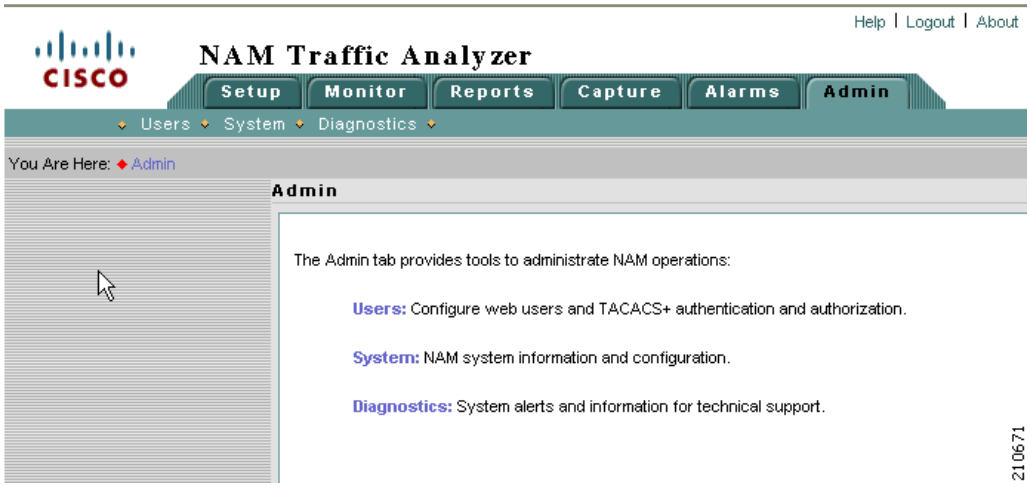
CHAPTER 2

User and System Administration

This chapter provides information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance. The top-level Admin window displays after you click the **Admin** tab on the NAM GUI. Figure 2-1 shows the top-level Admin window.

Figure 2-1 Top-Level Admin Window



This chapter has the following major sections:

- User Administration, page 2-2, describes how you configure either a local database or provide information for a TACACS+ database for user authentication and authorization. This section also describes the current user session window.
- System Administration, page 2-10, describes menu options that enable you to perform system administrative tasks and manage the NAM.
- Diagnostics, page 2-25, describes menu options that help you diagnose and troubleshoot problems.

User Administration

When you first install the NAM Traffic Analyzer, you use the NAM command-line interface (CLI) to enable the HTTP server and establish a username and password to access the NAM for the first time.

After setting up the initial user accounts, you can create additional accounts, enabling or disabling different levels of access independently for each user. You do this by assigning privileges that correspond to tasks each user can perform, such as configuring RMON collections, configuring system parameters, viewing RMON data, and so on.

Table 2-1 provides information about User Privileges and describes each privilege.

Table 2-1 User Privileges

Privilege	Access Level
Account Mgmt	Enables a user to create, delete, and edit user accounts.
System Config	Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.
Capture	Enables a user to perform packet captures and manage capture buffers Use the NAM Traffic Analyzer protocol decode.
Alarm Config	Enables a user to create, delete, and edit alarms on the switch/router and NAM.
Collection Config	Enables a user to create, delete, and edit the following: • Collections and reports • Protocol directory entries • Protocol groups • URL-based applications
Collection View	Enables a user to view monitoring data and reports (granted to all users).

For additional information about creating and editing users, see Creating a New User, page 2-4 and Editing a User, page 2-5.

Recovering Passwords

You can recover passwords by using CLI commands on the switch or router. A user with appropriate privileges can reset the NAM CLI and passwords to the factory default state.

For information on resetting the NAM passwords on 6500 Series NAMs, 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/4.1/switch/configuration/guide/swconfig.html

For information on resetting the NAM passwords on NM-NAM devices, see the *Network Analysis Module (NM-NAM)* feature module.

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xd/feature/guide/nm_nam.html#wp1060820

For information on resetting the NAM passwords on NME-NAM devices, see the *Network Analysis Module (NME-NAM) Installation and Configuration Note.*

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/branch_router/configuration/guide/BR_incfg.html#wp1314123

For information on resetting the NAM passwords on a Cisco NAM 2200 Series Appliance, see the *Installation and Configuration Guide for the NAM 2204 Appliance* or the *Installation and Configuration Guide for the NAM 2220 Appliance*

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_appliance/2204/installation/guide/instcfg.html

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_appliance/2220/installation/guide/instcfg.html

If you have forgotten NAM Traffic Analyzer administrator password, you can recover it using one of these methods:

- If other users have account management permission, delete the user for whom you have forgotten the password; then create a new one by logging in as that other user by clicking the Admin tab, then clicking **Users**.
- If no other local users are configured other than the user for whom you have forgotten the password, use the NAM **rmwebusers** CLI command; then enable http or https to prompt for the creation of a NAM Traffic Analyzer user.

