CHAPTER 5

Troubleshooting the NAM

This chapter provides troubleshooting information for the NAM, and includes these sections:

- Netflow Data Export, page 5-1
- Error Messages, page 5-8
- Web Username and Password Guidelines, page 5-13
- Supported MIB Objects, page 5-15
- Local Interfaces in the NAM ifTable, page 5-19

Note Additional troubleshooting help is available to the NAM Traffic Analyzer application users in the online help "Troubleshooting" section.

Netflow Data Export

This section contains troubleshooting information for NDE.

Web Application

Explanation When you are on the Monitor>Hosts, Monitor>Apps, or Monitor>Conversations page, the data shows only every other or more auto-refresh cycles. This problem is caused by the implementation operation of the NDE source device. Entries in the NetFlow cache are expired after being inactive for a time, or when the end of a connection is detected, or the expiration time has reached. The expired flow is exported to the destination. If the aging time is longer than the NAM refresh interval, there will be no expired flows and NetFlow packets flow in one refresh interval of the NAM.

Recommended Action To solve the problem, either increase the auto refresh interval on the Setup>Preferences menu, or change the aging time of the NetFlow entries. However, before you make any change to the aging time at the NDE source device, refer to the NDE usage guidelines for performance issues.

Cisco IOS:

For the MSFC or routers, use the following command to specify the aging time.

```
Router(config)# ip flow-cache timeout "active"||"inactive" seconds
Router(config)# mls aging "fast time" | "long" | "normal" seconds
```

Catalyst Operating System:

For the PFC, use the following commands to specify the aging time.

```
Router(enable) set mls agingtime [long-duration | fast | ip]
```

To set the aging time for flows that are long active, use the **long-duration** keyword.

To set the aging time for flows that does not exceed packets threshold, use the **fast** keyword.

To set aging time for IP flows, use the **ip** keyword.

Explanation The Monitor>Hosts and Monitor>Conversations page does not contain data of an active flow. This problem could be caused if the active flow is not expired yet, if the device has an NDE filter, or if a full cache is preventing insertion of new entries. The active flow is not in the NetFlow packets that are exporting to the NAM.

Recommended Action Check for filter, for long duration aging time, or for dropped flow packets as follows:

Verify for long duration aging time with these commands:

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

or

```
Router>(enable) show mls netflow aging
```

or

```
Router>(enable) show mls
```

Active flows that have active time below the long duration aging time are not expired yet, and they have not been exported to the NAM. The aging time could be set to lower value. Refer to the NDE usage guidelines for the device.

Verify for flow packets dropped with these commands:

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

or

```
Router>(enable) show mls netflow aging
```

or

```
Router>(enable) show mls
```

Flows could be dropped because they are not entered into the caches allowing their export to the NAM when they are expired. This condition may be that the NetFlow cache is full because of busy networks. To correct the problem, you could increase the cache sized. An alternative is to adjust NDE export with NDE flow mask or version 8 aggregation cache. Refer to the NDE usage guidelines for the device.

Explanation There is no data for the default NetFlow data source of the device.

Recommended Action In the GUI, go to the Setup>Data Sources>NetFlow>Listening Mode page and click on the Start button. Wait for a few auto refresh cycles. If the device is not displayed in the table, the NAM is not receiving any NetFlow packets from the device. This condition could be a network problem, or the device may not be configured correctly.

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

```
Router# show ip flow export
```

or

```
Router# show mls nde
```

Displayed information should show whether or not NetFlow export is enabled or disabled and show the IP address and port to which the NetFlow packets are being exported. If the information is not correct, refer to the configuration section in the User Guide for the *Network Analysis Module Traffic Analyzer Release 3.1* to correct it.

Explanation There is no data for NetFlow data sources that are configured for specific interfaces, but the default NetFlow data source for the device has data.

Recommended Action This problem could occur because there a NetFlow record does not exist that has the specified interfaces information. To find out what interfaces that NetFlow records have, do the following:

Step 1 Go to the Setup>Data Sources>NetFlow>Listening Mode screen.

Step 2 Click **Start** to initiate the listening process.

Step 3 Wait until the row for the device has more than three NDE packets counted.

Step 4 Select the device.

Step 5 Click **Details**. A window appears displaying a list of interfaces that the NAM has seen in the NDE packets.

