APPENDIX A

Troubleshooting

This appendix addresses some common issues you might encounter while using the NAM Traffic Analyzer.

General NAM Issues

Q. What information should I collect and what else should I do when the NAM is not responding?

A. Determine the answers to the following questions and gather the following information:

- Does **session** from the switch/router CLI work?
- Does **ping** over EOBC (127 subnet) work?
- Does **ping** to the management IP address work?

- Collect output of **show tech-support** command from both the NAM and the switch or router.
- Collect core files.
- Check if NAM is seated correctly in chassis
- Reset NAM
- Reset into maintenance image or helper
- Clear the configuration
- Reinstall the application image (possibly with the repartition option *--install*)

CPU Usage Percentage

Q. The NAM output of **show tech-support** command shows CPU usage that exceeds 100% for a process. Is there a problem with that process?

A. No; the value shown is the sum of all current CPU usage for this process. In the following example, PID 1925 shows 305% CPU usage. This means that the total usage percentage of all of the NAMs CPUs totaled 305%.

```
PID  USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+   COMMAND
1925 root      15   0 3266m 1.4g 5804 S  305  8.9   3569:25 mond
9626 root      20   0 10516 1172  784 R    2  0.0   0:00.01 top
   1 root      15   0  3676  568  476 S    0  0.0   0:03.87 init
```

Using a NAM with only one CPU, the CPU usage percentage will never exceed 100%, while using a NAM with two CPUs, the CPU usage percentage would never exceed 200%. Using a Cisco NAM 2220 appliance with eight CPUs, the CPU usage percentage can exceed 200% or more. The value shown represents the sum of all current CPUs used by this process, not the over the length of process run time.

A high individual CPU usage percentage value for NAMs with multiple CPUs is a different case, but not unexpected. A software change in NAM 4.0 provides improved performance but can show high CPU usage percentage, even when the NAM is not busy, as the NAM polls incoming packets. When more packets arrive, the time used for packet polling shifts to real packet processing.

To see current CPU usage percentages, including individual and average for all, click **Admin > System** to view the System Resources window as described in section System Resources, page 2-10.

Username and Password Issues

Q. Can I use my CLI username (root or guest) and password to log into the NAM Traffic Analyzer? Or, can I use my NAM Traffic Analyzer username and password to log into the NAM CLI?

A. No. Web and CLI users are administered separately. You can create web users with a local database or using TACACS+. You can create a web user with the same username and password as used on the CLI. However, you must still make password changes in both places.

Q. If I use TACACS+, must I still have web users defined in my local database?

A. No. You can use TACACS+ either in addition to a local database or instead of a local database. (The local database is always checked first.) To use only TACACS+, you can eliminate the local database users by either of these methods:

- Use the NAM CLI **rmwebusers** command to remove only local users, not TACACS+ users, as they are administered separately on the TACACS+ server.

- From the Admin tab, click **Users**, then delete all local database users individually.

Caution Do not delete all local database web users until you have verified that you can log into the NAM Traffic Analyzer as a TACACS+ user.

Q. How can I recover the local web admin user password?

A. You can recover the password in situations where you have forgotten the local web admin user password, or when another user with Account permission logged in and changed the local web admin user password.

To recover the local web admin user password:

Step 1 Access the NAM CLI.

Step 2 Enter the following commands:

```
web-user
user name <name>
exit
```

Step 3 At the prompt, enter the new password.

Step 4 Enter **Y** to confirm the new password.

Q. How can I recover when I mixed up the TACACS+ configuration between my NAM and TACACS+ server, and I do not have a local database user account to fix my TACACS+ configuration on my NAM?

A. If you cannot fix this problem from the TACACS+ server, go to the NAM CLI and enter **ip http tacacs+ enable** to reconfigure the TACACS+ settings.

Q. Are there restrictions on using passwords when performing upgrades or applying patches?

A. Yes. Do not include the password as an argument in upgrade and patch commands. Use command syntax of this form:

```
patch ftp://user@host/full-patch/filename
```

Enter the password when prompted.

Login Issues

Q. Why does my login session time out?

A. Your login session automatically times out after approximately 1 hour of inactivity, then logs you out of the NAM Traffic Analyzer.

Note If you are viewing a window in which the autorefresh feature is enabled, your login session does not time out.

Q. Why do users remain logged in after their user accounts are deleted?

A. If you delete user accounts while users are logged in, they remain logged in and retain their privileges. The session remains in effect until they log out. Deleting an account or changing permissions in mid-session affects only future sessions. To force off a user who is logged in, restart the NAM.

Q. Why am I unable to log into the NAM Traffic Analyzer with TACACS+ configured?

A. Verify that you entered the correct TACACS+ server name and secret key and that you are using the same the secret key as the one configured in the TACACS+ server. If you use a generic TACACS+ server, make sure that it supports Password Authentication Protocol (PAP) and that PAP is selected.

You can also check system alerts for any TACACS+-related messages.

Step 1 Log into the NAM Traffic Analyzer as a local user.

Step 2 Choose **Admin** > **Diagnostics**.