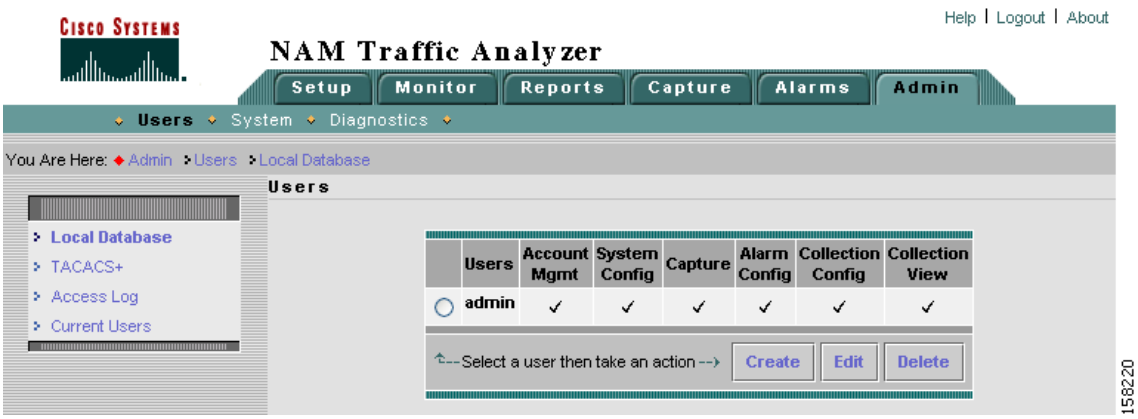
Changing Predefined NAM User Accounts on the Switch or Router

The predefined root and guest NAM user accounts (accessible through either a switch or router **session** command or a Telnet login to the NAM CLI) are static and independent of the NAM Traffic Analyzer. You cannot change these static accounts nor can you add other CLI-based users with the NAM Traffic Analyzer.

User Administration GUI

The User Administration GUI enables you to manage users. Figure 2-2 shows the top-level User Admin GUI window.

Figure 2-2 User Admin GUI



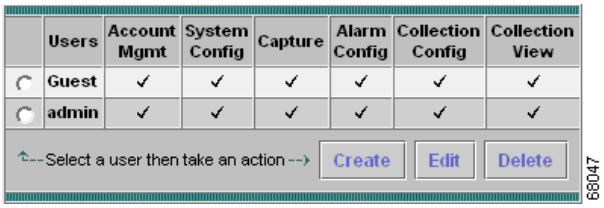
Creating a New User

To create a new user:

Step 1 Choose **Admin** > **Users**.

The GUI displays the users in the local database, as shown in Figure 2-3. Checks indicate the privileges each user has for the functions listed.

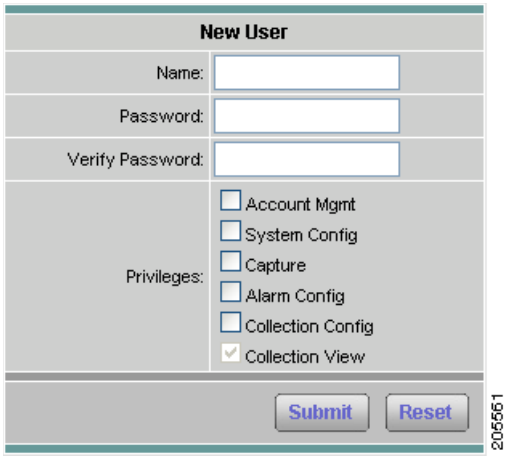
Figure 2-3 Users Table



Step 2 Click **Create**.

The GUI displays the New User Dialog Box (Figure 2-4).

Figure 2-4 New User Dialog Box



Step 3 Enter the information required to create new user and select each privilege to grant to the user. See Table 2-1 for an explanation of user privileges. Table 2-2 describes the fields in the New User Dialog Box.

Table 2-2 New User Dialog Box

Field	Description	Usage Notes
Name	The account name	Enter the user's account name.
Password Verify Password	The account password	Enter a password that adheres to your site security policies.
Privileges	Privileges associated with this account	Select each privilege to grant to the user.

Usernames and passwords cannot exceed 32 characters, can be alphanumeric, and can contain special characters except the following:

- Greater than (<)
- Less than (>)
- Comma (,)
- Period (.)
- Double quote (")
- Single quote (')

Step 4 Click **Submit** to create the user or **Reset** to clear the dialog of any characters you entered.

Editing a User

To edit a user's configuration:

Step 1 Choose **Admin > Users**.

The Users table displays.

Step 2 Select the username.

Step 3 Click **Edit**.

Step 4 In the Modify Users dialog box, change whatever information is necessary. See the New User Dialog Box (Figure 2-4) for a description of each field.

Click **Submit** to save your changes, or click **Reset** to clear the dialog of any characters you entered and restore the previous settings.

Deleting a User

To delete a user:

Step 1 Choose the **Admin > Users**.

The Users table displays.

Step 2 Select the username.

Step 3 Click **Delete**.

Note 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.

Establishing TACACS+ Authentication and Authorization

Terminal Access Controller Access Control System (TACACS) is an authentication protocol that provides remote access authentication, authorization, and related services such as event logging. With TACACS, user passwords and privileges are administered in a central database instead of an individual switch or router to provide scalability.

TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization.

When a user logs into the NAM Traffic Analyzer, TACACS+ determines if the username and password are valid and what the access privileges are.

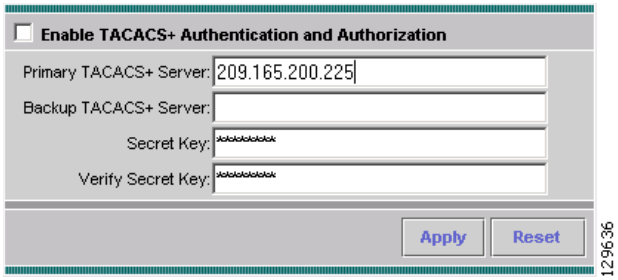
To establish TACACS+ authentication and authorization:

Step 1 Choose **Admin > Users**.

