need to enable the NetFlow feature on a per-interface basis.

See the following sections about NetFlow as a data source:

- Understanding NetFlow Interfaces, page 2-22
- Understanding NetFlow Flow Records, page 2-23
- Managing NetFlow Data Sources, page 2-24
- Configuring NetFlow on Devices, page 2-24

### Understanding NetFlow Interfaces

To use a device as an NDE data source for the NAM, you must configure the device itself to export NDE packets to UDP port 3000 on the NAM. You might need to configure the device itself on a per-interface basis. An NDE device is identified by its IP address. In the NAM, the default UDP port of 3000 can be changed with a NAM CLI command (see Configuring NetFlow on Devices, page 2-24).

You can define additional NDE devices by specifying the IP addresses and (optionally) the community strings. Community strings are used to upload convenient text strings for interfaces on the managed devices that are monitored in NetFlow records.
Remote NDE devices may export information pertaining to any or all of their individual interfaces. The NAM keeps track of the interface associated with any flow information received from the device. On the NDE Interface Analysis page (Analyze > Traffic > NDE Interface), you can view information for any selected interface on the device. This page will display the interface utilization or throughput over time, as well as show the top Applications, Hosts, and DSCP groups in both the input and output directions for the interface.

Understanding NetFlow Flow Records

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

- Input SNMP ifIndex
- Output SNMP ifIndex

This information might not be available because of NDE feature incompatibility with your Cisco IOS version, or because of an NDE flow-mask configuration.

In most cases, turning on NetFlow on an interface populates the NetFlow cache in the device with flows that are in the input direction of the interface. As a result, the input SNMP ifIndex field in the flow record has the ifIndex of the interface on which NetFlow was turned on. Sample NetFlow Network, Figure 2-2, shows a sample network configuration with a NetFlow router.

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

<table>
<thead>
<tr>
<th>Input Interface</th>
<th>Output Interface</th>
<th>Are Flows Reported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>Yes</td>
</tr>
<tr>
<td>a</td>
<td>c</td>
<td>Yes</td>
</tr>
<tr>
<td>b</td>
<td>c</td>
<td>No</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>No</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>No</td>
</tr>
<tr>
<td>c</td>
<td>b</td>
<td>No</td>
</tr>
</tbody>
</table>
Managing NetFlow Data Sources

A data source entry must exist on the NAM in order for it to accept NetFlow records from an external device. Data source entries may be created manually using the NAM web GUI or the CLI. When manually creating a data source, you may specify any name you want for the data source.

For convenience, manual creation of NetFlow data sources is not necessary. There is an “autocreate” feature which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device which sends NDE traffic to the NAM when the first packet is received.

Autocreated NetFlow data sources will be assigned a name in the format NDE-<IP Address>-ID-<Integer>, where <IP Address> is the IP address of the exporting device, and <Integer> is the Engine-ID that the device populates in the packets (part of the NetFlow Data Export standard). An example might be “NDE-192.168.0.1-ID-12” for device 192.168.0.1 sending NDE packets with the Engine ID field set to 12. You can edit these autocreated data sources and change the name if you want to, as well as optionally specifying SNMP credentials for the device, as described later in this guide.

Configuring NetFlow on Devices

The configuration commands for NetFlow devices to export NDE packets to the NAM are platform and device specific. The example configuration commands provided here are the ones most commonly found for devices running Cisco IOS. For more detailed information, see your device documentation.

For Devices Running Cisco IOS

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

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

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

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

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

For Devices Supporting Multi-Layer Switching Cache Running Cisco IOS

Step 1   Select the version of NDE.

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

Note   The NAM supports NDE versions 1, 5, 6, 7, 8, and 9 aggregation caches.
Step 2  Select NDE flow mask.
Prompt(config)# mls flow ip full

Step 3   Enable NetFlow export.
Prompt(config)# mls nde sender

Step 4   Export NetFlow to UDP port 3000 of the NAM.
Prompt(config)# ip flow-export destination <NAM IP address> 3000

For Devices Supporting NDE v8 Aggregations Running Cisco IOS

Step 1  Select a v8 aggregation.
Prompt(config)# ip flow-aggregation cache <aggregation-type>

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

Step 2  Enable the aggregation cache.
Prompt(config-flow-cache)# enable

Step 3  Export the flow entries in the aggregation cache to NAM UDP port 3000.
Prompt(config-flow-cache)#export destination <NAM address> 3000

For Devices That Support NDE Export From Bridged-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.
Step 3
Enable NDE export.
Prompt> (enable) set mls nde enable

Step 4
Export the NDE packets to the NAM.
Prompt> (enable) set snmp extended rmon netflow enable <NAM-slot>

Enabling Autocreation of NetFlow Data Sources Using the Web GUI

To configure the NAM to automatically create data sources when it receives NDE packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

Step 1
Choose Setup > Traffic > NAM Data Sources.

Step 2
Click the Auto Create button on the bottom left of the window.

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

Step 4
Click the Submit button.

Enabling Autocreation of NetFlow Data Sources Using the CLI

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

To configure the NAM to automatically create data sources when it receives NDE packets from an external device, use the following steps:

Use the autocreate-data-source command as follows:

root@172-20-104-107.cisco.com# autocreate-data-source netflow
NDE data source autocreate successfully ENABLED

The NAM will now automatically create a NetFlow data source for each device that sends NetFlow packets to it. The data source will have the specific Engine ID that is populated by the device in the NDE packets sent to the NAM. If the same device happens to send NDE packets to the NAM with different Engine ID values, a separate data source will be created for each unique Engine ID sent from the device.

Disabling Autocreation of NetFlow Data Sources Using the Web GUI

Step 1
Choose Setup > Traffic > NAM Data Sources.

Step 2
Click the Auto Create button on the bottom left of the window.

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

Step 4
Click the Submit button.
Disabling Autocreation of NetFlow Data Sources Using the CLI

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

```
root@172-20-104-107.cisco.com# no autocreate-data-source netflow
NDE data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

Creating NetFlow Data Sources Using the Web GUI

To manually configure a NetFlow data source on the NAM using the GUI, for example if the autocreation feature is turned OFF, use the following steps:

---

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

**Step 2** Click the Create button along the bottom of the window.

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

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

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

**Step 6** (Optional) If you know the specific value of the Engine ID on the device you would like to monitor, check the Engine check box, and enter the value of the Engine ID. If the Engine check box is left unchecked, then all NDE records exported by the device will be grouped into the same data source, regardless of the Engine ID populated in the NDE packets (in most cases the Engine check box can be left blank and you don’t have to worry about the Engine ID value).

Some devices have multiple Engines which independently export NDE records. For example, on some Cisco routers, NDE records can be exported by the Supervisor module as well as individual line cards. The packets exported may have the same source IP address, but the Engine ID exported by the Supervisor will be a different value than the Engine ID(s) exported by the line card(s). If you want to include only one Engine in the data source, you must check the “Engine” box and provide the value of that Engine ID.

**Step 7** (Optional) SNMP v1/v2c RO Community String: If SNMP v1 or v2c will be used to communicate with the device, enter the community string that is configured on the device that is going to export NetFlow packets to the NAM.

**Step 8** (Optional) “Enable SNMP v3”: If SNMP v3 will be used to communicate with the device, fill in the fields within the v3-specific dialog.

**Step 9** (Optional) If desired, fill in the SNMP credentials for the device. If valid SNMP credentials are provided, the NAM can upload readable text strings from the device to describe the interfaces on that device rather than just displaying the interfaces as numbers. You may specify either SNMPv2c or SNMPv3 credentials. See Table 2-10, SNMP Credentials.

---

**Table 2-10 SNMP Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode: No Auth, No Priv</td>
<td>SNMP will be used in a mode with no authentication and no privacy.</td>
</tr>
<tr>
<td>Mode: Auth, No Priv</td>
<td>SNMP will be used in a mode with authentication, but no privacy.</td>
</tr>
<tr>
<td>Mode: Auth and Priv</td>
<td>SNMP will be used in a mode with both authentication and privacy.</td>
</tr>
</tbody>
</table>
Creating NetFlow Data Sources Using the CLI

To manually configure a NetFlow data source on the NAM using the CLI, for example if the autocreation feature is turned off, use the following steps. Note that when using the CLI, there are two separate phases involved. First you must create a “device” entry on the NAM and remember the device ID. Then you must create a data source entry using this device ID. For convenience, these two phases are combined together when using the GUI to create NetFlow data sources.

Step 1  Enter the command `device netflow`. You will now be in netflow device subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# device netflow
```

Entering into subcommand mode for this command.
Type ‘exit’ to apply changes and come out of this mode.
Type ‘cancel’ to discard changes and come out of this mode.