Step 3 In the contents, click **Tech Support**.

Step 4 Scroll down to the **/var/log/messages** section.

Step 5 Look for messages similar to the following, then take the appropriate action.

Message	Likely Cause and Action
`...PAM-tacplus[612]:auth failed: Login incorrect`	The username and password do not match any usernames and passwords in the TACACS+ server. 1. Log into the TACACS+ server. 2. Configure the server to authenticate and authorize NAM users. (See the"Establishing TACACS+ Authentication and Authorization" section on page 2-6.)
`... httpd: tac_authen_pap_read: error reading PAP authen header, read -1 of 12: Connection reset by peer` `... PAM-tacplus[10455]: auth failed: Authentication error, please contact administrator.`	The NAM has not been added to the NAS (AAA client) list of the ACS/TACACS+ server. 1. Log into the TACACS+ server. 2. Make sure that the NAM is in the NAS (AAA client) list and TACACS+ is selected as the authentication method. (See the"Establishing TACACS+ Authentication and Authorization" section on page 2-6.)
`...httpd:tac_authen_pap_read: invalid reply content, incorrect key?` `...PAM-tacplus[616]:auth failed: Authentication error, please contact administrator.`	The TACACS+ secret key configured in the NAM does not match the secret key of the TACACS+ server. 1. Choose **Admin** > **Users**. 2. In the contents, click **TACACS+**. 3. Enter the correct secret key in the Secret Key and Repeat Secret Key fields. 4. Click **Apply**.

Message	Likely Cause and Action

`..httpd:tac_connect:connection to 172.20.122.183 failed:Connection timed out`
`...httpd:tac_connect:all possible TACACS+ servers failed`
`...PAM-tacplus[613]:connection failed srv 0: Connection timed out`
`...PAM-tacplus[613]:no more servers to connect`
	An incorrect TACACS+ server IP address is configured on the NAM.
	1. Click **Admin**.
	2. Click **Users**.
	3. In the contents, click **TACACS+**.
	4. Enter the correct TACACS+ server address.
	5. Click **Apply**.

`Not authorized...` (when accessing NAM Traffic Analyzer)	The user does not have the necessary access rights. 1. Log into the TACACS+ server. 2. Grant the appropriate rights to the user. (See the"Adding a NAM User or User Group" section on page 2-7.)

SPAN Related Issues

Note This section applies to NAM-1 and NAM-2 only.

Q. What if the SPAN session does not show up in the Active SPAN window?

A. If you have a switch that is running Catalyst OS, a SPAN session will become inactive if the module that contains the destination port is removed from the switch chassis. In this case, the NAM will not see the SPAN session because the SPAN configuration has been removed from the SNMP agent by the Supervisor engine module.

Q. Why does my create SPAN session fail on a switch running Cisco IOS?

A. For switches running Cisco IOS, a SPAN session can be partially defined with either a source type or destination port only. The NAM will not see this partial SPAN session. However, the partially configured SPAN session may cause the create SPAN request to fail if there is a conflict with either the source type or destination port.

Q. How do I change the SPAN session so it only spans in one direction—or, change the SPAN session type from switch port to VLAN or VLAN to switch port?

A. You cannot edit these characteristics using the NAM Traffic Analyzer after creating the SPAN session. Instead, you must delete the SPAN session and create a new one with the desired characteristics.

You can also simply click **Create** (without deleting the SPAN session) to overwrite the current SPAN.

Note You can only add or delete VLANs (if the current SPAN session is already VLAN) in a SPAN session in the Setup SPAN Sources dialog box. You cannot change the SPAN traffic type (such as changing VLAN to ports or changing the traffic direction).

Q. Why do I sometimes see the message, `Failed to create SPAN session for...`, when I create or edit a SPAN session in the Setup SPAN Sources dialog box?

A. This usually happens because you reached the SPAN limit on the switch. To determine the applicable limits, see the appropriate Catalyst OS or Cisco IOS documentation. The simplest solution is to delete the SPAN (or RSPAN, if applicable) session and try to edit or create a new one.

Packet Capturing Issues

Q. Why is the capture buffer locked and why are no packets being captured in the Capture Settings dialog box?

A. This happens because you selected **Lock when full**, which prevents the capture process from overwriting the contents when the buffer fills.

To restart a locked capture, you first have to clear it. You might want to save the capture buffer to a file before clearing it.

Note

- You can also select **Wrap when full** so the newly arriving packets overwrite the oldest packets when the capture buffer is full.

Q. Why am I having problems capturing packets, even after I configured the capture settings in the Capture Settings dialog box and clicked **Start**?

A. This might happen for several reasons.

Verify that the data source you selected in the **Capture packets from** list is spanned to the NAM.

Tip The NAM automatically learns VLANs from the switch, but does not automatically SPAN them—you must still SPAN them using the Active SPAN Sources window.

To verify that your SPAN session is working:

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

Step 2 Verify that packet traffic is spanned from the appropriate source.

Step 3 If not, click **Create** or **Edit**, to add the desired SPAN sources.