Step 2 In the content menu, click **TACACS+**.

The TACACS+ Authentication and Authorization Dialog Box (Figure 2-5) displays.

Figure 2-5 TACACS+ Authentication and Authorization Dialog Box



Step 3 Enter or select the appropriate information in the TACACS+ Authentication and Authorization Dialog Box (Table 2-3).

Table 2-3 TACACS+ Authentication and Authorization Dialog Box

Field	Usage Notes
Enable TACACS+ Authentication and Authorization	Determines whether TACACS+ authentication and authorization is enabled. • To enable, select the check box. • To disable, clear the check box.
Primary TACACS+ Server	Enter the IP address of the primary server.
Backup TACACS+ Server	Enter the IP address of the backup server (optional). **Note** If the primary server does not respond after 30 seconds, the backup server will be contacted.
Secret Key	Enter the TACACS+ password.
Verify Secret Key	Reenter the TACACS+ password.

Step 4 Do one of the following:

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

Tip If you cannot log into the NAM Traffic Analyzer with TACACS+ configured, verify that you entered the correct TACACS+ server name and secret key. For more information, see the "Username and Password Issues" section on page A-2.

Configuring a TACACS+ Server to Support NAM Authentication and Authorization

In addition to enabling the TACACS+ option from the Admin tab, you must configure your TACACS+ server so that it can authenticate and authorize NAM Traffic Analyzer users.

Note Configuration methods vary depending on the type of TACACS+ server you use.

Configuring a Cisco ACS TACACS+ Server

For Windows NT and 2000 Systems

To configure a Cisco ACS TACACS+ server:

Step 1 Log into the ACS server.

Step 2 Click **Network Configuration**.

Step 3 Click **Add Entry**.

Step 4 For the Network Access Server, enter the NAM hostname and IP address.

Step 5 Enter the secret key.

Note The secret key must be the same as the one configured on the NAM.

Step 6 In the Authenticate Using field, select **TACACS+**.

Step 7 Click **Submit/Restart**.

Adding a NAM User or User Group

To add a NAM user or user group:

Step 1 Click **User Setup**.

Step 2 Enter the user login name.

Step 3 Click **Add/Edit**.

Step 4 Enter the user data.

Step 5 Select **User Setup**.

Step 6 Enter a user password.

Step 7 If necessary, assign a user group.

Step 8 In the TACACS+ settings:

a. Select **Shell**.

b. Select **IOS Command**.

c. Select **Permit**.

d. Select **Command**.

e. Enter **web**.

f. In the Arguments field, enter:

```
permit capture
permit system
permit collection
```

```
permit account
permit alarm
permit view
```

Step 9 In Unlisted Arguments, select **Deny**.

Configuring a Generic TACACS+ Server

To configure a generic TACACS+ server:

Step 1 Specify the NAM IP address as a Remote Access Server.

Step 2 Configure a secret key for the TACACS+ server to communicate with the NAM.

Note The secret key must be the same as the one configured on the NAM.

Step 3 For each user or group to be allowed access to the NAM, configure the following TACACS+ parameters:

Parameter	Enter
service	`shell`
cmd	`web`

cmd-arg	One or more the following:
	`accountmgmt`
	`system`
	`capture`
	`alarm`
	`collection`
	`view`

password authentication method—Password Authentication Protocol (PAP)	`pap`

Viewing the Current User Sessions Table

The Current User Sessions table is a record of the users who are logged into the application. The user session times out after 30 minutes of inactivity. After a user session times out, that row is removed from the table.

To view the current user sessions table:

Step 1 Choose **Admin > Users**.

Step 2 In the contents, click **Current Users**.

The Current User Sessions Table (Table 2-4) displays.

Table 2-4 Current User Sessions Table

Field	Description
User ID	The user ID used to log in to the NAM.
From	The name of the machine the user logged in from.
Login Time	The time the user logged in.
Last Activity	The time stamp of the last user activity.

System Administration

The System option of the Admin tab provides access to the following functions:

System Resources

Choose **Admin** > **System** to view the System Overview window as shown in Figure 2-6.

Figure 2-6 System Overview Window

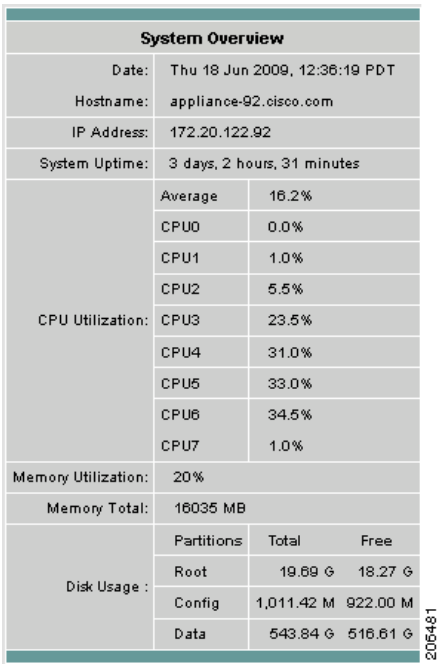


Table 2-5 describes the fields of the System Overview window for a NAM with multiple CPUs such as the Cisco NAM 2220 appliance.