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

Step 2  Enter `?` to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
  ?                      - display help
  address                - device IP address (*)
  cancel                 - discard changes and exit from subcommand mode
  community              - SNMPv2c community string
  exit                   - create device and exit from sub-command mode
  help                   - display help
  show                   - show current config that will be applied on exit
  snmp-version           - SNMP version to use to communicate with device
  v3-auth-passphrase     - SNMPv3 authentication passphrase
  v3-auth-protocol       - SNMPv3 authentication protocol
  v3-priv-passphrase     - SNMPv3 privacy passphrase
  v3-priv-protocol       - SNMPv3 privacy protocol
  v3-sec-level           - SNMPv3 security level
  v3-username            - SNMPv3 username
```

Step 10  Click the Submit button.
Chapter 2      Setting Up The Cisco NAM

Welcome to the Cisco NAM.,

Traffic

(*) - denotes a mandatory field for this configuration.

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

Step 3  Enter the IP address of the device as shown in this example (required):

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

Step 4  If desired, enter the SNMP credentials for the device, as in the example below. If you specify
snmp-version v2c, then you should enter the community string for the device. If you specify
snmp-version v3, then you should enter the security level, username, authentication protocol,
authentication passphrase, privacy protocol, and privacy passphrase.

root@172-20-104-107.cisco.com(sub-device-netflow)# snmp-version v2c
root@172-20-104-107.cisco.com(sub-device-netflow)# community public

Step 5  Type show to look at the device configuration that will be applied and verify that it is correct:

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

DEVICE TYPE         : NDE (Netflow Data Export)
DEVICE ADDRESS      : 192.168.0.1
SNMP VERSION        : SNMPv2c
V2C COMMUNITY       : public
V3 USERNAME         :
V3 SECURITY LEVEL   : No authentication, no privacy
V3 AUTHENTICATION   : MD5
V3 AUTH PASSPHRASE  :
V3 PRIVACY          : DES
V3 PRIV PASSPHRASE  :

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

Step 6  Enter exit to come out of the subcommand mode and create the device. Remember the ID value that was
assigned to the new device, you will need it to create the data source!

root@172-20-104-107.cisco.com(sub-device-netflow)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#

Step 7  Enter the command data-source netflow. You will now be in netflow data source subcommand mode as
shown here:

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

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

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

Step 8  Enter ? to see all the command options available, as in the example below:

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

?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - netflow device ID (*)
device-id                 - netflow Device ID
engine-id                 - netflow Engine ID
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
show                      - show current config that will be applied on exit

(* ) - denotes a mandatory field for this configuration.
Step 9  Enter the device ID from Step 4 (required):
root@172-20-104-107.cisco.com(sub-data-source-netflow)# device-id 1

Step 10 Enter the name you would like for the data source (required):
root@172-20-104-107.cisco.com(sub-data-source-netflow)# name MyFirstNdeDataSource

Step 11 If desired, supply the specific Engine ID for this NDE data source (optional):
root@172-20-104-107.cisco.com(sub-data-source-netflow)# engine-id 123

Step 12 Enter show to look at the data source configuration that will be applied and verify that it is correct:
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show
DATA SOURCE NAME : MyFirstNdeDataSource
DATA SOURCE TYPE : NDE (Netflow Data Export)
DEVICE ID        : 1
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123

Step 13 Enter exit to come out of the subcommand mode and create the data source:
root@172-20-104-107.cisco.com(sub-data-source-netflow)# exit
Data source created successfully, ID = 3

The data source is now created, and NDE records from the device will be received and accepted by the NAM as they arrive.

Deleting NetFlow Data Sources Using the Web GUI

To delete an existing NetFlow data source, use the following steps. Note that if the autocreation feature is turned on, and the device continues to send NDE packets to the NAM, the data source will be recreated again automatically as soon as the next NDE packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

Step 1 Choose Setup > Traffic > NAM Data Sources.
Step 2 Click on the data source you would like to delete.
Step 3 Click the Delete button along the bottom of the window.

Deleting NetFlow Data Sources Using the CLI

To delete a NetFlow data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.
**Step 1** Show all data sources so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show data-source
```

Data Source ID : 1
DATA SOURCE NAME : DATA PORT 1
TYPE : Data Port
PORT NUMBER : 1
-----------

Data Source ID : 2
DATA SOURCE NAME : DATA PORT 2
TYPE : Data Port
PORT NUMBER : 2
-----------

Data Source ID : 3
DATA SOURCE NAME : MyFirstNdeDataSource
TYPE : NDE (Netflow Data Export)
DEVICE ID : 2
DEVICE ADDRESS : 192.168.0.1
ENGINE ID : 123
-----------

```
root@172-20-104-107.cisco.com#
```

**Step 2** Use the `no data-source` command to delete the data source:

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

**Step 3** Show all devices so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show device
```

DEVICE ID : 1
DEVICE TYPE : NDE (Netflow Data Export)
IP ADDRESS : 192.168.0.1
SNMP VERSION : SNMPv2c
V2C COMMUNITY : public
V3 USERNAME : 
V3 SECURITY LEVEL : No authentication, no privacy
V3 AUTHENTICATION : MD5
V3 AUTH PASSPHRASE : 
V3 PRIVACY : DES
V3 PRIV PASSPHRASE : 
INFORMATION : No packets received
STATUS : Inactive
------

```
root@172-20-104-107.cisco.com#
```

**Step 4** Use the `no device` command to delete the device:

```
root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#
```
Note that if the autocreation mode is on, and the device continues to send NDE packets to the NAM, the data source (and device entry) will be re-created again automatically as soon as the next NDE packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

## Testing NetFlow Devices

You can test the SNMP community strings for the devices in the Devices table. To test a device, select it from the Devices table, then click Test. The Device System Information Dialog Box displays. Table 2-11, Device System Information Dialog Box describes the fields.

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

Table 2-11 Device System Information Dialog Box

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

**Note**

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

## WAAS

### Understanding WAAS

Cisco Wide Area Application Services (WAAS) software optimizes the performance of TCP-based applications operating in a wide area network (WAN) environment and preserves and strengthens branch security. The WAAS solution consists of a set of devices called Wide Area Application Engines (WAEs) that work together to optimize WAN traffic over your network.

When client and server applications attempt to communicate with each other, the network devices intercept and redirect this traffic to the WAEs to act on behalf of the client application and the destination server.

WAEs provide information about packet streams traversing through both LAN and WAN interfaces of WAAS WAEs. Traffic of interest can include specific servers and types of transaction being exported. NAM processes the data exported from the WAAS and performs application response time calculations and enters the data into reports you set up.
The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network not optimized.

You can use the WAAS Top Talkers Detail Dashboard to analyze the traffic for optimization. See Top Talkers Detail, page 3-17 for more information.

Cisco WAAS helps enterprises to meet the following objectives:

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

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

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

Response Time Monitoring from WAAS Data Sources

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

The NAM provides different ART metrics by collecting data at different points as packets flow along their paths. The NAM provides five different collection points, each represented by a WAAS data source. Figure 2-3, “WAAS Data Sources (Data Collection Points)”, shows an example of the data collection points. The solid line represents data exported from a WAAS device and/or directly monitored traffic like SPAN. The broken line represents data exported from a WAAS device only.
Figure 2-3   WAAS Data Sources (Data Collection Points)

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

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

You can also configure a data source to use Export Passthrough data. For more information about configuring WAAS data sources, see Editing WAAS Data Sources, page 2-38.

Monitoring Client Data Sources

By monitoring the TCP connections between the client and the WAE device (Client segment in Figure 2-3), you can measure the following ART metrics:

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

Monitoring WAN Data Sources

By monitoring the TCP connections between the edge and core WAE devices (Client WAN and Server WAN segments in Figure 2-3), you can measure the following:
• Bandwidth usage (bits/packets) after optimization
• Network Time of the WAN segment

Monitoring Server Data Sources

By monitoring the TCP connections between the core WAE devices and the servers (Server segment in Figure 2-3), you can measure the following ART metrics:
• Server Response Time (without proxy acceleration/caching server)
• Network Time between the core WAE device and the servers

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

Deployment Scenarios

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

Table 2-13 WAAS Data Source Configurations

<table>
<thead>
<tr>
<th>Deployment Scenario</th>
<th>Edge WAE Data Source</th>
<th>Core WAE Data Source</th>
</tr>
</thead>
</table>
| 1                   | • Clients in the edge (branch)  
                      • Servers in the core (data center)  
                      • NAM in the core | Client  
                      | Server  
                      | Server WAN |
| 2                   | • Clients in the edge (branch)  
                      • Servers in the core (data center)  
                      • NAM in the edge | Client  
                      | Client WAN  
                      | Server |
| 3                   | • Servers in the edge (branch)  
                      • Clients in the core (data center)  
                      • NAM in the core | Server  
                      | Client  
                      | Client WAN |
| 4                   | • Servers in the edge (branch)  
                      • Clients in the core (data center)  
                      • NAM in the edge | Server  
                      | Server WAN  
                      | Client |
Chapter 2      Setting Up The Cisco NAM

The Cisco WAAS Central Manager, which runs on Cisco WAE Appliances. The Cisco WAAS Central Manager provides a centralized mechanism for configuring features, reporting, and monitoring, and can manage a topology containing thousands of Cisco WAE nodes.

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

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

### Step 1
From the WAAS Central Manager, configure the NAM IP address and login credentials.

### Step 2
From the router or switch, configure the data source(s) for baseline (SPAN).

### Step 3
From the WAAS Central Manager, configure the Site definition. See Sites, page 2-65 for more information.

### Step 4
In the Monitor section of WAAS Central Manager, one can observe the Top Talkers under the Network Analysis tab. See Top Talkers Detail, page 3-17 for more information.

### Step 5
From the WAAS Central Manager, configure the WAAS Flow Agent and branch/data center WAEs.

### Step 6
Create Device Groups for the branch and data center on the WAAS Central Manager, and assign a device to the Device Groups.

### Step 7
Enable the Flow Agent on the WAAS, pointing to the NAM IP. Segments are automatically selected (enabled only if the NAM is configured). The NAM will start to compute baseline ART, protocol distribution, and Top Talkers.

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

### Step 9
Turn on the Flow Agent and identify the servers to monitor to get ART improvements.
Managing WAAS Devices

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

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

After you enable flow export to the NAM using WAAS CLI commands like those above, WAAS devices will be detected and automatically added to the NAM’s WAAS device list.

You must then configure the WAAS segments you want to monitor as WAAS data sources: Client, Client WAN, Server WAN, and/or Server. See Editing WAAS Data Sources, page 2-38, for more detailed information.

You can also use the WAAS Central Manager to centrally issue WAAS CLI commands to configure a large number of WAEs at one time. Starting with Cisco NAM 5.1, the Cisco NAM GUI is accessible from within the WAAS Central Manager interface. For more information about WAAS Central Manager, refer to the technical documentation:


Note: In addition to configuring the WAAS devices, you must specify which application servers you want to monitor among the servers being optimized by WAAS devices. See WAAS Monitored Servers, page 2-87, 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

This section contains the following topics:
- Adding Data Sources for New WAAS Device, page 2-37
- Editing WAAS Data Sources, page 2-38
- Deleting a WAAS Data Source, page 2-39

Adding Data Sources for New WAAS Device

The NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up the NAM to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

Note: This step is not usually necessary because export-enabled WAAS devices are detected and added automatically. See Managing WAAS Devices, page 2-37, for more information about how to enable WAAS export to the NAM.
To manually add a WAAS device to the list of devices monitored by the NAM:

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

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

The NAM Data Source Configuration Dialog appears.

**Step 3** Choose “WAAS” from the list of Types.

**Step 4** Enter the device IP address in the IP field.

**Step 5** Check the check boxes for the appropriate WAAS Segments. See (Table 2-12).

**Step 6** (Optional) If Response Time Export is enabled (see Custom Export, page 2-61), and you want to export passthrough traffic, check the **Passthrough Response Time** check box.

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

### Editing WAAS Data Sources

The NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up the NAM to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

To edit a WAAS device’s custom data source:

**Step 1** Choose **Setup > Traffic > NAM Data Sources.** The data sources are displayed.

**Step 2** Choose the WAAS device you want to modify, and then click the **Edit** button.

You can configure the WAAS data sources to monitor the following WAAS segments as shown in Figure 2-3, **WAAS Data Sources (Data Collection Points):**

- Client—This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to NAM for monitoring.
- Client WAN—This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring.
- Server WAN—This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to NAM for monitoring.
- Server—This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to NAM for monitoring.

SPAN data sources might take the place of the WAE Server data sources listed in Table 2-13. For example, if you already configure SPAN to monitor the server LAN traffic, it is not necessary to enable the Server data source on the WAE device.

**Note** The following step is optional and applies only when the NAM is configured to export data to an External Response Time Reporting Console, such as the NetQos Super Agent.

**Step 3** To export WAAS pass-through data to the External Response Time Reporting Console, check the **Passthrough Response Time** check box.
Chapter 2  Setting Up The Cisco NAM

**Deleting a WAAS Data Source**

To delete a WAAS custom data source:

**Step 1** Choose Setup > Traffic > NAM Data Sources. The data sources are displayed.

**Step 2** Choose the WAAS custom data source you want to delete, then click the **Delete** button.

A dialog box displays the device address and asks if you are sure you want to delete the device.

**Auto Create of New WAAS Devices**

If you have numerous WAE devices, you can set up the NAM to configure newly discovered WAE devices using a predefined configuration template using the NAM Auto Config option.

**Note** If most of your WAE devices are edge WAE, you might want to set the auto config to be that of the edge device, then manually configure the data center WAE. For example, select the Client segment for monitoring.

To configure WAAS autoconfiguration:

**Step 1** Choose Setup > Traffic > NAM Data Sources. The data sources are displayed.

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

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

**Step 4** Check the check boxes for the desired Segments. See Editing WAAS Data Sources, page 2-38, for more information.

**Performance Agent**

The Performance Agent (PA) can monitor interface traffic and collect, analyze, aggregate, and export key performance analytics to a Cisco Network Analysis Module for further processing and GUI visualization. PA integration with NAM 5.1 enables you to have a lower cost way to gain visibility into Application Response Time at the branch. NAM integration with PA also reduces complexity of needing to manage a separate NAM product within the branch.

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