Step 6 Make sure that the interfaces selected for the NetFlow devices are included in the list. If the interfaces are not included in the list, configure the NetFlow source devices using the following commands:

For the IP routed cache use these commands:

```
Router(config)# interface type slot/port
Router(config-if)# ip route cache flow
```

For MLS cache:

Cisco IOS:

```
Router(config)# mls nde interface
```

Catalyst operating system:

```
Console>(enable) set mls nde destination-ifindex enable
```

or,

Catalyst operating system:

```
Console>(enable) set mls nde source-ifindex enable
```

Make sure that the flow mask is set to “full,” “interface-destination-source,” or “interface-full.”

If the information is not correct, refer to the configuration section in the User guide for *Network Analysis Module Traffic Analyzer Release 3.1* to correct it.

Explanation When creating a NetFlow data source from the Setup>Data Sources>NetFlow>Custom Data Sources screen, only the local device's address appears in the drop down box.

Recommended Action A device is created in the Setup>Data Sources>NetFlow>Devices screen. After adding a device from this screen, a default NetFlow data source for the device appears in the Setup>Data Sources>Netflow>Custom Data Sources screen. Now, the drop down box displays the device address included in the list.

Explanation When creating a NetFlow data source, no available interfaces list is displayed.

Make sure the provided community string is correct by doing the following:

Step 1 Go to the Setup>Data Sources>NetFlow>Devices menu.

Step 2 Click on the radio button of the device to display interfaces information.

Step 3 Click **Test**.

A pop up window appears displaying the status of the device. If there is error in this window, the community string may not be correct. Correct the community string by selecting the device, click **Edit**, and provide the correct community string. Also, ensure that the remote device accepts SNMP connections.

Explanation Monitor>Conversations page has the source column being 0.0.0.0 for all entries. This problem occurs due to the NDE device flow mask being set to "destination."

To set the flow mask to "full," "interface-destination-source," or "interface-full," do the following:

For Cisco IOS:

```
Prompt(config)# mls flow ip "full"||"interface-destination-source"||"interface-full"
```

For the Catalyst operating system:

```
Router(enable) set mls flow "destination-source" || "full"
```

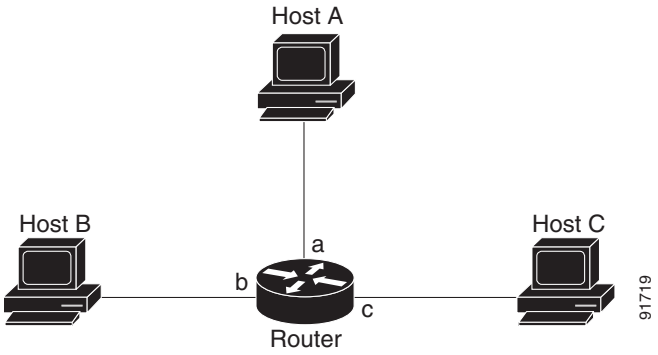
Note The NAM supports NDE versions 1, 5, 6, 7, 8, source-prefix, destination-prefix, prefix, and protocol-port aggregations.

NDE Flow Records Interfaces

Explanation An NDE packet has multiple NDE flow records. Each flow record has fields of flow input SNMP if-index and flow output SNMP if-index. The information may not be available due to unsupported NDE feature of the Cisco IOS or Catalyst operating system version, or NDE flow masks configuration.

Figure 5-1 and Figure 5-2 show the network configuration for this situation, and Table 5-1 and Table 5-2 show the reporting flow records.

Figure 5-1 NDE Configuration



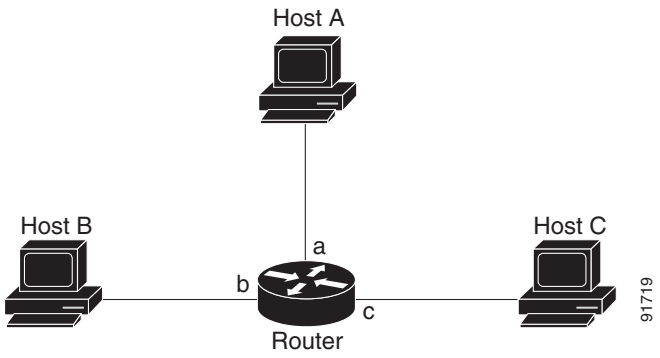
The configuration is as follows:

```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router config)# exit
Router#
```

Table 5-1 Reporting Flow Records

Input Interface	Output Interface	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	No
b	a	No
c	a	No
c	b	No

Figure 5-2 NDE Configuration




```
Router# configuration terminal
Router(config)# interface a
Router(config-if)# ip route cache flow
Router(config-if)# exit
```

```
Router(config)# interface b
Router(config-if)# ip route cache flow
Router(config-if)# exit
Router(config)# ip flow export destination NAM-Address 3000
Router(config)# exit
Router#
```

Table 5-2 Reporting Flow Records

From	To	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	Yes
b	a	Yes
c	a	No
c	b	No

Recommended Action In most cases, turning on NetFlow on an interface will populate the NetFlow cache in a switch or router with flows that are in the input direction of the interface. As a result, the input SNMP if-index field in the flow record will have the if-index of the interface that has NetFlow turned on.