Table 2-5 System Overview

Field	Description
Date	Current date and time synchronized with the switch, router, or NTP server.
Hostname	NAM hostname.
IP Address	NAM IP address.
System Uptime	Length of time the host has been running uninterrupted.
CPU Utilization	Percentage of CPU resources being consumed by the NAM. Average, at top, indicates the average CPU usage of all CPUs. Each individual CPU in a multi-CPU platform is listed separately.
Memory Utilization	Percentage of memory resources being consumed by the NAM.
Disk Usage	Shows **root**, **config**, and **data** partitions with their total and free space.

Setting and Viewing Network Parameters

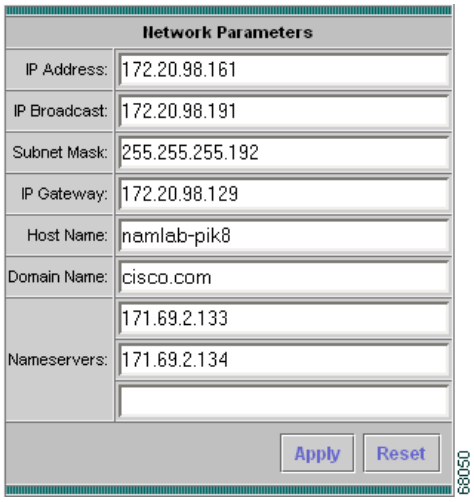
To view and set network parameters:

Step 1 Choose **Admin > System**.

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

The Network Parameters Dialog Box (Figure 2-7) displays.

Figure 2-7 Network Parameters Dialog Box



Step 3 Enter or change the information in the Network Parameters Dialog Box (Table 2-6):

Note NAM 4.1 does not support using IPv6 for the network parameter IP address.

Table 2-6 Network Parameters Dialog Box

Field	Description
IP Address	NAM IP address.
IP Broadcast	NAM broadcast address.
Subnet Mask	NAM subnet mask.
IP Gateway	NAM IP gateway address.
Host Name	NAM host name.
Domain name	NAM domain name.
Nameservers	NAM nameserver address or addresses.

Step 4 Do one of the following:

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

Setting and Viewing the NAM SNMP System Group

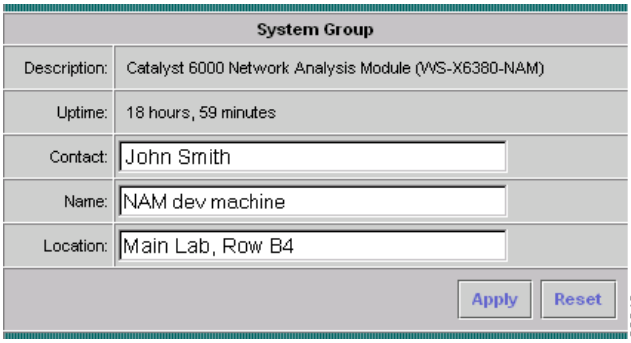
To view and set the NAM SNMP system group:

Step 1 Choose **Admin > System**.

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

At the top of the window, the SNMP System Group Dialog Box (Figure 2-8) and NAM Community Strings Dialog Box (Figure 2-9) are displays.

Figure 2-8 SNMP System Group Dialog Box



Step 3 Enter or change the information in the System SNMP Dialog Box (Table 2-7).

Table 2-7 System SNMP Dialog Box

Field	Description
Contact	The name of the person responsible for the NAM.
Name	The name of the NAM.
Location	The physical location of the switch or router in which the NAM is installed.

Step 4 Do one of the following:

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

Working with NAM Community Strings

You use community strings so that other applications can send SNMP get and set requests to the NAM, set up collections, poll data, and so on.

Creating NAM Community Strings

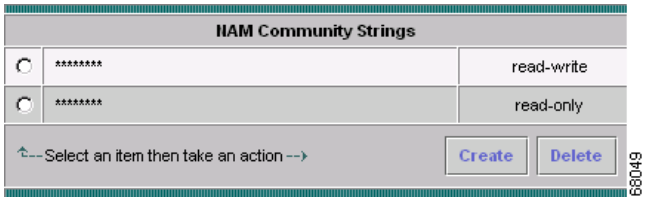
To create the NAM community strings:

Step 1 Choose **Admin > System**.

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

At the bottom of the window, the NAM Community Strings Dialog Box displays (Figure 2-9).

Figure 2-9 NAM Community Strings Dialog Box



Step 3 Select an entry, then click **Create**.

The Create Community String Dialog Box (Figure 2-10) displays.

Figure 2-10 Create Community String Dialog Box

Step 4 Enter the community string (use a meaningful name).

Step 5 Enter the community string again in the Verify Community field.

Step 6 Assign read-only or read-write permissions using the following criteria:

- Read-only allows only read access to SNMP MIB variables (get).
- Read-write allows full read and write access to SNMP MIB variables (get and set).

Step 7 Do one of the following:

- To make the changes, click **Submit**.
- To cancel, click **Reset**.

Deleting NAM Community Strings

To delete the NAM community strings:

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

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

At the bottom of the window, the NAM Community Strings Dialog Box (Figure 2-9) displays.

Step 3 Select an entry, then click **Delete**.

Caution Deleting the NAM community strings blocks SNMP requests to the NAM from outside SNMP agents.

The community string is deleted.