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

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

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

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

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

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


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

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

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

Enabling Autocreation of PA Data Sources Using the NAM GUI

To configure the NAM to automatically create data sources when it receives PA packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

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

**Step 2** Click the **Auto Create** button on the bottom left of the window.

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

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

Creating PA Data Sources Using the NAM GUI

To manually configure a PA data source on the NAM using the GUI, for example if the autocreation feature is turned OFF, use the following steps. The autocreate feature is turned on by default, so these steps are typically not necessary.

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

**Step 2** Click the **Create** button along the bottom of the window.

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

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

**Step 5** Click the “Version v1/v2c” radio button if SNMP v1 or v2c will be used to communicate with the device. Enter the community string that is configured on the device that is going to export PA packets to the NAM. Enter the same string in the “Verify” field. If you chose SNMPv1 or v2c, skip to **Step 8**.

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

**Step 7** Click the “Mode” radio button that corresponds with the desired credentials, and fill in the necessary fields. If valid SNMP credentials are provided, the NAM can upload readable text strings from the device to describe the interfaces on that device rather than just displaying the interfaces as numbers. You may specify either SNMPv2c or SNMPv3 credentials.

See Table 2-15, **SNMP Credentials** for more information.
Chapter 2  Setting Up The Cisco NAM

Traffic

Step 8  Click the Test Connectivity button. You will be shown a success or failure message.
Step 9  Click the Submit button.

Disabling Autocreation of PA Data Sources Using the NAM GUI

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

Hardware Deduplication

Note

This section applies only to Cisco NAM 2200 Series appliances.

Cisco NAM 5.1 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.

Table 2-15  SNMP Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode: No Auth, No Priv</td>
<td>SNMP will be used in a mode with no authentication and no privacy.</td>
</tr>
<tr>
<td>Mode: Auth, No Priv</td>
<td>SNMP will be used in a mode with authentication, but no privacy.</td>
</tr>
<tr>
<td>Mode: Auth and Priv</td>
<td>SNMP will be used in a mode with both authentication and privacy.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter a username, which will match the username configured on the device.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>Enter the authentication password associated with the username that was configured on the device. Verify the password.</td>
</tr>
<tr>
<td>Auth Algorithm</td>
<td>Choose the authentication standard which is configured on the device (MD5 or SHA-1).</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Enter the privacy password, which is configured on the device. Verify the password.</td>
</tr>
<tr>
<td>Privacy Algorithm</td>
<td>Enter the privacy algorithm, which is configured on the device (AES or DES).</td>
</tr>
</tbody>
</table>
In addition to the duration-based timeout, there is also a fixed packet-count timeout. There cannot be more than 7 packets between the duplicate packets. If packets 0 and 8 are identical, packet 8 will be dropped. If packets 0 and 9 are identical, packet 9 will not be dropped.

To configure packet deduplication:

**Step 1** Choose Setup > Traffic > Hardware Deduplication.
The Deduplication window displays.

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

**Step 3** Enter a value in the Time Window (1-127 in milliseconds) for the search or buffer period.
The value you set in the Time Window indicates the length of time (n milliseconds) in which two packets can be considered duplicates. If the Time Window is 100 ms but two identical packets arrive 120ms apart, the second packet would not be dropped. If the identical packets arrive 80 ms apart, the second packet would be dropped.

**Step 4** Click to choose a segment of the packet to inspect for deduplication.
The default inspects the entire packet. The second option inspects all segments except the ISL portion of the packet. The third option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The fourth option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The final (bottom) option inspects only the UDP/TCP and payload segments of the packet.

**Note** Regardless of the option you choose, the packet checksum is ignored.

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

---

### Alarms

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose what types of events for which you want the NAM to notify you, and how you want to be notified.

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

**Step 1** Depending on the type of alarm action you would like to configure, define the way you would like to be notified (by e-mail, trap, trigger capture, or syslog).
- For e-mail server settings: Choose Administration > System > E-Mail Setting
- For trap settings: Choose Administration > System > SNMP Trap Setting
- For capture session settings: Choose Capture > Packet Capture/Decode > Sessions
- For syslog settings: Choose Administration > System > Syslog Setting

**Step 2** Define the Alarm Action at Setup > Alarms > Actions.

**Step 3** Define the Threshold for this alarm at Setup > Alarms > Thresholds.

The NAM 5.1 menu selections for setting up Alarms are:
Alarm Actions

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation and be alerted to potential problems.

Note
NAM 5.1 supports IPv6 for all alarm functionality.

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

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

Table 2-16  Alarm Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name given to the alarm at setup.</td>
</tr>
<tr>
<td>Email</td>
<td>If turned on, will show “Enable”. If not turned on, will show “Disable.” E-mail server settings are configured on Administration &gt; System &gt; E-Mail Setting.</td>
</tr>
<tr>
<td>Trap</td>
<td>If configured, will show “Community: xxxxx” as configured on Administration &gt; System &gt; SNMP Trap Setting. If not configured, will be blank.</td>
</tr>
<tr>
<td>Trigger Capture</td>
<td>If configured, will show “Session: xxxxx” as configured on Capture &gt; Packet Capture/Decode &gt; Sessions. If no captures are configured, will be blank.</td>
</tr>
<tr>
<td>Syslog Remote</td>
<td>If turned on, will say “Enable”. If turned off, will say “Disable.” Settings configured on Administration &gt; System &gt; Syslog Setting.</td>
</tr>
<tr>
<td>Status</td>
<td>“Missing Trap” means that the trap configured for that alarm action has been deleted.</td>
</tr>
<tr>
<td></td>
<td>“OK” means the Alarm action was successfully created.</td>
</tr>
</tbody>
</table>
Alarm Action Configuration

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

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

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

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

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

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

To configure e-mail alarm actions:

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

The Alarm Action page displays any configured actions. If none of the four actions (e-mail, trap, capture, or syslog) are configured, you will see “No data available.”

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

**Step 3** Enter a Name for the action (up to 63 characters).

**Step 4** Choose the type of alarm action:

- **Email**: The NAM will use the e-mail address configured in **Administration > System > E-Mail Setting**. NAM alarm mail is sent as a result of NAM alarms, not router or switch alarms.
  
  The NAM sends up to five e-mails per hour per function (traffic and NDE, voice signaling, RTP, and application response time). Also, in each e-mail, there could be up to five alarm messages. These limits are in place to avoid e-mail overload.
  
  If you have configured e-mail alarms and do not receive e-mail, then your NAM does not have any alarms.
  
  If the NAM is planning to send you many alarm messages, the e-mail may state, for example, “5 of 2,345 alarm messages.”

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

- **Trigger Capture**: From the Session drop-down, choose the session (the list will be empty if there is no capture session configured in **Capture > Packet Capture/Decode > Sessions**). Click the “Start” or “Stop” radio button.

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

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

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

To edit an alarm action:

Step 1 Choose **Setup > Alarms > Actions**.
The Alarm Action table displays any configured Alarms.

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

Deleting Alarm Actions

To delete an alarm:

Step 1 Choose **Setup > Alarms > Actions**.
The Alarm Action table displays any configured Alarms.

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

Thresholds

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

---

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

The NAM Threshold Alarms window (**Setup > Alarms > Thresholds**) displays already-configured thresholds. If you hover over the arrow next to the threshold Name, as shown in Figure 2-5, a detailed view of the selected threshold will display.
You can set up alarm thresholds by defining threshold conditions for monitored variables on the NAM. Figure 2-6 shows the threshold types you can configure:

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

- Setting Host Thresholds, page 2-48
- Setting Conversation Thresholds, page 2-49
- Setting Application Thresholds, page 2-50
Setting Host Thresholds

Step 1  Choose Setup > Alarms > Thresholds.

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

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

Table 2-18 Host Alarm Thresholds

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the Host Alarm Threshold a name.</td>
</tr>
<tr>
<td>Site</td>
<td>Choose a site from the list. See Sites, page 2-65 for information on setting up a site.</td>
</tr>
<tr>
<td>Host</td>
<td>Choose a host from the list. You can enter the name of the host if the drop-down list does not contain the desired host.</td>
</tr>
<tr>
<td>Application</td>
<td>Choose an application from the list. You can enter the first few characters to narrow the selection in the drop-down list.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Choose a DSCP value from the list. You can enter the first few characters to narrow the selection in the drop-down list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the drop-down lists, choose a Rising action and a Falling action (optional). During threshold creation, by default, the falling action is the same as rising action. See Alarm Actions, page 2-44 for information on setting up alarm actions.</td>
</tr>
<tr>
<td>Host Metrics (per second)</td>
<td>Choose the type of metric from the list, and then enter a value for a Rising threshold and a Falling threshold.</td>
</tr>
<tr>
<td>Add Metrics (button)</td>
<td>Click the Add Metrics button to add another row.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Click the Delete button to remove that Metrics row.</td>
</tr>
</tbody>
</table>

Note  If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.
Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit**.

Setting Conversation Thresholds

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

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

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

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

Add Metrics (button)    | Click the **Add Metrics** button to add another row.                        |
Delete (button)         | Click the **Delete** button to remove that Metrics row.                     |

**Note** If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

Step 4 Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5 When finished, click **Submit**.
Setting Application Thresholds

Step 1  Choose Setup > Alarms > Thresholds.
Step 2  Click the Create button and choose the Application tab.
Step 3  The Application Alarm Threshold Configuration window displays. Fill in the fields as appropriate. Table 2-20, Application Alarm Thresholds describes the fields available in this window.

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

Note  If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

Step 4  Click Submit to set the thresholds, click Reset to reset the thresholds to their default value, or click Cancel to remove any changes you might have made.

Step 5  When finished, click Submit.

Setting Response Time Thresholds

Step 1  Choose Setup > Alarms > Thresholds.
### Setting Up The Cisco NAM

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

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

**Table 2-21 Response Time Thresholds**

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

**Note**  If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

**Step 4**  Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5**  When finished, click **Submit**.

### Setting DSCP Thresholds

**Step 1**  Choose **Setup > Alarms > Thresholds**.
Step 2  Click the **Create** button and choose the **DSCP** tab.

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

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

Note: If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

Step 4  Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

Step 5  When finished, click **Submit**.

### Setting RTP Stream Thresholds

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

Step 2  Click the **Create** button and choose the **RTP Streams** tab.

Step 3  The RTP Stream Alarm Threshold Configuration window displays. Fill in the fields as appropriate. *Table 2-23, RTP Streams Thresholds* describes the fields available in this window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Give the RTP Streams Alarm Threshold a name.</td>
</tr>
<tr>
<td>Severity</td>
<td>Choose High or Low. These will display on the Alarm Summary dashboard (Monitor &gt; Overview &gt; Alarm Summary), where you can choose to view High, Low, or High and Low alarms.</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up The Cisco NAM

Alarms

Note
If you leave a selection blank, it means that that parameter will not be considered. If you select “Any,” it will use any of the selections for that parameter, if encountered.

Step 4  Click Submit to set the thresholds, click Reset to reset the thresholds to their default value, or click Cancel to remove any changes you might have made.

Step 5  When finished, click Submit.

Setting Voice Signaling Thresholds

You can set up the NAM to monitor voice call quality. When Cisco Call Manager’s call detail records option is enabled, Cisco IP phones, both SCCP and SIP, will report the call’s jitter and packet loss at the end of the call. The NAM intercepts this information and raises an alarm when the alarm condition crosses the rising threshold.
To set up a voice signaling threshold:

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

**Step 2** Click the Create button and choose Voice Signaling tab.

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

**Table 2-24 Voice Signaling Thresholds**

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

**Note** If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

**Step 4** Click Submit to set the voice signaling thresholds, click Reset to reset the thresholds to their default value, or click Cancel to remove any changes you might have made.

**Step 5** When finished, click Submit.

### Setting NDE Interface Thresholds

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

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

The NDE Interface Alarm Threshold Configuration window displays. The fields are described in Table 2-25, NDE Interface Alarm Thresholds.
Chapter 2  Setting Up The Cisco NAM

Alarms

Table 2-25  NDE Interface Alarm Thresholds

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

Note  If you leave a selection blank, it means that that parameter will not be considered. If you select “Any”, it will use any of the selections for that parameter, if encountered.

Step 3 Click Submit to set the thresholds, click Reset to reset the thresholds to their default value, or click Cancel to remove any changes you might have made.

Editing an Alarm Threshold

To edit an alarm threshold:

Step 1 Choose Setup > Alarms > Thresholds.
The Thresholds table displays.

Step 2 Select the alarm to edit, then click Edit.
The dialog box displays for the type of alarm; for example, “Host Threshold.”

Step 3 Make the necessary changes.

Step 4 Click Submit to save your changes, click Reset to reset the thresholds to the values set before you edited them, or click Cancel to cancel the edit and return to the previous page.

Deleting a NAM Threshold

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

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

**Step 1** Set up the e-mail and capture settings.

a. Choose **Administration > System > E-Mail Setting** to define the e-mail settings.

b. Choose **Capture > Packet Capture/Decode > Sessions** and create a capture session for this particular server.

**Step 2** Define an Alarm Action.

a. Choose **Setup > Alarms > Actions**.

b. Click the **Create** button.

c. Enter a Name.

d. Check the **Email** check box.

e. Check the **Trigger Capture** check box, choose the session you created in **Step 1** from the drop-down menu, and select the Start or Stop radio button.

f. Click the **Submit** button.

**Step 3** Define the Threshold for this alarm.

a. Choose **Setup > Alarms > Thresholds**.

b. Click the **Create** button.

c. Choose the Response Time tab.

d. Give the Response Time Alarm Threshold a Name, and choose the Application and Severity.

e. Choose the server from the Host drop-down list.

f. Choose the action you created in **Step 2**, define the metrics for the thresholds, and click the **Submit** button.

Data Export

The NAM 5.1 selections for setting up Data Export are:

- **NetFlow**, page 2-56
- **Scheduled Exports**, page 2-60
- **Custom Export**, page 2-61

NetFlow

NetFlow collects traffic statistics by monitoring packets that flow through the device and storing the statistics in the NetFlow table. NDE converts the NetFlow table statistics into records, and exports the records to an external device, which is called a NetFlow collector. The NAM sends out NDE packets only in NDE v9 format.
There are currently six record types (or templates) that NAM exports (four in Core Stats, one in ART):

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

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

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

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

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

The following sections describe setting up NetFlow Data Export:

- Viewing Configured NetFlow Exports, page 2-57
- Configuring NetFlow Data Export, page 2-58
- Editing NetFlow Data Export, page 2-60

**Viewing Configured NetFlow Exports**

To view already-configured NetFlow Exports:

**Step 1** Choose Setup > Data Export > NetFlow.
Step 2  

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

Figure 2-7    NetFlow Exports Window

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

The fields are described in Table 2-26.

Configuring NetFlow Data Export

To configure NetFlow Data Export:

Step 1  Choose Setup > Data Export > NetFlow.
Step 2  Click the Create button.
Step 3  At the NetFlow Export Configuration window, fill in the fields. See Table 2-26, NetFlow Exports Fields for field descriptions.

Table 2-26    NetFlow Exports Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the NetFlow Export.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The IP address of the device to be exported to. Only IPv4 addresses are supported.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The port number of the device to be exported to. Valid characters: 1-9. Length: Min 1, Max 65535.</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up The Cisco NAM

Table 2-26  NetFlow Exports Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Record Type</td>
<td>The record types supported by NAM for NetFlow are:</td>
</tr>
<tr>
<td></td>
<td>• Application</td>
</tr>
<tr>
<td></td>
<td>• Host</td>
</tr>
<tr>
<td></td>
<td>• ART Client Server Application</td>
</tr>
<tr>
<td></td>
<td>• Application Conversations</td>
</tr>
<tr>
<td></td>
<td>• Network Conversations</td>
</tr>
<tr>
<td></td>
<td>• RTP Metrics</td>
</tr>
<tr>
<td>Export Interval (min)</td>
<td>Choose the desired export time interval (1, 5, 10, 15, 30, or 60 minutes). The Export Interval column values are dependent upon Aggregation intervals.</td>
</tr>
<tr>
<td></td>
<td>• Core/media aggregation interval value is utilized for the following record types: Application, Host, Network Conversation, Application conversation, and RTP Metrics.</td>
</tr>
<tr>
<td></td>
<td>• Response Time aggregation interval is utilized for the Client Server Response Time record type.</td>
</tr>
<tr>
<td>Options (button)</td>
<td>The NetFlow option selection contains a set of check boxes. These allow independent selections of on or off settings for individual NetFlow options, which can be exported in addition to the NDE packets with data and templates, as follows:</td>
</tr>
<tr>
<td></td>
<td>• Mapping of integer application ID values into application names (as strings)</td>
</tr>
<tr>
<td></td>
<td>• Mapping of integer site ID values into site names and descriptions (as strings)</td>
</tr>
<tr>
<td></td>
<td>If there are several NetFlow Export Descriptors defined for the same destination, then the last user’s selection of option exports flags is enforced on all descriptor instances that exist for the same export destination.</td>
</tr>
<tr>
<td>Filter</td>
<td>After you choose the Export Record Type (above), the Filter menus populate depending on your selection.</td>
</tr>
<tr>
<td></td>
<td>• Site: List of created sites for the NAM (configured in Setup &gt; Network &gt; Sites). Select Any to use any of the selections for that parameter.</td>
</tr>
<tr>
<td></td>
<td>Note  When you choose a record type with two sites (for example serverSite and clientSite in Client Server Response Time), the value specified by the filter will apply to either of these fields. If a certain site is chosen, then the filter will match records having the specified value in any of the site fields.</td>
</tr>
<tr>
<td></td>
<td>• Application: All applications created on the NAM (configured in Setup &gt; Classification &gt; Applications). Select Any to use any of the selections for that parameter.</td>
</tr>
<tr>
<td></td>
<td>• Source: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Sources.</td>
</tr>
<tr>
<td></td>
<td>• Destination: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Destinations.</td>
</tr>
<tr>
<td></td>
<td>• Host: List of available hosts. Click the right arrow to add it to the list of Chosen Hosts. If more than one host is selected, the filter will apply to records with the value being one of the selected set.</td>
</tr>
<tr>
<td></td>
<td>• Client: Enter a valid host address (hostname, IPv4 address, IPv6 address, or MAC address). Click the right arrow to add it to the list of Chosen Clients.</td>
</tr>
<tr>
<td></td>