Step 4 Click **Submit**.

Step 5 Choose **Capture > Settings**.

Step 6 Click **Start**.

You should also verify that you selected filters carefully in the Capture Settings dialog box. The filter you created might be too restrictive. (For more information, see Chapter 6, “Capturing and Decoding Packet Data.”)

If you still cannot capture packets, try to remove all capture filters:

Step 1 Choose **Capture > Buffers**.

Step 2 Select the capture buffer and click **Settings**.

Step 3 Deselect the Address, Protocol, Port, and Custom check boxes.

Step 4 To restart the capture, click **Start**.

You might also have selected a filter based on a protocol that has been deleted from the NAM protocol directory (by an SNMP manager or another web user).

To see the protocols available for filtering, do the following:

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

Step 2 In the contents, click **Protocol Directory**.

Capture might fail to start because no memory is available for capture buffers. To find out about NAM capture memory usage, choose **Capture > Buffers**. Clear or delete old buffers to free up capture memory.

Q. Why do I see duplicate captured packets?

A. When packets appear twice in the Capture Decode dialog box, it might be because you are spanning in both directions (transmit and receive).

Q. Why does the automatic capture trigger not stop or start?

A. The alarm associated with the automatic capture might have not occurred yet. Go to **Alarms > NAM** to see the list of past alarm occurrences. In addition, for start capture triggers, the capture buffer should initially be in a paused state.

If the buffer is cleared or running, a start capture trigger does not work. For stop capture triggers, the capture buffer should be running initially. If the buffer is paused or cleared, a stop trigger does not work. For more information, see the "Configuring Capture Settings" section on page 6-3.

Q. Why am I unable to start a capture from the Monitor window?

A. When the buffer has been completely allocated to other capture processes and the available buffer is 0 MB, the capture process will not start. To solve this problem, clear an existing capture process to free up the buffer so new processes can be started.

Q. Why does the layer two information in packets captured on an internal port of the NM-NAM look wrong.

A. The router copies the packets to the NM-NAM in the CEF path. At that time the layer two has been stripped off. A special layer two header is used to send the packet to the NM-NAM

Q. Why do I see additional traffic on the NM-NAM internal port besides what I configured to be monitored.

A. Besides the traffic copied to the NM-NAM by the analysis-module monitoring feature, management traffic might also be directed to the NM-NAM that is captured.

Alarm and Interface/Port Stats Issues

Q. Why does one of the alarms in the Setup/Alarm/NAM MIB Thresholds window show the Data Source as Collection Deleted?

A. Data Sources are mapped to a table collection index. When you delete the collection from the Setup/Monitor/Core window, the table index is deleted. Because the alarm data source can no longer map to a table index, you must delete the alarm and recreate it.

Q. Why am I unable to create threshold alarms or view interface or port statistics?

A. Two typical reasons might be because there is no connectivity between the switch and the NAM, or that mini-RMON is not enabled on the switch.

For WS-SVC-NAM-1 and WS-SVC-NAM-2 devices

To verify that there is connectivity, go to **Setup > Chassis Parameters > Chassis Information** and view the SNMP read from switch and SNMP write to switch results. For more information on the Switch Information table, see the "Viewing the Switch Information" section on page 3-2.

To verify that Mini-RMON is enabled on the switch, go to **Setup > Chassis Parameters > Port Stats (Mini-RMON)** and view the Current Status in the table. For more information on enabling Mini-RMON, see the "Enabling Mini-RMON Collection" section on page 3-49.

For NM-NAM or NME-NAM Devices

To verify that there is connectivity, check that the community strings are configured. You can also go to **Setup > Router Parameters** and click the **Test** button to verify that the community string is correct. For more information on testing the router community strings, see the "Testing the Router Community Strings" section on page 3-30.

Q. Why do I see negative values on the Alarms window?

A. The alarm counters wrapped back to zero between the last poll and the current poll.

Q. Why does the Cumulative Data table for port/interface statistics take a long time to load?

A. This might be because of poor or nonexistent connectivity. To check your connectivity, go to **Setup >Chassis Parameters** and click **Test**.

Note For NM-NAM or NME-NAM devices, go to **Setup>Router Parameters**.

NetFlow and NBAR Monitoring Problems

Q. Why is there no data for the default NetFlow data source of the device?

A. Select **Setup > Data Sources > NetFlow > Listening Mode** and click **Start**. If the device is displayed in the table, see the "Why is there no data in collections even though the Listening Mode table shows that the NAM is receiving NDE packets from the device?" question on page A-9. If the device is not displayed in the table after three refresh cycles, the NAM is not seeing NetFlow packets from the device. There is either a network problem or the device is not configured properly.

To verify that a NetFlow device is configured to send NetFlow packets to UDP port 3000 of the NAM, use the following command:

```
prompt#show ip flow export
```

or

```
prompt#show mls nde
```

Displayed information shows whether NetFlow export is enabled or disabled, to what IP address and port NetFlow packets are being exported, and the number of NDE packets that were sent to the NAM. For more information on configuring your NetFlow device, see the "Configuring NetFlow on Devices" section on page 3-19 or your accompanying device documentation.