Interface Special (0)

Explanation NDE packets sometimes have NetFlow records reporting either or both input if-index and output if-index fields being 0. This may be due to one or more of the following reasons:

- Flows that are terminated at the device.
- Configurations of the device.
- Unsupported NetFlow feature of the platform at the device.

Recommended Action Remove flows terminated at the device, check the device configuration, make sure there are no unsupported features on this platform at the device.

NDE Flow-mask and v8 Aggregation Cache

This section describes how some of the flow-masks and NDE version 8 aggregation flows affect the data collection screens in the NAM. Table 5-3 lists these affects. Due to lack of information, some collections may have “Others” only in the Monitor>Apps, 0.0.0.0 in Monitor>Hosts and Monitor>Conversation pages.

Table 5-3 Affects on Data Collection Screens

Flow	Affect
Full flow-mask is supported	Highly recommended. Refer to the NDE usage guidelines for the device to apply full flow-masks. **Note** Although the NAM supports NDE aggregation, the information you receive for a specified aggregation type is limited to that aggregation and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode.
Destination only flow-mask.	• Monitor>Apps displays "Others" only. • Monitor>Apps detail popup screen has no data. • Monitor>Hosts has 0.0.0.0. Detail popup screen has no data. • Monitor>Conversations has 0.0.0.0 to some hosts. Detail popup screen has no data. • Support NetFlow custom data sources that are set up for specific interfaces.
Destination-Source flow-mask.	• Monitor>Apps displays "Others" only. • Monitor>Apps detail popup screen has no data. • Monitor>Hosts has data. Detail popup screen has no data. • Monitor>Conversations has data. Detail popup screen has no data. • Support NetFlow custom data sources that are set up for specific interfaces.
NDE version 8-Protocol-Port-Aggregation.	• Monitor>Apps displays data. • Monitor>Apps detail pop up displays no data. only 0.0.0.0. • Monitor>Host displays only 0.0.0.0. • Monitor>Conversation displays only 0.0.0.0 to 0.0.0.0. • No data for custom NetFlow data sources that are setup for some specific interfaces. • No DiffServ other than TOS 0 and DSCP 0. • Setup>Data Sources>NetFlow Listening Mode detail popup screen does not display interfaces information.
NDE version 8-Destination-Prefix-Aggregation	• Monitor>Apps displays only "Others." • Monitor>Host displays data with subnets as well as 0.0.0.0. The detail pop up screen displays no data. • Monitor>Conversation displays data with 0.0.0.0 to subnets (as well as 0.0.0.0 to 0.0.0.0). Detail pop up screen displays no data. • Support NetFlow custom data sources that are set up for specific interfaces. • No DiffServ other than TOS 0 and DSCP 0.

Table 5-3 Affects on Data Collection Screens (continued)

Flow	Affect
NDE version 8-Prefix-Aggregation.	• Monitor>Apps displays “Others” only. • Monitor>Host displays data as subnets (as well as 0.0.0.0). The detail pop up screen displays no data. • Monitor>Conversation displays data (as well as 0.0.0.0 to 0.0.0.0). Detail pop up screen displays no data. • Support NetFlow custom data sources that are setup for specific interfaces. • No DiffServ other than TOS 0 and DSCP 0.
NDE version 8-Source-Prefix-Aggregation	• Monitor>Apps displays “Others” only. • Monitor>Host displays data with subnets (as well as 0.0.0.0). The detail pop up screen displays no data. • Monitor>Conversation displays data with subnets to 0.0.0.0 (as well as 0.0.0.0 to 0.0.0.0). Detail popup screen displays no data. • Support NetFlow custom data sources that are set up for specific interfaces. • No DiffServ other than TOS 0 and DSCP 0.
NDE version 8-AS-Aggregation	Not supported.

Error Messages

Symptom When a **reset** command is entered from the supervisor CLI, the system always boots into the maintenance image.

Possible Cause If the boot device is configured in the supervisor as cf:1, typing a **reset** *module* command always boots to the maintenance image.