<td>• Server: List of available servers. Click the right arrow to add it to the list of Chosen Servers.</td>
</tr>
</tbody>
</table>
Step 4  Click the Submit button to save the configuration, or click the Reset button to clear the fields, or click the Cancel button to exit without configuration.

---

Editing NetFlow Data Export

To edit NetFlow Data Export:

Step 1  Choose Setup > Data Export > NetFlow.
Step 2  Highlight the export you want to edit and click the Edit button.
Step 3  Make the desired changes.
Step 4  Click:
- The Submit button to submit the edits
- The Reset button to clear the changes you made
- The Cancel button to close the dialog box and return to the previous window.

Scheduled Exports

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

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

To set up a Scheduled Export:

Step 1  In most windows under the “Monitor” or “Analyze” menus, the Interactive Report is available on the left side. Click the Export button in the Interactive Report box.
Step 2  Choose the Export Type (Daily or Weekly).
Step 3  Choose the Export Time (when you would like the report delivered to you): Day and Hour.
Step 4  Choose the Report Time (if Daily) or the Data Time Range (if Weekly). This is the interval of time you would like measured.
- The Report Time for a daily report is restricted to the current 24 hours.
- The Report Time for a weekly report is always from 17:00 to 17:00, for however many days chosen.

For example:
- If you choose Export Type “Weekly,” Data Time Range “Last 2 Days,” and Export Time: Day “Wednesday” and Hour “13:00,” the report will show data from Sunday at 17:00 to Tuesday at 17:00.
- If you choose Export Time: Day “Wednesday” and Hour “18:00,” the report will show data from Monday at 17:00 to Wednesday at 17:00.
Step 5  Enter the e-mail address to which you would like the report delivered.
**Step 6** Choose the delivery option (HTML or CSV).

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

**Step 8** Click:
- The **Reset** button to clear the values in the dialog box
- The **Preview** button to preview the report
- The **Submit** button to submit the request for the scheduled job
- The **Cancel** button to close the dialog box and return to the previous window

---

**Editing a Scheduled Export**

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

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

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

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

**Step 5** Click:
- The **Submit** button to submit the request for the scheduled job
- The **Reset** button to clear the values in the dialog box
- The **Cancel** button to close the dialog box and return to the previous window.

---

**Deleting a Scheduled Export**

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

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

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

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

---

**Custom Export**

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

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

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

**Step 1** From the NAM GUI, choose **Setup > Data Export > Custom Export**.
The Response Time Export window displays.

**Step 2** Check the **Enable Export** check box.

**Step 3** Enter the IP address of the external reporting console in the IP Address field.

**Step 4** Enter the UDP port number of the external console (blank is default).

**Step 5** Optionally, click **Export Non-WAAS Traffic**.

This enables the export of SPAN and other data as well as WAAS traffic.

**Step 6** Click **Submit** to enable traffic export, or click **Reset** to clear the changes from the window.

---

**Managed Device**

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

The NAM 5.1 menu selections for setting up Managed Devices are:

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

**Device Information**

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

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

**Note** Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.
This section describes how to set router/managed device parameters.

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

**Step 1** Choose **Setup > Managed Device > Device Information.**

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

**Table 2-27 Device Information (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow Status</td>
<td>For Catalyst 6500 Series devices running Cisco IOS, if NetFlow is configured on the device, Remote export to NAM &lt;address&gt; on port &lt;number&gt; displays, otherwise the status will display Configuration unknown.</td>
</tr>
</tbody>
</table>

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

**Table 2-27 Device Information (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware description of the router.</td>
</tr>
<tr>
<td>Managed Device Software Version</td>
<td>Current software version of the router.</td>
</tr>
<tr>
<td>Managed Device System Uptime</td>
<td>Total time the switch has been running.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of the router.</td>
</tr>
<tr>
<td>Contact</td>
<td>Name of the network administrator for the router.</td>
</tr>
<tr>
<td>Managed Device</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>SNMP v1/v2c RW Community String</td>
<td>Name of the SNMP read-write community string configured on the router</td>
</tr>
<tr>
<td>Verify String</td>
<td>Verify the SNMP.</td>
</tr>
<tr>
<td>Enable SNMP V3</td>
<td>Check the check box to enable SNMP Version 3 (starting with NAM 5.0, you have the ability to manage devices with SNMPv3). If SNMPv3 is not enabled, the community string is used.</td>
</tr>
<tr>
<td>Mode: No Auth, No Priv</td>
<td>SNMP will be used in a mode with no authentication and no privacy.</td>
</tr>
<tr>
<td>Mode: Auth, No Priv</td>
<td>SNMP will be used in a mode with authentication, but no privacy.</td>
</tr>
<tr>
<td>Mode: Auth and Priv</td>
<td>SNMP will be used in a mode with both authentication and privacy.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter a username, which will match the username configured on the device.</td>
</tr>
</tbody>
</table>
Table 2-28  Router/Managed Device System Information (continued)

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

**Step 2**  Click the Test Connectivity button to perform an SNMP test. Click Close when finished.

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

### NBAR Protocol Discovery

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

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

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

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

If NBAR Protocol Discovery is enabled, the NBAR Interfaces window lists known interfaces by name and type. **Table 2-29, NBAR Interface Details** describes the fields in the window.

**Table 2-29  NBAR Interface Details**

<table>
<thead>
<tr>
<th>Field / Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (check box)</td>
<td>Check indicates that NBAR is enabled.</td>
</tr>
</tbody>
</table>
To narrow the list of interfaces, choose “Interface Name” or “Interface Description” from the drop-down list, enter any part of the interface name or description in the text box, and click the Filter button. To clear the Filter text box, click Clear. To return to showing all interfaces, check the All check box and click the Submit button.

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

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

**Network**

The NAM 5.1 menu selections for setting up the Network are:

- **Sites**, page 2-65
- **NDE Interface Capacity**, page 2-70
- **DSCP Groups**, page 2-70

**Sites**

A *site* is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems. If you want to limit the view of your network analysis data to a specific city, a specific building, or even a specific floor of a building, you can use the Sites function.

If there are multiple data sources configured for the same site, the same traffic may be accounted for more than once, resulting in inflated traffic statistics. For example, if the NAM is configured to receive SPAN traffic for a particular site, and also is receiving Netflow records for that same site, they will both be combined in the traffic statistics. In this case, if you then want to only see the statistics for a particular data source, you would need to use the Interactive Report window on the left side of the window to specify both the Site and Data Source.

The site definition is very flexible and can accommodate various scenarios. The site definition is used not only for viewing of data, but for data export and data retention as well. Normally, a site is defined by its subnet(s), but a site can also be defined using the following rules:

- Subnet (IP address prefix)
- Subnet from a data source
Chapter 2  Setting Up The Cisco NAM

 Networks

- Subnet from a given VLAN of a SPAN data source
- WAE device serving the site

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

Note
The same rule cannot be defined in multiple sites.

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

See the following sections to set up sites:
- Definition Rules, page 2-66
- Viewing Defined Sites, page 2-67
- Defining a Site, page 2-68
- Editing a Site, page 2-69

Definition Rules

Specifying a Site Using Subnets

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

Site Data-Center = subnet 172.20.0.0/16

In certain scenarios when there are overlapping IP address spaces in the networks (for example, in private networks where hosts from different sites have the same IP addresses), then data sources or VLANs can be used to differentiate the subnets. For example:

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

Specifying a Site Using WAE devices (WAAS Data Sources)

For WAAS traffic, you can define a site associated with a WAE device without specifying the site’s subnets. Simply select all of the WAAS data sources coming from the WAE device(s) serving that site.

Site SanJose = WAE-SJ-Client, WAE-SJ-CltWAN, and WAE-SJ-Passthrough data sources.

Note
We recommend that you use subnets to specify WAAS-optimized sites. Use this method only if the site’s subnets cannot be determined.

Specifying a Site Using Multiple Rules

You can define a site using a combination of multiple rules described above. For example, if a site has both optimized and non-optimized traffic, it can be defined using a combination of WAAS data sources and a subnet from a NDE data source.
When defining a site using multiple data sources, be careful to make sure that those data sources do not have duplicated traffic to avoid double counting the site traffic statistics.

**Resolving Ambiguity (Overlapping Site Definitions)**

Conflicting rules are not allowed in site definitions. Of the following two scenarios, the second one is not allowed.

1. 1.2.3.0/24 from SPAN1 = SiteA
2. 1.2.3.0/24 from SPAN1 = SiteB

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

1. 1.2.3.0/24 = Site D
2. WAE1-Client datasrc = Site E

The longest prefix has higher priority (same data source/VLAN). In the following two scenarios, the first would receive the higher priority.

1. 1.2.3.0/24 from SPAN1 = Site A
2. 1.2.0.0/16 from SPAN1 = Site C

The more refined (specific) rule has higher priority. In the following two scenarios, the first would receive the higher priority.

1. 1.2.3.0/24 from SPAN1 = Site A
2. 1.2.3.0/24 (any datasrc) = Site D

**Viewing Defined Sites**

To view already-defined sites:

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

**Step 2**  The Sites window appears. Defined sites will be listed in the table.

The fields are described in Table 2-30, Sites Window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of what the site includes.</td>
</tr>
<tr>
<td>Rule</td>
<td>Lists the first rule assigned to the selected site. If you see periods next</td>
</tr>
<tr>
<td></td>
<td>to the site rule (...), then multiple rules were created for that site. To</td>
</tr>