NAM System Time

The NAM gets the UTC (GMT) time from one of two sources, depending on its the NAM type. All NAMs can be set up to get their time from an external NTP server. Following is the second option per NAM type:

- NAM-1 and NAM-2 can get their time from the switch.
- NME-NAMs can get their time from the router.
- Cisco 2200 Series appliances can get their time from a local CLI **clock set** command.

After the NAM acquires the time, you can set the local time zone using the NAM System Time configuration screen. Figure 2-11 shows the NAM System Time Configuration Screen for NAM-1, NAM-2, and NME-NAMs. You can configure the NAM system time by using one of the following methods:

- Synchronizing the NAM System Time with the Switch or Router, page 2-17

  This option is valid only for NAM-1, NAM-2, and NME-NAMs.
- Synchronizing the NAM System Time Locally, page 2-17

  This option is valid only for Cisco NAM 2200 Series appliances.
- Configuring the NAM System Time with an NTP Server, page 2-17

Figure 2-11 NAM System Time Configuration Screen for NAM-1, NAM-2, and NME-NAMs

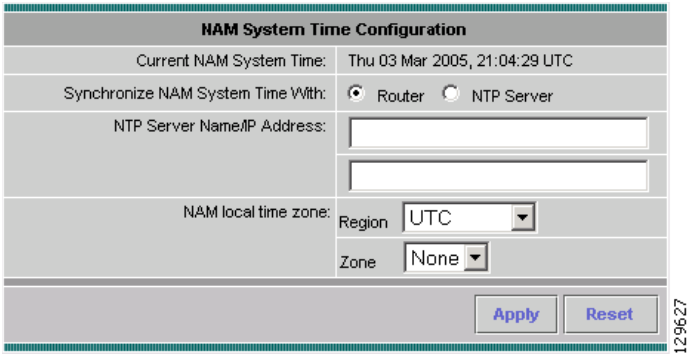
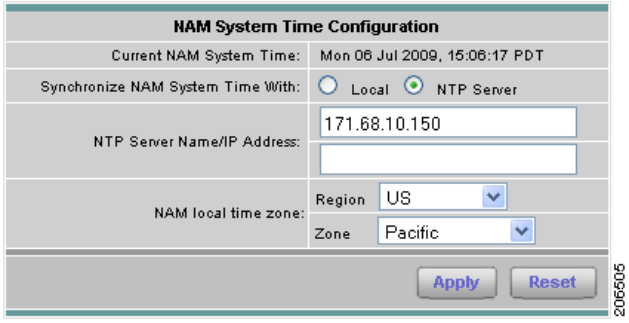


Figure 2-12 shows the Cisco NAM 2200 Series Appliance System Time Configuration Screen.

Figure 2-12 Cisco NAM 2200 Series Appliance System Time Configuration Screen



Synchronizing the NAM System Time with the Switch or Router

Note This section is valid only for NAM-1, NAM-2, and NME-NAMs.

To configure the NAM system time from the switch or router:

Step 1 Click the Switch or Router radio button.

Step 2 Select the Region and local time zone from the lists.

Step 3 Do one of the following:

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

Synchronizing the NAM System Time Locally

Note This section is valid only for Cisco NAM 2200 Series appliances.

To configure the NAM system time locally using the NAM appliance command line:

Step 1 Log in to the NAM appliance command line interface.

Step 2 Set the clock using the CLI **clock set** command.

clock set <*hh:mm:ss:*> <*mm/dd/yyyy*>

Step 3 On the NAM appliance GUI, click **Admin** > **System**.

Step 4 Click NAM System Time in the contents menu.

Step 5 Click the **Local** radio button.

Step 6 Select the Region and local time zone from the lists.

Step 7 Do one of the following:

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

Configuring the NAM System Time with an NTP Server

To configure the NAM system time with an NTP server:

Step 1 On the NAM applianc e GUI, click **Admin** > **System**.

Step 2 Click NAM System Time in the contents menu.

Step 3 Click the **NTP Server** radio button.

Step 4 Enter one or two NTP server names or IP address in the NTP server name/IP Address text boxes.

Step 5 Select the Region and local time zone from the lists.

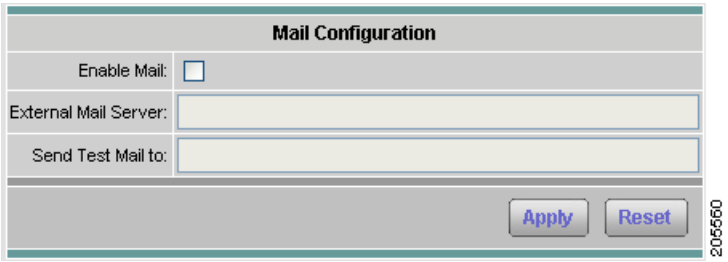
Step 6 Do one of the following:

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

E-Mail Configuration

You can configure the NAM to provide E-Mail notification of alarms and to E-Mail reports. Figure 2-13 shows the Mail Configuration Window. For information about how to configure a report to send using E-Mail, see Table 5-18, Scheduled Exports Window Options, in section Scheduled Exports, page 5-28.

Figure 2-13 Mail Configuration Window



The following procedure describes how to configure the NAM for E-Mail notifications.

Step 1 Choose **Admin > System**.

Step 2 Click **E-Mail Configuration**.

The Mail Configuration Window (Figure 2-13) displays. Table 2-8 describes the Mail Configuration Options.