Recommended Action Override the configured boot device in the supervisor by entering the boot string during reset.

- In Cisco IOS software, to boot to the application image, use the **hw-module mod 9 reset hdd:1** command.
- In Catalyst operating system software, to boot to the application image, use the **reset 9 hdd:1** command**.**

Symptom You receive a verification failed message when installing a patch on the NAM.

Possible Cause The time and date on the NAM are not correct; the patch is not the same as an official Cisco patch; the patch might be of the previous release of NAM; the FTP process may have failed; or the FTP image being pointed to is not a patch (it may be a full application image).

Recommended Action Be sure that the signature verification is used to ensure that the patch is an authentic Cisco patch. Be sure that the patch is for the correct NAM release. For example, a patch for the NAM 2.2 release cannot be applied to a NAM running the NAM 3.1 software. Be sure the date and time on the NAM either is set to synchronize with the switch or with the Network Time Protocol (NTP). Make sure the URL location is valid for the patch (username in particular)

Symptom You are unable to log into the maintenance image with the same password for the NAM application image.

Note This message is applicable only for the WS-SVC-NAM-1 and the WS-SVC-NAM-2 modules.

Possible Cause The NAM application image and the maintenance image have different password databases for the root and guest accounts. The default passwords for root and guest differ between the maintenance image and the NAM application image. Any password change performed in the NAM application image does not change the maintenance image password and vice versa.

Recommended Action Use the maintenance image password.

Symptom You lost your password for the maintenance image and want to recover it.

Possible Cause The maintenance image does not support resetting passwords from the switch. Upgrading the maintenance image sets the password for root and guest to default in the maintenance image.

Recommended Action Use the default maintenance image passwords. Refer to Table 4-1 on page 4-2 or Table 4-5 on page 4-12.

Symptom When attempting to load the new NAM 3.1 image on the NAM the following message is received:

```
Incompatible image! Upgrade aborted.
```

Possible Cause This image is not supported on the specified NAM. There are three NAM 3.1 images available: One each for the WS-SVC-NAM-1, WS-SVC-NAM-2 and one for the WS-X6380-NAM. This symptom occurs only if an incompatible image is used.

Recommended Action Do not use the NAM software release 2.2 image on the WS-X6380-NAM. The application and maintenance file image formats are different between the WS-X6380-NAM and the newer WS-SVC-NAM-1 and WS-SVC-NAM-2. The newer NAM shares a common format and the same image filename for upgrades can be used.

Symptom When attempting to load the WS-X6380-NAM image on a WS-SVC-NAM-1 or WS-SVC-NAM-2 the following message is received:

```
ERROR: /tmp/upgrade:No space left on device
```

Possible Cause This image is not supported on the specified NAM. There are three NAM 3.1 images available: One each for the WS-SVC-NAM-1, WS-SVC-NAM-2 and one for the WS-X6380-NAM. This symptom occurs only if an incompatible image is used.

Recommended Action Do not use the WS-X6380-NAM image on a WS-SVC-NAM-1 or WS-SVC-NAM-2. The application and maintenance file image formats are different between the WS-X6380-NAM and the newer WS-SVC-NAM-1 and WS-SVC-NAM-2. The newer NAM shares a common format, and the same image filename for upgrades can be used between these newer modules.

Symptom A SPAN session does not show up in the Traffic Analyzer **Active SPAN** window.

Possible Cause In Catalyst operating system software, a SPAN session becomes inactive if the module containing the destination port is removed from the switch chassis. The NAM is not seen by the SPAN session because the SPAN configuration is removed from the SNMP agent by the supervisor engine.

Recommended Action Replace the module.

Symptom In Cisco IOS software, a SPAN create request failed for a partially configured SPAN session.

Possible Cause The NAM does not see this partial SPAN session, or the SPAN create request can fail if there is a conflict in either the source type or destination port.

Recommended Action Because SPAN session can be partially defined with either source or destination only, reconfigure the SPAN session with both a source and destination.

Symptom When the NAM initially boots, by default it runs a partial memory test and you want to run a complete memory test.

Possible Cause The partial memory test is the default configuration.

Recommended Action To perform a full memory test, enter the **hw-module module** *module_number* **reset** *device:partition* **mem-test-full** command.

Note A full memory test takes significantly more time to complete.

This command is specific to Cisco IOS and is not available in Catalyst operating system software. (See the "Resetting the NAM" section on page 4-15.)