<tr>
<td></td>
<td>see the list of all rules, click the quick view icon (after highlighting the</td>
</tr>
<tr>
<td></td>
<td>site, click the small arrow on the right).</td>
</tr>
<tr>
<td>Status</td>
<td>Shows if the site is Enabled or Disabled.</td>
</tr>
</tbody>
</table>
Defining a Site

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

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

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

**Step 3** The Site Configuration window appears. Enter a Name, Description, Subnet, Data Source, and/or VLAN as appropriate.

See Figure 2-8 for an example.

**Figure 2-8 Site Configuration Window**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Unique text string for naming a site.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Optional text string for describing site.</td>
</tr>
<tr>
<td><strong>Disable Site</strong></td>
<td>If you check this check box, the NAM will skip this site when classifying traffic. This is useful if the site is no longer active, but the user would still like to access historical site data in the database. Otherwise, the user should delete sites that are not needed.</td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
<td>IP address subnet (IPv4/IPv6 address and mask); for example, 10.1.1.0/24. Click the blue “i” to get information about Site Rules. You can click the <strong>Detect</strong> button to tell the NAM to look for subnets in the traffic. See the next section, Subnet Detection.</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up The Cisco NAM

Step 4  Click the Submit button.

Note  The “Unassigned” site (with a description of “Unclassified hosts”) includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.

Subnet Detection

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

Table 2-32  Subnet Detection

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

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

Editing a Site

You can edit sites that have been created. Note that the “Unassigned” site cannot be edited or deleted.

Step 1  Choose Setup > Network > Sites.
Step 2  Highlight the site that you have configured.
Step 3 Click the **Edit** button.

Step 4 Edit the desired field.

Step 5 Click **Submit** to save the changes, or click **Reset** and **OK** to reinstate the site’s previous settings, or click **Cancel** to cancel any changes and return to the main Sites page.

---

### NDE Interface Capacity

After you have set up NetFlow data sources (see NetFlow, page 2-22), you can go to the NDE Interface Capacity window at Setup > Network > NDE Interface Capacity to specify the speed of each interface. This allows the NAM to calculate interface utilization on the NDE Interface Traffic Analysis window (Analyze > Traffic > NDE Interface). Otherwise, the NAM can only display the throughput of the interface, but cannot show its utilization.

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

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

To add an interface, continue to Creating an NDE Interface, page 2-70.

### Creating an NDE Interface

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

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

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

### DSCP Groups

Differentiated services monitoring (DiffServ) is designed to monitor the network traffic usage of Differentiated Services Code Point (DSCP) values. To monitor DSCP, you must configure at least one aggregation profile, and one or more aggregation groups associated with each profile. This section describes how to set up the DSCP groups.
You can define two or three different groups of traffic, and assign the various DSCP values to each group. Or you can assign one particular value for the first group and give it a name, and then assign all the rest to the other (or default) group and give that a name.

For detailed information about setting DSCP values, see *Implementing Quality of Service Policies with DSCP*:

These topics help you set up and manage the DSCP groups:
- Creating a DSCP Group, page 2-71
- Editing a DSCP Group, page 2-72
- Deleting a DSCP Group, page 2-73

## Creating a DSCP Group

To create a DSCP Group:

1. **Step 1** Choose *Setup > Network > DSCP Groups.*
   The DSCP Groups table displays.
2. **Step 2** Click the *Create* button.
   The DSCP Group Configuration window displays.
3. **Step 3** Fill in the fields as described in *Table 2-34, DSCP Group Setup Dialog Box.*

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name of the profile.</td>
<td>Enter the name of the profile you are creating. The maximum is 64 characters.</td>
</tr>
<tr>
<td><strong>Label Format</strong></td>
<td>DSCP</td>
<td>DSCP numbers from 0 to 63. After selecting the DSCP radio button, you can freely choose any of the 64 possible values and assign them to Groups.</td>
</tr>
<tr>
<td><strong>AF / EF / CS</strong></td>
<td>Assured Forwarding (AF) guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, Expedited Forwarding (EF) is used for traffic that is very sensitive to delay, loss and jitter, such as voice or video traffic. Class Selector (CS) the last 3 bits of the 6-bit DSCP field, so these correspond to DSCP 0 through DSCP 7.</td>
<td></td>
</tr>
<tr>
<td><strong>Bit Field</strong></td>
<td>Six bits in the IP header of a packet. See Table 2-35.</td>
<td></td>
</tr>
</tbody>
</table>

*Table 2-35, DSCP Group Label Formats* shows the available formats and associated values.
Step 4 Click **Submit** to save your changes, or click **Reset** to cancel.

### Editing a DSCP Group

To edit a DSCP group:

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

The DSCP groups window displays.

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

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

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

Classification

In Network Analysis Module release 5.0, the RMON-based protocol directory was replaced with a new application ID classification system. When defining applications, you will be able to view and select from a list of candidate IP addresses and port numbers for the traffic being analyzed.

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

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

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

The menu selections for setting up Classification are:

- Applications, page 2-73
- Application Groups, page 2-76
- URL-based Applications, page 2-77
- Encapsulations, page 2-80

Applications

The NAM recognizes an application on the basis of port number, port number range, stateful inspection of traffic (for example, voice signaling traffic or FTP), heuristics (for example, MS-RPC or SUN-RPC), or standardized application identifiers exported by Cisco platforms with NDE. If the NAM is not able to recognize an application using any of these mechanisms, the application type of the traffic is reported as “unknown.” You can configure the application reported as “unknown” to create custom applications.

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

Figure 2-9 shows an example of what the window may look like.
Table 2-36, Applications describes the fields on the Applications setup page.

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

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

To create a new application:

**Step 1** Choose Setup > Classification > Applications.  
The Applications window displays.

**Step 2** Choose the type you would like to create and click Create.  
The Application Configuration window displays.

**Step 3** Enter a name in the Name field.

**Step 4** Enter a Selector value. This is an arbitrary number, unique within an engine-id. It will be automatically assigned if left blank.  
This allows you to configure applications consistently across multiple NAMs, so that the same user-created application is exported with the same value.

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

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

**Step 6** Enter a port number; the range will vary depending on the protocol family selected. This is an arbitrary number you assign to handle the additional ports for the protocol family. This protocol number must be unique so it does not conflict with standard protocol/port assignments.

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

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

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

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

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

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

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

---

**Editing an Application**

In NAM 5.1, you can only modify the user-defined applications, and not the standard applications. You can only edit an application for which it states “Custom” in the Engine ID column.

To edit an application:

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

**Step 2**
Select the application to edit, and click **Edit**.
The Application Configuration window displays.

**Step 3**
Make the desired changes (you will only be able to change the name and protocol/port/port range).

**Step 4**
Do one of the following:
• To accept the changes, click **Submit**.
• To leave the configuration unchanged, click **Cancel**.
• To delete the protocol, click **Delete**.

---

**Deleting a Protocol**

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

---

**Application Groups**

An application group is a set of applications that can be monitored as a whole. The following topics help you set up and manage the application group:

• Creating an Application Group, page 2-76
• Editing an Application Group, page 2-77
• Deleting an Application Group, page 2-77

---

**Creating an Application Group**

To create an application group:
Chapter 2      Setting Up The Cisco NAM

Classification

Step 1 Choose Setup > Classification > Application Groups.
The Application Groups window displays.

Step 2 Click the Create button.

Step 3 Enter the name in the Application Group Name field.

Step 4 Use the next Application field and the Filter button to narrow the list of selectable applications.

Step 5 Select an application and click the Add button. Applications appear in the Selected Applications box.
You can select multiple applications at once by using the Shift button, and then click Add.

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

Editing an Application Group

To edit an application group:

Step 1 Choose Setup > Classification > Application Groups.

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

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

Deleting an Application Group

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

URL-based Applications

URL-based applications are extensions to the list of applications. When the URL in an HTTP request (a URL on any port that is part of the iana-l4:http protocol, or protocol named “http” under the “iana-l4” engine ID) matches the criteria of a URL-based application, the traffic is classified as that protocol. The device interface statistics are collected by regularly (once a minute) polling the ifTable statistics of all interfaces on the managed device.

A URL-based application can be used the same way as any other application. For example, a URL-based application can be used in collections, captures, and reports.

An incoming URL is matched against the criteria of the configured URL-based application, in the order of the index, until a match is found. When a match is found, the remaining URL-based applications are not considered.

A URL consists of the following parts:

- a host
- a path
- an argument

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

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

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

**Step 2** Click Create.

The Create URL-based Application window displays.

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

**Step 3**

Click:
- The Submit button to submit the request
- The Reset button to clear the values in the window
Chapter 2  Setting Up The Cisco NAM