Q. Why is there no data in collections even though the Listening Mode table shows that the NAM is receiving NDE packets from the device?

A. Verify that you have data for the collections in the **Monitor > Hosts**, **Monitor > Apps and Monitor > Conversations** pages. If there is NetFlow data on the Monitor pages, then the auto refresh interval might be too fast. For more information on troubleshooting the auto refresh interval, see the "Why are the Monitor > Hosts, Monitor > Apps and Monitor > Conversations pages showing data only every two (or more) auto refresh cycles?" question on page A-9 and the "Why does the Network Conversations table on the Monitor>Conversations page have 0.0.0.0 for all entries in the source column?" question on page A-11.

If there is *no* NetFlow data on the Monitor pages, then you might be using an incompatible version of NDE. Make sure that the NDE version is 1, 5, 6, 7, or 8. For more information, see the "Why do the Monitor>Hosts and Monitor>Conversations pages have no active flow data?" question on page A-10.

Note NDE version v8-AS-Aggregation is not supported.

Q. Why are the **Monitor > Hosts**, **Monitor > Apps** and **Monitor > Conversations** pages showing data only every two (or more) auto refresh cycles?

A. This is caused by the implementation of the NDE source device. Entries in the NetFlow cache expire after a certain level of inactivity, if the end of a connection is detected, or if an expiration time is reached. The expired flow will still be exported to the destination. If the aging time is longer than the NAM refresh interval, no NetFlow packets will appear in one refresh interval of the NAM.

To solve this problem, choose **Setup > Preferences** and increase the auto refresh interval on the NAM, or change the aging time of the NetFlow entries. Before you change the aging time on the NDE source device, consult your NDE usage guidelines.

For devices running Cisco IOS, use the following commands to specify the aging time.

```
Prompt(config)#ip flow-cache timeout <active || inactive> <seconds>
```

or

```
Prompt(config)#mls aging <fast time || long || normal> <seconds>
```

For devices running Catalyst OS, use the following command to specify the aging time.

```
Prompt>(enable) set mls agingtime <long-duration || fast || ip>
```

Where:

- long-duration—Sets the aging time for flows that are long active.

- fast—Sets the aging time for flows that do not exceed packet thresholds.
- ip—Sets aging time for IP flows.

Q. Why are there no collections for a custom NetFlow data source?

A. Verify that the data source is setup on an interface with an Input direction. Output and Both directions are recommended only for special cases. They might require you to enable NetFlow on all interfaces to get comprehensive output direction flow data. For more information on NetFlow flow records, see the "Understanding NetFlow Flow Records" section on page 3-19.

You can verify the interface direction by clicking the Detail button on the NetFlow Listening Mode table. For more information on using the NetFlow Listening Mode, see the "Using the Listening Mode" section on page 3-27.

The custom NetFlow data source might also be collecting data on a wrong interface ifIndex. This is due to ifIndices in the remote NetFlow devices not being persisted after device reboots. It is recommended you use the ifIndex persist feature for any supported devices. For devices running Cisco IOS, the ifIndex can be persisted per interface or globally for all ifIndices.
For example:

- snmp ifindex persist
- snmp-server ifindex persist

For devices running Catalyst OS, ifIndices are always persisted.

Q. Why do the Monitor>Hosts and Monitor>Conversations pages have no active flow data?

A. Either the active flow has not expired, the device has an NDE filter, or the cache is full and new entries cannot be inserted into the cache. In any of these cases, the active flow is not in the NetFlow packets that are being exported to the NAM.

To solve this problem make sure there is no NDE filter on the device, check for long aging times, and check for dropped flow packets.

To check for long aging times to see if the active flow has expired, enter one of the following commands:

```
Prompt>(enable)show ip cache flow

Prompt>(enable)show mls netflow aging

Prompt>(enable)show mls
```

Active flows that have an active time *below* the long duration aging time are not yet expired and have not been exported to the NAM. You can set the aging time to a lower value. For information on how to do this, refer to the user documentation for the NDE device.

Q. Why is there no data for a NetFlow data source configured for specific interfaces, but there *is* data for the default NetFlow data source?

A. There might be no NetFlow record that has the specific interface information. Use the Listening Mode to find out what interfaces have NetFlow records.

Step 1 Choose **Setup > Data Sources > NetFlow> Listening Mode**.

Step 2 Click **Start**.

Step 3 Wait until the device table has more than three MDE packet counts.

Step 4 Select the device in interest.

Step 5 Click **Details**.

If the interfaces are not in the Details window, you must configure the NetFlow source device manually.

For Devices Running Cisco IOS

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

For Devices Running Catalyst OS

```
Prompt>(enable) set mls nde destination-ifindex enable
Prompt>(enable) set mls nde source-ifindex enable
```

Make sure the flow mask is set to full or interface-full.

Q. Why is only the local device address appearing in the drop-down list when I create a NetFlow data source from the **Setup** > **Data Sources** > **NetFlow** > **Custom Data Sources** page?