Table 2-8 Mail Configuration Options

Field	Description
Enable Mail	Enables E-Mail of reports and notification of alarms
External Mail Server	Distinguished name of external mail server
Send Test Mail	List E-Mail addresses for up to three E-Mail recipients

Step 3 Check **Enable EMail**.

Step 4 Enter the distinguished name of the **External Mail Server**.

Step 5 Click **Apply** to save your modifications, or click **Reset** to clear the dialog of any characters you entered or restore the previous settings.

FTP Configuration

You can configure the NAM to provide FTP notification of alarms and to EMail reports. Figure 2-14 shows the FTP Configuration Window. For information about how to configure a report to be transferred using FTP, see Table 5-18, Scheduled Exports Window Options, in section Scheduled Exports, page 5-28.

Figure 2-14 FTP Configuration Window

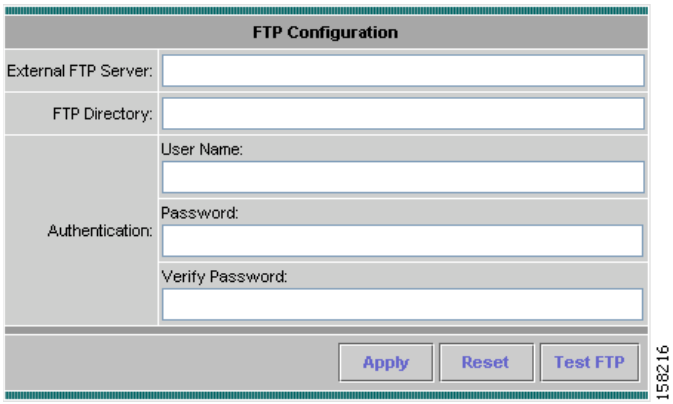


Table 2-9 describes the fields used for FTP configuration.

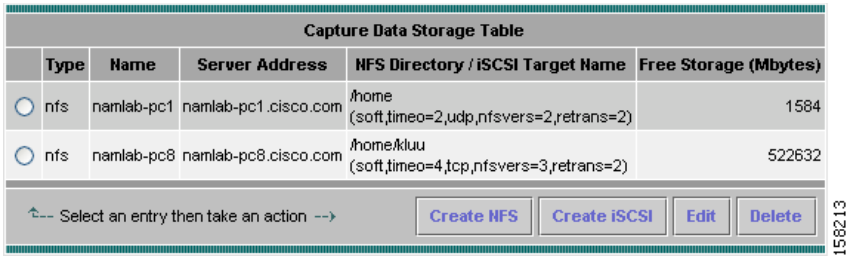
Table 2-9 FTP Configuration Options

Field	Description
External FTP Server	Host name or IP address of FTP server
FTP Directory	Full directory pathname of location to store FTP files
Authentication	User name and password fields used to for authentication with external FTP server.

Capture Data Storage

Use the Capture Data Storage option to set up remote file systems to store capture data. You must set up the capture data storage locations prior to setting up data captures. Choose **Admin > Capture Data Storage** to open the Capture Data Storage window (shown in Figure 2-15).

Figure 2-15 Capture Data Storage Window



This section provides the following:

Creating NFS Storage Locations

The NFS server must be configured properly to allow NAM to write data to it. The NAM accesses the NFS directories with UID=80 (www) and UID=0 (root). The NFS directories must be fully accessible by these UIDs.

One way to do this is to use the NFS option *all_squash* to map these UIDs to `anonuid=<userID>`, where < userID> is a local user ID with full access rights to the NFS directories.

Configuring the NFS Server

The following example shows how to set up an NFS directory (**/home/SomeUserName**) in a Linux server for a NAM (at IP address 1.1.1.2) to store capture data. To setup an NFS server directory to store capture data:

Step 1 Locate a UID that has read and write access to the target NFS directory.

For example, if the target NFS directory is **/home/SomeUserName**, open the **/etc/password** file and search for a user entry that contains something like the following:

```
SomeUserName:x:503:503::/home/SomeUserName:/bin/tcsh
```

In this example, the UID is 503.

Step 2 Edit the **/etc/exports** file and add a line like the following:

```
/home/SomeUserName    1.1.1.2/255.255.255.255(rw,all_squash,anonuid=503)
```

Step 3 Activate the change:

/usr/bin/exportfs -a

Note If the NFS directory contains subdirectories that are not writable by the NAM, these subdirectories will not be listed in NAM capture screens.

Configuring the NFS Storage Location on the NAM

The following procedure describes how to create an NFS storage location by specifying a remote file system partition.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window (Figure 2-15) displays and lists any capture data storage locations already configured.

Step 2 Click **Create NFS**.

Step 3 Enter the requested parameters in the New NFS Storage window.

Table 2-10 describes the NFS Storage location parameters.

Table 2-10 NFS Storage Location Parameters

Field	Description
Name	Name of the remote file system entry
Server	DNS name of the remote file system entry
Directory	Pathname of the remote file system partition
Basic NFS Options	Each fields shows a default value. If you need to use values other than those available in the menus, use Advanced NFS Options.
Protocol	Choose TCP or UDP
Timeout	You can set the timeout to a value from 0.1 seconds to 1.0 seconds
NFS Version	Choose from NFS versions 1-4
Retries	Choose from 1-5 retries
Advanced NFS Options	This field contains the default values for creating an NFS storage location. You can edit the text to use NFS options that are outside the ranges in the pull-down menus of the Basic NFS Options.