You can also use the **hw-module module** *module_number* **mem-test-full** command. For example:

```
Router(config)# hw-module module 5 mem-test-full
```

For the Catalyst operating system software, you can enable a full memory test when you use the **set boot device** *bootseq mod#* **mem-test-full** command. This option is disabled by default. For example:

```
Console (enable) set boot device cf:1 4 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning:Device list is not verified but still set in the boot string.

Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to FULL
```

This example shows how to reset the partial memory test:

```
Console> (enable) set boot device cf:1 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
Warning:Device list is not verified but still set in the boot string.
Console> (enable)
Console> (enable) show boot device 4
Device BOOT variable = cf:1
Memory-test set to PARTIAL
```

Symptom When you click the **Test** button in the **Set up>Switch Parameters** menu window, the popup window indicates that both the SNMP read and write to the switch failed.

Possible Cause Verify that the SNMP read-write community string entered is the same as the SNMP read-write community string defined for the switch.

Note The password is case sensitive.

Recommended Action If the community string is correct and the test still fails, check that the switch has enabled the IP permit list as follows:

Step 1 Log in to the switch in enable mode.

Step 2 Enter the **show IP permit** command.

If the IP permit list is enabled, make sure that the NAM internal address is added to the IP permit list. The NAM address is 127.0.0.X, where X is the NAM module number times 10+1. For example, if the NAM is at module 4, then its address should be 127.0.0.41.

After you determine the NAM internal IP address, go to Step 3.

Step 3 Enter the **set IP permit NAM-address SNMP** command.

Symptom When a NAM is running in a switch with Catalyst operating system software, the NAM may be shown as unreachable when you use the **ping** command or the NAM Traffic Analyzer application.

Possible Cause The NAM IP address and the IP address of the switch (interface sc0) are not in the same subnet. This problem can occur if you change the switch IP address and the NAM VLAN assignment. The NAM automatically synchronizes its VLAN assignment to the same VLAN in which the switch (interface sc0) resides. When this occurs, the NAM IP address resides on a

different subnet from the VLAN assigned to the NAM. The router then drops any packet destined to the NAM IP address. You cannot add a static route to the router because of route overlap caused by improper VLAN assignments and subnetting.

Recommended Action Make sure that the NAM IP address and the switch are in the same subnet and in the same VLAN.

Symptom You cannot connect to the NAM.

Possible Cause The initial configuration is incorrect or not configured.

Recommended Action Reconfigure the NAM as described in the "Configuring the NAM" section on page 3-1.

Symptom You cannot connect to the NAM Traffic Analyzer application.

Possible Cause The configuration for the HTTP server is not correct.

Recommended Action Check the NAM configuration for the HTTP server as described in the "Configuring the HTTP or HTTP Secure Server" section on page 3-21.

Symptom The NAM fails to upgrade.

Possible Cause The URL to the server or the image name is incorrect.

Recommended Action Make sure the URL you specified is valid. Make sure the image name you specified in the URL is an official Cisco image name.

Symptom You cannot enable the HTTP server.

Possible Cause No web users are configured, or a secure server is already enabled.

Recommended Action Configure web users as described in the "Configuring the HTTP or HTTP Secure Server" section on page 3-21.

Symptom After configuration, the TACACS+ authentication and authorization fails.

Possible Cause There are three possible causes: the name and password do not match the login configuration in the TACACS+ server; the TACACS+ secret key configured in the NAM does not match the secret key configured in the server; and the wrong TACACS+ server IP address is configured in the NAM.

Recommended Action To determine the cause to take the appropriate course of action follow these steps:

Step 1 Log in as a local user.

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

Step 3 Scroll down to view the /var/log/messages area.

Step 4 Look for the following messages near the end of the log and take the recommended actions:

```
...PAM-tacplus[612]:auth failed:Login incorrect
```

Possible Cause The name and password do not match the login configuration in the TACACS+ server.

Recommended Action Log in to the TACACS+ server and configure the authenticate and authorize NAM user. (See the TACACS+ documentation for information on login configuration.)

```
...httpd:tac_authen_pap_read:invalid reply content, incorrect key?
...PAM-tacplus[616]:auth failed:Authentication error, please contact
administrator.
```

Possible Cause The TACACS+ secret key configured in the NAM does not match the key in the TACACS+ server.

Recommended Action Choose **Admin > User > TACACS+** and enter the correct secret key.

```
...httpd:tac_connect:connection to 172.18.122.183 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
```

Possible Cause The wrong TACACS+ server IP address is configured on the NAM.