A. First you must add the device in the **Setup** > **Data Sources** > **NetFlow** > **Devices** page. A default NetFlow data source for the device is displayed on the **Setup** > **Data Sources** > **NetFlow** > **Custom Data Sources** page. The drop down list now contains the devices.

Q. Why is there no available interfaces list when I create a NetFlow data source?

A. Make sure the community string is correct. Use the Test button on the NetFlow Devices table on the **Setup** > **Data Sources** > **NetFlow** > **Devices** page. For more information, see the "Testing NetFlow Devices" section on page 3-25.

If there is an error, the community string might not be correct. Select the device from the NetFlow Devices table, click **Edit**, and enter the correct community string. Also make sure that the remote device accepts SNMP connections.

Q. Why does the Network Conversations table on the Monitor>Conversations page have 0.0.0.0 for all entries in the source column?

A. This is because the NDE device has the flow mask set to destination. To set the flow mask to full, interface-destination-source, or interface-full, use the following commands.

For Devices Running Cisco IOS

```
Prompt(config)#mls flow ip <full || interface-full>
```

For Devices Running Catalyst OS

```
Prompt>(enable) set mls flow full
```

Note The NAM supports NDE versions 1, 5, 6, 7, 8, and 9 source-prefix, destination-prefix, prefix, and protocol-port aggregations.

For more information on flow masks and the Monitor pages, see the "NDE Flow Masks and V8 Aggregation Caches" section on page 4-5.

Q. Why is NBAR not available on switches?

A. Although NBAR can be configured using the command line on the Catalyst 6500 switches, currently the switches do not provide the MIBs to configure and monitor NBAR.

Report Problems

Q. Why does my report not show any data for some or all of the time periods?

A. This could be for several reasons:

- The report might have been created recently and no data has been collected yet. It takes at least two polling intervals for the first data point to show up.
- The applicable traffic data source is not being sent to the NAM. For example, the SPAN session might have been configured improperly and it does not contain applicable traffic for the report. Go to **Setup > Data Source** to make sure that the data source for the report is properly configured.
- The report is disabled.
- The NAM was shut down or was not running during the time period.
- The report target is inactive.

Q. Why does the report status shows OK, but the report has no data during some or all of the time periods?

A. There might be an error condition or exception. From the reports window, select the tabular report style and click **system events** to view the report error conditions and exceptions. For more information on report error conditions and exceptions, see Table 5-15 on page 5-22.

Q. Why is there no data in all of my PortStat reports?

A. PortStat reports require the mini-RMON feature on the switch. Make sure that the switch supports mini-RMON and that it is enabled.

Q. Why is there no data in all of my VLAN reports?

A. Top N VLAN reports and target VLAN reports with the Supervisor engine module as a data source require the SMON feature in the switch Supervisor. Make sure that the Supervisor engine module supports the SMON feature and that it is enabled.

Q. Why does the data in my Response Time reports stay constant for multiple time periods?

A. You might have selected a reporting interval that is too long. Select **Setup > Monitor> Response Time Monitoring** and select a shorter report interval. It is recommended that you select the same polling interval as your Response Time reports. For example, if you select a 60 minute report interval and a 15 minute polling interval for your reports, the report data will be over-polled and the same data will repeat for every four consecutive 15 minute intervals.

Q. What happens to a report if I change the DNS resolution setting?

A. The Monitor window will not be able to see the report. If you create a report with DNS turned on, the report will be set up with the DNS name as the host. If you then turn DNS off, the Monitor window will look for the IP address instead of the DNS name.

Image Upgrade and Patch Issues

Q. How do I upgrade the application image of my NAM?

A. For NAM-1 and NAM-2 see the Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Installation and Configuration.

Note For NME-NAM see the *Network Analysis Module (NM-NAM) Feature Guide*.

Q. Why am I having problems upgrading my NAM image?

A. Verify the following:

1. The NAM booted into the correct partition
   - To upgrade the NAM application image, you must boot the NAM into the maintenance partition.
   - To upgrade the NAM maintenance image, you must boot the NAM into the application partition.
2. The URL specifies the correct image location. If it does not, enter the correct URL.
3. The upgrade was not interrupted. If it was, reboot the NAM and start the upgrade again.

Note For more information, see the *Network Analysis Module (NM-NAM)* feature module.

Q. Why am I having problems applying a patch?

A. Verify the following:

- Does the URL specify the correct image location? If not, enter the correct URL.
- Was the patch process interrupted? If so, start the process again.

Q. How can I verify which patches are installed on the NAM?

A. You can use the command-line **show patches** command or click **About** in the toolbar in the NAM Traffic Analyzer user interface.

Web Browser Response Time and Display Issues

Q. Why do my browser windows (such as the Packet Decode window or those under the Monitor tab) sometimes refresh so slowly?

Q. Why is the Packet Decoder window so slow in displaying packets?

A. You might need to verify that your DNS name servers point to valid DNS servers.

Tip
- If the name servers point to nonexistent or misconfigured DNS servers, lookups time out after 20 to 30 seconds.
- In an environment without DNS, no name servers should be configured.