Classification

- The Cancel button to close the dialog box and return to the previous window

Example

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

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

Editing a URL-Based Application

To edit URL-based applications:

Step 1  Choose Setup > Classification > URL-based Applications.
Step 2  Select a radio button and click Edit.

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

Change the information as desired.

Step 3  Click:
- The Submit button to submit the request
- The Reset button to clear the values in the window
- The Cancel button to close the dialog box and return to the previous window.

Deleting a URL-based Application

To delete a URL-based application:

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

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

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

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

To configure encapsulation:

Step 1 Choose Setup > Classification > Encapsulations.

The Encapsulations configuration page appears.

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

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

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

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

Step 3 Click Submit to change the Encapsulation Configuration.

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

Monitoring

Before you can monitor data on the NAM, you must set up the data collections. The NAM 5.1 menu selections for setting up Monitoring are:

- Aggregation Intervals, page 2-81
Aggregation Intervals

The NAM has short-term and long-term aggregation intervals (this was referred to as long-term reporting in NAM 4.x). In NAM 5.x, the aggregated data will be displayed in the dashboards if the query is longer than one day.

The purpose of gathering short term aggregation interval data is for troubleshooting. It has a finer granularity than long term data (by default, the short term aggregation interval for Traffic/Media is one minute, and short term response time interval is five minutes).

The purpose of gathering long term interval data is for trending analysis. The smallest aggregation interval for long term data is one hour (60 minutes).

Caution

If you modify the aggregation intervals, existing collected data that is not in the same aggregation interval will be completely removed. Data will then start being collected from the beginning again at the moment the intervals are modified and applied.

Traffic and Media refer to applications, hosts, RTP streams, and voice calls monitoring. Response Time refers only to application response time. The NAM does not support long term aggregations of data for the following media: conversations, RTP streams, and voice signaling calls monitoring.

To set up aggregation intervals:

Step 1
Choose Setup > Monitoring > Aggregation Intervals.

Step 2
Choose the desired durations for Short Term Interval and Long Term Interval.

Step 3
Check the Collect only hosts from user-defined sites (exclude hosts from Unassigned site) check box if you want the NAM long term data to only contain information for hosts classified to the user-defined sites. This check box only applies to the long term data; short term will always collects all hosts.

Note
Enabling the “Collect only hosts from user-define sites” option can significantly speed up report queries, because it excludes unclassified hosts’ statistics from the database.

Step 4
Click Submit.

When you first start the NAM, in monitoring windows that show site information, you will see a site named “Unassigned” and with a description of “Unclassified Hosts.” The Unassigned site includes any that do not match the site configurations. By default, long-term storage will include data for all sites, including the Unassigned site. In some cases, you may not want to view long term data of hosts that are not in your network, in which case you would check the check box.
The aggregation intervals determine how much data can be stored in the NAM database. See Table 2-38, Data Retention for information about data retention.

Table 2-38 Data Retention

<table>
<thead>
<tr>
<th>Aggregated Data Type</th>
<th>WS-SVC-NAM-1 and WS-SVC-NAM-2</th>
<th>All other platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Normal)</td>
<td>24 hours</td>
<td>72 hours</td>
</tr>
<tr>
<td>(Minimum)</td>
<td>5 hours</td>
<td>14 hours</td>
</tr>
</tbody>
</table>

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

Response Time

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

**Step 1** Choose Setup > Monitoring > Response Time.

The Response Time Configuration page displays. The settings you make on this window comprise the time distribution in milliseconds for the detailed Server Application Response Time data collection.

**Step 2** Check the Enable Response Time Monitor check box.

**Step 3** After “Monitored Server Filter”, you will see “Disabled” or “Enabled.” If a WAAS server has been configured under Setup > Monitoring > WAAS Servers, you will see “Enabled.” Click the Configure Filter button to configure a filter.

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

Table 2-39 Response Time Configuration Window

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

Voice

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

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

To set up voice monitoring:

Step 1  Choose Setup > Monitoring > Voice.
The Voice Monitoring page displays.

Step 2  Check the Enable Call Signal Monitoring check box.

Step 3  Accept the default MOS Score value range or modify the values as you prefer. See Table 2-40, Voice Monitor Setup Window.

Table 2-40  Voice Monitor Setup Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Monitoring</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables voice monitoring</td>
</tr>
<tr>
<td>MOS Values</td>
<td></td>
</tr>
<tr>
<td>Excellent</td>
<td>Highest quality MOS score (5.0 being highest). The default value is 5.00.</td>
</tr>
<tr>
<td>Good</td>
<td>Quality less than excellent; MOS score ranges from this setting to less than excellent. The default value is 4.33.</td>
</tr>
<tr>
<td>Fair</td>
<td>Quality less than good; MOS score ranges from this setting to less than good. The default value is 4.02.</td>
</tr>
<tr>
<td>Poor</td>
<td>Quality less than excellent; MOS score ranges from this setting to less than fair. The default value is 3.59.</td>
</tr>
</tbody>
</table>

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

Table 2-41  Maximum and Default Voice/Video and RTP Stream Parameters per Platform

<table>
<thead>
<tr>
<th>Field</th>
<th>2220 Appliance</th>
<th>2204 Appliance</th>
<th>NAM-2(x)</th>
<th>NAM-1(x)</th>
<th>NME-NAM</th>
<th>NAM SRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP Streams</td>
<td>4,000 (2000)</td>
<td>1,500 (750)</td>
<td>800 (400)</td>
<td>400 (200)</td>
<td>100 (50)</td>
<td>800 (400)</td>
</tr>
<tr>
<td>Max Active Calls</td>
<td>2,000 (1,000)</td>
<td>750 (375)</td>
<td>400 (200)</td>
<td>200 (100)</td>
<td>50 (25)</td>
<td>50 (25)</td>
</tr>
</tbody>
</table>
Chapter 2  Setting Up The Cisco NAM

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.


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

RTP Filter

When the NAM is initially started, RTP stream traffic will automatically start being monitored. The NAM enables you to monitor all RTP stream traffic among all SPANed traffic, without having to know the signaling traffic used in negotiating the RTP channels. RTP Stream Monitoring is enabled by default under Setup > Monitoring > RTP Filter. To disable it, uncheck the Enable RTP Stream Monitoring check box and click the Submit button to apply the change.

To create an RTP filter:

Step 1  Choose Setup > Monitoring > RTP Filter.
Step 2  Click the Create button.
Step 3  From the drop-down menu, choose the protocol (IP or IPv6).
Step 4  Enter the Source Address, Source Mask, Destination Address, and Destination Mask.
Step 5  Click OK.

URL

The URL collection listens to traffic on TCP port 80 of a selected datasource and collects URLs. Any protocol which has its master port set to TCP port 80 can be used for URL collections. Only one collection on a single datasource can be enabled at a time.

A URL, for example: http://host.domain.com/intro?id=123, consists of a host part (host.domain.com), a path part (intro), and an arguments part (?id=123).

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

This section contains the following procedures:

- Enabling a URL Collection
- Changing a URL Collection
Disabling a URL Collection

Enabling a URL Collection

To enable a URL collection:

**Step 1** Choose **Setup > Monitoring > URL**.

The URL window displays.

*Figure 2-11 URL Collection Configuration Dialog Box*

- **Step 2** Check the **Enable** check box to initiate URL Collection.

  **Note** The collection will not begin until you click **Submit**.

- **Step 3** Provide the information described in **Table 2-42, URL Collection Configuration Dialog Box**.

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

  **Note** Depending on which radio button option is collected, the format of the URL varies. For example, the leading http part is only present if the host part is collected. Keep this variable in mind, when configuring a *match only* expression.
Step 4  Check the **Recycle Entries** check box to recycle entries.

Step 5  Check the check box for one of the following:
- Collect complete URL (Host, Path and Arguments)
- Collect Host only (ignore Path and Arguments)
- Collect Host and Path (ignore Arguments)
- Collect Path and Arguments (ignore Host)
- Collect Path only (ignore Host and Arguments)

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

## Changing a URL Collection

To change a URL collection:

**Step 1**  Choose **Setup > Monitoring > URL**.

The URL page (**Figure 2-11**) displays.

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

**Note**  Changing any parameters and applying the changes flushes the collected URLs and restarts the collection process.

**Step 3**  Click **Submit** to save your changes, or click **Reset** to cancel.

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

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

To disable a URL collection:

**Step 1** Choose **Setup > Monitoring > URL Collection**.

**Step 2** Uncheck the **Enable** check box.

**Step 3** Click **Submit**.

WAAS Monitored Servers

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

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

This section contains the following topics:
- Adding a WAAS Monitored Server, page 2-87
- Deleting a WAAS Monitored Server, page 2-88

Adding a WAAS Monitored Server

To add a WAAS monitored server:

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

*Figure 2-12  WAAS Monitored Servers Table*

<table>
<thead>
<tr>
<th>Filter Response Time for all Data Sources by Monitored Servers</th>
<th>Select All</th>
<th>10.100.5.1</th>
</tr>
</thead>
</table>

**Step 2** Check the **Filter Response Time for all Data Sources by Monitored Servers** check box if you want the NAM to compute response time data only for the servers from this list for all data sources, including non-WAAS data sources. All other servers will be ignored in response time monitoring views. This enables you to reduce NAM workload and to improve NAM overall performance.

**Step 3** Click **Add**.
The Add WAAS Server(s) dialog box displays.

**Step 4** Enter the server IP address in the Server Address field. You can paste multiple IP addresses here as well.

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

---

### Deleting a WAAS Monitored Server

To delete a WAAS monitored server data source:

**Step 1** Choose **Setup > Monitoring > WAAS Servers**.

The WAAS Servers page displays any WAAS monitored servers.

**Step 2** Select the monitored WAAS server to delete, then click **Delete**.

A confirmation dialog displays to ensure you want to delete the selected WAAS monitored server.

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