Recommended Action Choose **Admin > User > TACACS+** and enter the correct TACACS+ server address.

Symptom The TACACS+ user can log in successfully but receives the "Not authorized..." error messages when accessing NAM Traffic Analyzer application.

Possible Cause You do not have the necessary access rights.

Recommended Action Log in to the TACACS+ server and grant access rights to the affected users. (See the TACACS+ documentation for information on login configuration.)

Web Username and Password Guidelines

Observe the following web username and password guidelines:

- You cannot use the CLI username (root or guest) and password to log into the NAM Traffic Analyzer application because they are administered separately. You also cannot use your NAM Traffic Analyzer application username and password to log into the NAM CLI.

  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.

- You can use TACACS+ in addition to a local database or instead of a local database. (The local database is always checked first.) To use only TACACS+, eliminate the local database users by either of these methods:
  - Use the NAM CLI **rmwebusers** command to remove only local users, not TACACS+ users, because they are administered separately on the TACACS+ server.
  - From the **Admin** tab, click **Users**, and 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 application as a TACACS+ user.

- 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 password if no TACACS+ server is configured on the NAM, follow these steps:

Step 1 Access the NAM CLI.

Step 2 Remove all web users by entering:

```
rmwebusers
WARNING: Doing this will stop the web server and remove
all locally defined web users from web user database.

Are you sure you want to continue (y/n) [n]? y

Disabling HTTP server...
Successfully disabled HTTP server.

All locally defined web users have been
removed from web user database.
root@namlab-kom2.cisco.com#
```

Step 3 Start the HTTP (or HTTPs, if applicable) server by entering:

```
ip http server enable
ip http secure server enable
```

Step 4 At the prompt, enter the web admin username and password.

You can now log in using the new admin account and create other web accounts by clicking the **Admin** tab, then clicking **Users**.

To recover the password if the TACACS+ server is configured on the NAM, follow these steps:

Step 1 Log into the NAM Traffic Analyzer application as a TACACS+ user.

You must be configured on the TACACS+ server with Account Management permission.

Step 2 Change the password of the local web admin user.

Note If a TACACS+ server has been configured and the local web user account is deleted, you can still create the web admin user on the TACACS+ server. In this case, the admin user created on the TACACS+ server can log into the NAM Traffic Analyzer application and change the password of the local web admin user, you do not need to create another admin user.

When the TACACS+ configuration may become confused between the NAM and the TACACS+ server, and a local database user account is not available to fix the TACACS+ configuration on the NAM, you may not be able to fix this problem from the TACACS+ server. To recover the passwords, follow these steps:

Step 1 Access the NAM CLI.

Step 2 Enter these commands:

```
rmwebusers
ip http tacacs+ disable
ip http server enable
```

(or **ip http secure server enable** if using HTTPs)

Step 3 When prompted, enter the new local database admin username and password.

Step 4 Log into the NAM Traffic Analyzer application.

Step 5 Click the **Admin** tab.

Step 6 Click **Users**.

Step 7 In the contents, click **TACACS+**.

Step 8 Enter the correct information.

Step 9 Click **Apply**.

There are restrictions on using passwords when performing upgrades or applying patches. Do not include the password as an argument in upgrade and patch commands. Use the following command syntax:

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

Enter the password when prompted for it.

Supported MIB Objects

Table 4 lists the RMON and RMON2 MIB objects supported by the supervisor engine and the NAM. The supervisor engine implements some objects from the RMON MIBs as specified in Table 4. The supervisor engine RMON implementation is completely independent of the NAM implementation, and no MIB objects are shared.

To collect etherStats from a physical interface on the switch, configure the etherStatTable on the supervisor engine instead of on the NAM. The etherStats are collected accurately on multiple physical interfaces simultaneously.

If you are interested in the etherStats for a specific VLAN, configure the etherStatsTable on the NAM. For the data source, use the ifIndex corresponding to that VLAN.

Any alarmVariable configured on the supervisor engine must reference a MIB object on the supervisor engine. An alarmVariable configured on the NAM must reference a MIB object on the NAM.

Note You cannot configure an alarmVariable on the NAM that references a MIB object on the supervisor engine or configure an alarmVariable on the supervisor engine that references a MIB object on the NAM.