  You also might need to turn off automatic hostname resolution:

Step 1 Choose **Setup > Preferences**.

Step 2 Deselect the Perform IP Host Name Resolution check box.

Step 3 Click **Apply**.

Note For more information, see the "Hostname Resolution Issues" section on page A-15.

The browser windows might also refresh slowly because of the amount of data to be sorted and displayed. Consider limiting your collection (such as the number of conversations) and reducing the maximum entries in the appropriate Monitoring window (in the Setup tab) to improve response time.

Q. Why does the formatting of my browser window or popup windows sometime look incorrect?

A. If browser displays are not formatted correctly, click your browser **Refresh** button. If popups are not formatted correctly, close and reopen the popup.

NAM Switch Date and Time Synchronization Issues

Q. Why are the NAM date and time different than the switch date and time?

A. When you boot the NAM, the NAM date and time are synchronized with the date and time on the switch. However, if the dates and times do not match, go to **Admin> System>NAM System Time** to synchronize the NAM system time with the switch or an NTP server. For more information on using the NAM System Time, see the "NAM System Time" section on page 2-14.

Q. Why does the NAM display an incorrect time when I change the time synchronization method from NTP to switch?

A. For Supervisors running Catalyst OS images earlier than 7.5(1), the NAM system time is synchronized with the switch only at startup. The NAM will not resynchronize time with the switch when you change from NTP time to switch time. To work around this problem, reset the NAM.

Diagnostic Error Message Issues

Q. What do these errors in the Diagnostics Tech Support window indicate?

```
Fri Nov 16 11:33:33 2001] [error] [client 172.20.9.52] File does not exist:
/usr/local/ apache/htdocs/scripts/..%2f../winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/MSADC/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/c/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/d/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/..%5c../winnt/system32/cmd.exe
```

A. These errors might indicate a virus-infected client searching for the next system to infect.

Some viruses look for vulnerabilities in a webserver running on port 80. Several remedies exist, including:

- Disinfecting clients (note their IP addresses).
- Implementing access control lists (ACLs) to prevent access to the NAM.
- Running the NAM webserver on a different port (because many virus attacks target only port 80.)

Hostname Resolution Issues

Q. Why did my importing of a remote hosts file fail when I used the **`ip hosts add ...`** command?

A. This might happen because:

- The hosts file is not formatted correctly. For more information see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note:*

  http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html

- The local hosts file is limited to 1000 entries. Verify that you are not trying to add more than 1000 entries. You can use the NAM CLI command **show tech-support**, then look for a line that reads;

  `Total number of entries in hosts files: nn`

Tip

- To review the entries configured in the file, use the **show hosts** command.
- If you need to add more than 1000 hosts, use DNS or select the 1000 most critical hosts for local name resolution.

Q. Why are there long delays during remote Telnet sessions to the NAM?

A. The problem might be with the DNS server address. The DNS server address must be set to the IP address of an operational DNS server. When the NAM cannot reach the server because of an incorrect address, inability to connect to the server, or a non-operational server, you might experience long delays.

To resolve this problem, change the DNS server to the IP address of a working server, or eliminate the server:

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

Step 2 In the contents, click **Network Parameters**.

Step 3 Change the parameters as needed.

Step 4 Click **Apply**.

You can also use the NAM CLI command **`ip nameserver`** *`nameserver_addr`* (to select a specific nameserver) or eliminate the nameserver completely with the command **`ip nameserver disable`**.

Q. Why are there long delays while waiting for diagnostic tech support output?

A. The problem might be with the DNS server address. To resolve this problem, change the DNS server to the IP address of a working server, or eliminate the server:

Step 1 Choose **Admin > System**.

Step 2 In the contents, click **Network Parameters**.

Step 3 Change the parameters as needed.

Step 4 Click **Apply**.

You can also use the NAM CLI command **`ip nameserver`** *`nameserver_addr`* (to select a specific nameserver) or eliminate the nameserver completely with the command **`ip nameserver disable`**.

Q. Are there restrictions on adding or deleting certain IP addresses to my local hosts file using the **`ip hosts add ...`** and **`ip hosts delete ...`** commands?

A. Yes. Do not add or delete host entries using the NAM IP address or IP addresses beginning with 127.*x.x.x*.

Data Mismatch Issues

Q. I clicked the Monitor tab, then **Hosts** or **Conversations**. The Network Host Table displayed. When I click a hostname, the data in the popup chart and tables sometimes do not match. Why does this happen?

A. The sources of the data used for the chart and tables in the detail popups are independent and might age out at different intervals.

HTTPS/Security Certificate Issues

Q. Why do I see warning messages that my certificate has expired when I point my web browser to the NAM using https?

A. This happens because your certificate has expired. To resolve this, you can either:

- Generate a self-signed certificate.
- Generate a certificate-signing request. Send the request to the certification authority, then install the certificate you receive.
- To do either of these, you use NAM CLI commands. For more information, see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note:*

  http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html

Q. What do I do when I see warning messages in my web browser that the name on the security certificate does not match the name of the site?