Step 4 Click **Submit** to create the NFS storage location. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

Editing NFS Storage Locations

The following procedure describes how to edit an existing NFS storage location.

Note If you have set up capture sessions that use the NFS file system entry you want to edit (or modify), you must delete those capture sessions before editing the NFS file system entry. You can find active capture buffers by clicking **Capture > Buffers**, then choose each capture that is *running* and click **Status**. If the capture is using the filesystem to be edited, click **Clear**.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window (Figure 2-15) displays and lists any capture data storage locations already configured.

Step 2 Click to select the NFS storage location you want to modify and click **Edit**.

The Edit Remote Storage Entry window displays the parameters of the select NFS storage location.

Step 3 Modify the parameters as desired.

Table 2-10 describes the NFS Storage location parameters.

Step 4 Click **Submit** to change the parameters of the NFS storage location. Otherwise click **Reset** to remove all of the entries, or click **Cancel** to cancel the change.

Creating iSCSI Storage Locations

The following procedure describes how to create an iSCSI storage location for storing NAM capture data.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window (Figure 2-15) displays and lists any capture data storage locations already configured.

Step 2 Click **Create iSCSI**.

Step 3 Enter the requested parameters in the New iSCSI Storage window.

Table 2-11 describes the iSCSI Storage location parameters.

Table 2-11 iSCSI Storage Location Parameters

Field	Description
Name	Name of the remote storage entry
Server	DNS host name or IP address of the iSCSI server.

Table 2-11 iSCSI Storage Location Parameters

Field	Description
Target Name	iSCSI target name configured on the remote iSCSI server
Format Disk:	Check **Format a new partition** to cause the NAM to format the iSCSI target into a single Linux partition. Check **Use existing partition#** when the remote iSCSI target disk has already been formatted and has a partition table.

Step 4 Click **Submit** to create the iSCSI storage location. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

Note Before the new iSCSI storage entry takes effect, you must reboot the NAM system.

Editing iSCSI Storage Locations

The following procedure describes how to edit an existing NFS storage location.

Note If you have set up capture sessions that use the iSCSI file system entry you want to edit (or modify), you must delete those capture sessions before editing the iSCSI file system entry. You can find active capture buffers by clicking **Capture > Buffers**, then choose each capture the is *running* and click **Status**. If the capture is using the filesystem to be edited, click **Clear**.

Step 1 Choose **Admin > Capture Data Storage**.

The Capture Data Storage window (Figure 2-15) displays and lists any capture data storage locations already configured.

Step 2 Click to select the iSCSI storage location you want to modify and click **Edit**.

The selected iSCSI storage location parameters window displays

Step 3 Modify the parameters as desired.

Table 2-11 describes the iSCSI storage location parameters.

Step 4 Click **Submit** to change the iSCSI storage location parameters. Otherwise click **Reset** to remove your entries or **Cancel** to cancel the change.

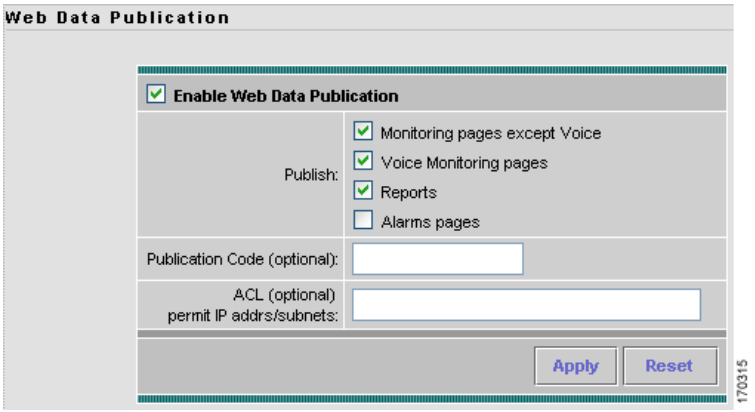
Note Before the changes to the iSCSI storage entry take effect, you must reboot the NAM system.

Web Publication

Web publication allows general web users and web sites to access (or link to) selected NAM monitor and report screens without a login session.

Web publication can be open or restricted using Access Control List (ACL) and/or publication code. The publication code, if required, must be present in the URL address or cookie to enable access to published data. Figure 2-16 shows the Web Data Publication Window.

Figure 2-16 Web Data Publication Window



To enable web publishing:

Step 1 Choose **Admin > System**.

Step 2 In the System menu, click **Web Publishing**.

Step 3 Check each item you want to make available for web publishing.

Table 2-12, Web Data Publication Properties, describes the fields of the Enable Web Publishing window.

Table 2-12 Web Data Publication Properties

Field	Description
Monitoring pages except Voice	Check to publish all Monitor screens except Voice
Voice Monitoring pages	Check to publish Voice Monitoring screens
Reports	Check to publish all reports
Alarms pages	Check to publish NAM and Switch Alarms pages
Publication Code	Pass code required in a URL's cookie to access the published page. For example, a publication code set to *abc123* could access the published **Monitor > PortStat** window: http://<nam-hostname>/monitor/sup/ether/supetherstats.php?sortCol=utilization&publicationcode=abc123
ACL permit IP addrs/subnets	No entry provides open access to all. Enter IP addresses or subnets to permit only those IP addresses or subnets access to web publications.

Step 4 Click **Apply** to enable web publishing or **Reset** to clear the dialog of any characters you entered.