Table 4 Supervisor Engine Module and NAM RMON Support

Module	Object Identifier (OID) and Description	Source
Supervisor Engine	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)...mib-2(1).rmon(16).statistics(1).tokenRingMLStatsTable(2) ...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)	RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Counters for packets, octets, broadcasts, errors, etc.	
Supervisor Engine	...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2) ...mib-2(1).rmon(16).history(2).tokenRingMLHistoryTable(3) ...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4)	RFC 2819 (RMON-MIB) RFC 2819 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Periodically samples and saves statistics group counters for later retrieval.	
Supervisor Engine	...mib-2(1).rmon(16).alarm(3)	RFC 2819 (RMON-MIB)
	A threshold that can be set on critical RMON variables for network management.	
Network Analysis	...mib-2(1).rmon(16).alarm(3)	RFC 2819 (RMON-MIB)
	A threshold that can be set on critical RMON variables for network management.	
Network Analysis	...mib-2(1).rmon(16).hosts(4)	RFC 2819 (RMON-MIB)
	Maintains statistics on each host device on the segment or port.	
Network Analysis	...mib-2(1).rmon(16).hostTopN(5)	RFC 2819 (RMON-MIB)
	A user-defined subset report of the Hosts group, sorted by a statistical counter.	
Network Analysis	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	RFC 2819 (RMON-MIB)
Network Analysis	...mib-2(1).rmon(16).matrix(6)	RFC 2819 (RMON-MIB)
	Maintains conversation statistics between hosts on a network.	
Network Analysis	...mib-2(1).rmon(16).filter(7)	RFC 2819 (RMON-MIB)
	A filter engine that generates a packet stream from frames that match a specified pattern.	

Table 4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
Network Analysis	...mib-2(1).rmon(16).capture(8)	RFC 2819 (RMON-MIB)
	Manages buffers for packets captured by the Filter group for uploading to the management console.	
Supervisor Engine	...mib-2(1).rmon(16).event(9)	RFC 2819 (RMON-MIB)
	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	
Network Analysis	...mib-2(1).rmon(16).event(9)	RFC 2819 (RMON-MIB)
	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	
Supervisor Engine	...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1) ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2) ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5) ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)	RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Aggregates detailed Token Ring statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDir(11)	RFC 2021 (RMON2-MIB)
	A table of protocols for which the Network Analysis Module monitors and maintains statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDist(12)	RFC 2021 (RMON2-MIB)
	A table of statistics for each protocol in protocolDir(11).	
Network Analysis	...mib-2(1).rmon(16).addressMap(13)	RFC 2021 (RMON2-MIB)
	List of MAC-to-network-layer address bindings.	
Network Analysis	...mib-2(1).rmon(16).nlHost(14)	RFC 2021 (RMON2-MIB)
	Statistics for each network layer address.	
Network Analysis	...mib-2(1).rmon(16).nlMatrix(15)	RFC 2021 (RMON2-MIB)
	Traffic statistics for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).alHost(16)	RFC 2021 (RMON2-MIB)
	Statistics by application layer protocol for each network address.	
Network Analysis	...mib-2(1).rmon(16).alMatrix(17)	RFC 2021 (RMON2-MIB)
	Traffic statistics by application layer protocol for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).usrHistory(18)	RFC 2021 (RMON2-MIB)
	Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.	

Table 4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
Supervisor Engine	...mib-2(1).rmon(16).probeConfig(19).	RFC 2021 (RMON2-MIB)
	Displays a list of agent capabilities and configurations.	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). dataSourceCaps(1).dataSourceCapsTable(1).	RFC 2613 (SMON-MIB)
	Maps physical entities and VLANs to ifEntries.	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonVlanStatsControlTable(1).	RFC 2613 (SMON-MIB)
	Traffic statistics by VLAN ID number.	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1). smonStats(2).smonPrioStatsControlTable(3).	RFC 2613 (SMON-MIB)
	Traffic statistics by 802.1p user priority value.	
Network Analysis	...frontier(141).mibdoc2(2).netscout2(1).art(5).artControlTable(2).	draft-warth-rmon2-artmib-01.txt
	Application response time statistics.	(ART-MIB)
Network Analysis	...mib-2(1).rmon(16).mediaIndependentStats(21).	RFC 3273 (HC-RMON-MIB)
	Counters for packets, octets, broadcasts, errors, etc.	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonMaxAggGroups(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlLocked(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlChanges(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). .dsmonAggControlLastChangeTime(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggControlTable(5) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonAggProfileTable(6) rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). .dsmonAggGroupTable(7)	RFC 3287 (DSMON-MIB)
	Aggregation or profile control variables and tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsControlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsTable(2)	RFC 3287 (DSMON-MIB)
	Per-datasource statistics collection tables	