A. To resolve this, you can either:

- Generate a self-signed certificate—When doing so, enter **no** when asked whether to re-use the certificate-signing request. This generates a new certificate-signing request, then a self-signed certificate. Enter your hostname when prompted for the Common Name.
- Generate a certificate-signing request—Enter your hostname when prompted for the Common Name. Send the request to the certification authority, then install the certificate you receive.
- To do either of these, you use NAM CLI commands. For more information, see *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note:*

  http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/switch/configuration/guide/swconfig.html

  If you have done the above and still see the warning message, try to enter the full host name of the NAM in the browser address window. For example, if the full host name of the NAM is nam1.cisco.com, enter https://nam1.cisco.com instead of https:/nam1.

Q. What do I do when I see warning messages in my browser that the security certificate was issued by a company I have not chosen to trust?

A. View the certificate to determine whether you want to trust the certifying authority. You may see this message if the HTTPS certificate of the NAM is the factory (test) certificate, or a self-signed certificate. Click **Proceed**.

SNMP Issues

Q. Does the NAM support SNMPv3?

A. The NAM supports only SNMPv1 and SNMPv2c, including both external SNMP managers interacting with the NAM and the NAM interacting with the switch for mini-RMON port statistics and switch-based alarms.

Q. When I click **Test** on the Router Parameters dialog box, a window displays that SNMP read from the router failed.

A. You must verify that the SNMP read-write community strings entered are the same SNMP read-write community strings defined for the *router*. If the community strings are correct, and the test fails, verify that the router has IP permit list enabled.

For Switches Running Catalyst OS only

Step 1 Log into the switch in enable mode

Step 2 Enter `show IP permit`.

If IP permit list is enabled, verify that the internal address of the NAM is added to the list.

Note To view the NAM internal IP address from Traffic Analyzer, click **Test** from the Switch Community String dialog box under **Setup > Chassis Parameters**. The Switch Community String Test dialog box is displayed.

Enter **set IP permit** *NAM ip address* **SNMP**.

Q. Must I enable the NAM SNMP agent when I use the NAM Traffic Analyzer?

A. No. You only need the SNMP agent to support SNMP communication from external SNMP managers. To disable SNMP on the NAM:

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

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

Step 3 In the NAM Community Strings pane, select and delete all NAM community strings.

Q. When I set the timing buckets and report interval of an ART collection using SNMP, why do the settings of other ART collections also change?

A. NAM supports a global setting for ART timing buckets and report interval. So any settings you make using SNMP will apply to all ART collections. See Setting Up Response Time Configuration, page 3-54, for information about using the GUI to configure ART timing and report interval.

Note The method you use last overrides previous settings. So if you change the settings using SNMP, those settings will override the settings made using the GUI, and vice versa.

Protocol Support Issues

Q. Why do some protocols (such as sunrpc) sometimes appear twice in the application statistics windows?

A. Only the highest-level protocols are displayed. In some cases, a higher-level protocol might run on more than one lower layer protocol. For example, sunrpc might run on TCP and UDP. The NAM Traffic Analyzer would display two line items so you can differentiate between the two. Hold your mouse over the protocol and a small popup displays the full protocol stack involved.

Q. When I click the Monitor tab, then **DiffServ**, then **Application Stats**, I sometimes see a protocol such as http with a larger number of packets (or bytes) per second than the lower-layer protocol TCP. Why does this happen?

A. The differentiated services monitoring (DiffServ) statistics counts the packets only in the highest-level protocol possible. Therefore, a ...tcp.http packet counts as only an http packet. Packets classified as TCP mean that was the highest level the NAM could process. This might happen because it was an unrecognized TCP port or a state-based protocol in which the NAM did not detect a preceding packet to classify it.

Q. Where can I find a list of all protocols that the NAM supports?

A. A list of all protocols the NAM monitors is displayed in the Protocol Directory table under **Setup>Monitor**. You can also retrieve and modify the protocols using an SNMP tool.

Q. If I do not see a protocol listed on the **Setup>Capture>Settings** page, does that mean the NAM does not recognize that protocol, and it therefore is not displayed in the Monitor displays?

A. If the Protocols check box is selected and All is selected from the Protocols drop-down list, then all of the protocols the NAM can monitor will be listed in the selection box. You can use the Protocols drop-down list to select a more appropriate subset of protocols for your given environment.

Q. Are all of the protocols that the NAM tracks for Monitor displays (such as Monitor Apps, Monitor Overview) available for decode in the Capture Decode dialog box?

A. No. Decodes are available only for some of the protocols supported by the NAM. For additional decodes, you might consider using a third-party application. You can use the Capture Download feature to export your trace file to the third-party application.

Q. What does the protocol entry labeled *"others"* signify on some of the NAM web windows?

A. The protocol entry labeled *"others"* represents the sum of traffic for which the NAM was unable to identify the topmost application layer in the packet data. For example, these can be unrecognized TCP/UDP ports or dynamically assigned ports for which the NAM was not able to analyze the setup transactions. One way to gain more information is to use the capture capability of the NAM to capture packet data, then look for packets that cannot be fully decoded in the **Capture > Decode** window.