Table 4 Supervisor Engine Module and NAM RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
	rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistStatsTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistTopNTable(4)	RFC 3287 (DSMON-MIB)
	Per-protocol statistics collection tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNCtlTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostTopNTable(4)	RFC 3287 (DSMON-MIB)
	Per-host statistics collection tables	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5). dsmonCapabilities(1)	RFC 3287 (DSMON-MIB)
	DSMON capabilities variable	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixCtlTable(1) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixSDTable(2) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixDSTable(3) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNCtlTable(4) rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6). dsmonMatrixTopNTable(5)	RFC 3287 (DSMON-MIB)
	Matrix statistics collection tables	

Local Interfaces in the NAM ifTable

There are three versions of the Network Analysis Module (NAM) for the Catalyst 6500 Series switch. These are:

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

This section explains the differences between the newer NAM-1 and NAM-2 and the previous version the WS-X6380-NAM and how to configure and manage the NAM-1 and NAM-2 in respect to their management and data ports for SNMP and CLI as seen both from the NAM and the Supervisor module.

The WS-X6380-NAM shows up in the Supervisor CLI and ifTable as two ports. The first port is the data port, used for receiving SPAN traffic. The second port is the management port. On the NAM these two ports show up in the ifTable as the first two ports (with ifIndex.1 for data and ifIndex.2 for management).

The WS-SVC-NAM-1 shows up in the Supervisor CLI (in the Catalyst operating system) and ifTable as three ports. The first port is unused. The second port is the management port. The third port is the data port (for receiving SPAN traffic). The Supervisor CLI (in Cisco IOS) abstracts the ports ("analysis module . . ."). On the NAM's ifTable the management port shows up as the first port (ifIndex.1) and the data port shows up as the second (ifIndex.2).

The WS-SVC-NAM-2 shows up in the Supervisor CLI (in the Catalyst operating system) and ifTable as eight ports. Ports 1, 3, 4, 5, and 6 are unused. Port 2 is the management port (the same as on WS-SVC-NAM-1). Ports 7 and 8 are both data ports and can be SPAN targets. The Supervisor CLI (in Cisco IOS) abstracts the ports ("analysis module . . ."). On the NAM's ifTable the interfaces are as follows:

- ifIndex.1: Is designated the management port.
- ifIndex.2: Represents the traffic from both data ports (also known as "All SPAN").
- ifIndex.3: Represents the traffic from the first data port (named "data port 1")
- fIndex.4: Represents the traffic from the second data port (named "data port 2")

Note For WS-SVC-NAM-1 and WS-SVC-NAM-2 the data ports are 802.1q trunk ports. Packets are received with an 802.1q header (except for packets with the ports native VLAN Id), affecting offsets (for example filters on IP headers) in packets.

Table 5-5 NAM Local Interface Designations

	WS-X6380-NAM	WS-SVC-NAM-1	WS-SVC-NAM-2
SNMP OID	cisco.5.1.3.1.1.2.223	cisco.5.1.3.1.1.2.914	cisco.5.1.3.1.1.2.291
Supervisor engine number of ports	2	3	8
Supervisor engine management port	2	2	2
Supervisor engine data ports	1	3	7,8
NAM management port	ifIndex.2	ifIndex.1	ifIndex.1
NAM data port	ifIndex.1	ifIndex.2	ifIndex.2, ifIndex.3, ifIndex.4

Explanation When I import a configuration using "config network", the download of configuration file goes through fine, but import operation failed giving an error.

Recommended Action Use the **show log config** command to determine where exactly the configuration failed. Depending on the seriousness of failure you could either ignore or correct the configuration file and try the **config network** command again.

Explanation From NAM-1 or NAM-2 application image tried to upgrade Maintenance image, I got this error: Image verification failed.

```
The image you are trying to upgrade is not a valid Maintenance image or is not
compatible with this release.
```

Recommended Action You need to use the correct maintenance image for NAM-1 or NAM-2 and WS-X6380-NAM maintenance image should not be used.

Explanation From WS-X6380-NAM application image, when I try to upgrade the maintenance image I get this error.

```
Incompatible image! Upgrade aborted.
```

Recommended Action You need to use the correct maintenance image for WS-X6380-NAM and the NAM-1, NAM-2 maintenance image should not be used.

Explanation When I try to upgrade the WS-X6380-NAM Maintenance image, I get the following error:

```
 restore operation failed.
```

Explanation You are trying to load an application image the NAM-1 or NAM-2, which causes this error. Try loading WS-X6380-NAM application image to correct this problem.