Voice Monitoring Issues

Q. Why are some columns blank in the detail windows that display VoIP phones and phone calls?

A. The amount of detail the NAM can provide for IP telephony traffic depends on the physical placement of the NAM relative to the IP phones, Call Managers, H.323 gatekeepers, and MGCP gateways. It also depends on what subset of traffic in the switch or router is being spanned or copied to the NAM. The NAM sometimes cannot directly observe the call setup transactions for phones on remote networks. In general, all detailed phone and call information that the NAM can observe is populated into the fields of the web displays.

Q. Why do some displays show that the phone protocol is SCCP (H.323 or MGCP) when it is really something else?

A. The protocol associated with a phone denotes the protocol by which the NAM initially *learned* about the phone, not necessarily the protocol used by that phone.

For example, if an SCCP phone calls an H.323 phone, and the NAM directly observes only the SCCP side of the call setup, it associates the SCCP protocol with both sides of the call because that is how the NAM learned about *both* phones.

Q. Why don't I see quality statistics (jitter, packet loss) for my SCCP phone calls?

A. For the NAM to report jitter and packet loss statistics for SCCP calls, Call Maintenance Records and Call Detail Records must be enabled on the Cisco Call Managers.

To turn on CMR and CDR in Cisco Call Manager 3.1, follow these steps:

Step 1 Go to the Cisco CallManager Administration window.

Step 2 Choose **Service > Service Parameters**.

Step 3 Choose the IP address of your Cisco CallManager server.

Step 4 Click the **Next** button.

Step 5 Choose the Cisco CallManager service.

Step 6 Choose **True** in the Parameter Value field for Call Diagnostics Enabled.

Step 7 Scroll down to the CdrEnabled service parameter and choose **True** for the value.

Step 8 Click the **Update** button.

Step 9 Call detail records start logging immediately.

Note This procedure is only valid on CallManager version 3.1, but other versions have a very similar process.

Q. What is the MGCP Endpoint in the **Monitor > Voice > Known Phones** window?

A. An MGCP Endpoint entry represents a MGCP gateway trunk port that one or more IP phones use to communicate with phones in the PSTN.

Q. Why do some MGCP Call Detail tables have Q.931 detail information?

A. When Cisco Call Manager and Cisco MGCP gateway traffic is copied to the NAM, the phone number and phone alias information for the MGCP calls might be obtained from Q.931 traffic. When this happens, the MGCP Call Detail table will have separated Q.931 table above it with detail information.

WAAS Application Response Time Issues

Q. Why is there no data in the response time monitor screens?

A. Response Time calculation requires that NAM sees traffic in both directions: from clients to servers and vice versa. If NAM sees traffic in one direction only, it will not be able to calculate and monitor response time. Check you SPAN configuration to make sure that NAM receives traffic in both directions. Also check if there is asymmetric routing in the network, in which returning traffic may follow a different path from originating traffic.

Q. Why does the WAAS device status remain *Inactive*?

A. Use the following WAAS CLI commands to enable the WAAS device to export flow data to the NAM for monitoring.

flow monitor tcpstat-v1 host <*NAM IP address*>

enable

Q. Why is there no data for the WAAS data source?
or
Why does the WAAS device status remain *Pending* and not *Active*?

A. Go to **Setup > Data Sources > WAAS > Monitored Servers** and make sure that you specify the correct application servers to be monitored (for example. web and FTP servers).

Note The monitored servers should be among the servers whose traffic is being optimized by WAAS.

Use the following WAAS CLI command to verify that you have configured the correct monitored servers:

show statistics flow filters

```
Number of Filters:        7
  Status:                   Enabled
  Capture Mode:             FILTER

  Flags:
  CSN: Client-Side Non-Optimized (Edge), SSO: Server-Side Optimized (Edge)
  CSO: Client-Side Optimized (Core), SSN: Server-Side Non-Optimized (Core)
  PT: Pass Through (Edge/Core/Intermediate), IC: Internal Client

      Server             Flow Hits                     Flags
  ---------------  ---------------------  ----------------------------------
  172.20.107.123                     120  CSO SSN
  1.2.3.4                              0  CSO SSN
  10.96.1.2                            0  CSO SSN
  10.31.10.1                           0  CSO SSN
  10.31.10.2                           0  CSO SSN
```

If the WAAS CLI command **show statistics flow filters** output shows ***zero flow hits*** for the servers, these servers have no traffic being optimized, and the WAAS device has no data to export to the NAM to be monitored. In this case, check your WAAS configuration to determine which servers are being optimized, and configure the NAM to monitor these servers.

Finally, make sure you configure the correct data sources for the WAAS devices. Typically, you should configure the Client data sources for wide-area edge (WAE) edge devices and configure Server and Server WAN data sources for WAE core devices. See the section Configuring WAAS Data Sources, page 3-35, for more information.

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

Cisco Wide Area Application Services Configuration Guide, OL-16376-01
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4019/configuration/guide/waas4cfg.html