Response Time Export

You can enable response time data export to an external reporting console such as NetQoS SuperAgent. This window works in conjunction with the **Setup > Data Sources > WAAS--Devices > Add/Config** window. After you enable Response Time Export there, the **Export Passthru to External Console** option appears on the Add/Config WAAS Device window.

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

Step 1 From the NAM GUI, choose **Admin > System > Response Time Export**.

The Export window displays.

Step 2 Enter the IP address of the external reporting console in the IP Address field.

Step 3 Optionally, enter the UDP port number of the external console.

Step 4 Click **Export** to enable the NAM to export data.

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 **Apply** to enable traffic export.

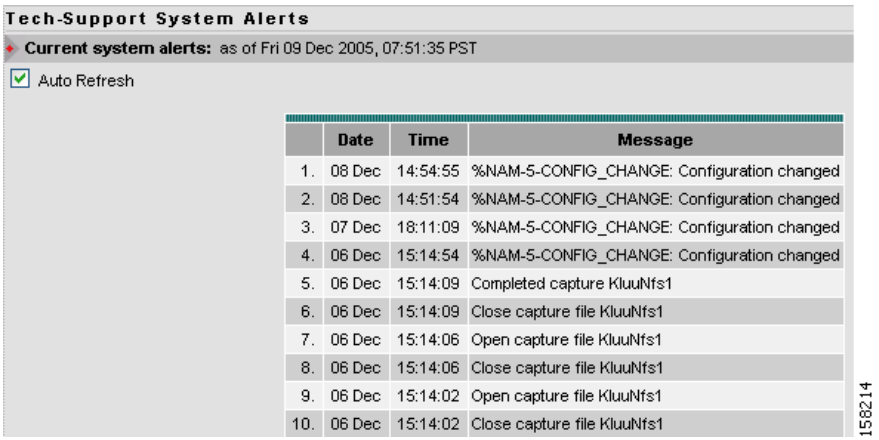
Diagnostics

The Diagnostics option of the **Admin** tab provides tools to aid in troubleshooting. You can use these tools when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC). There are options for:

Viewing System Alerts

You can view any failures or problems that the NAM Traffic Analyzer has detected during normal operations. To view System Alerts, choose **Admin > Diagnostics**. System Alerts is the default window. Figure 2-17 shows the System Alerts Window.

Figure 2-17 System Alerts Window



Each alert includes a date, the time the alert occurred, and a message describing the alert. The NAM displays up to one thousand (1,000) of the most-recent alerts. If more than 1,000 alerts have occurred, you need to use the NAM CLI command **show tech support** to see all of the alerts.

If you notice an alert condition and troubleshoot and attempt to solve the condition causing the alert, you might want to click **Clear** to remove the list of alerts to see if additional alerts occur.

Viewing the Audit Trail

The Audit Trail option displays a listing of recent critical activities that have been recorded in an internal **syslog** log file. Syslog messages can also be sent to an external log.

The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NDE data source changes
- Enabling and disabling data collections
- Creating and deleting reports
- Starting and stopping captures
- Adding and deleting users

Each log entry will contain the following:

- User ID
- Time stamp
- IP address (in case of remote web access)
- Activity description

To access the audit trail window:

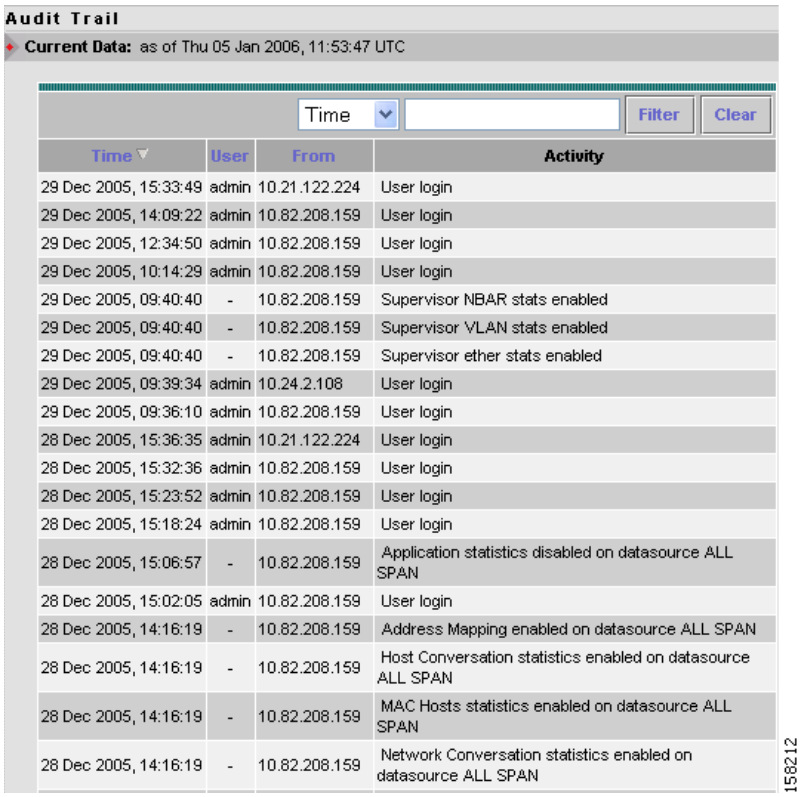
Step 1 Choose **Admin > Diagnostics.**

Step 2 Click **Audit Trail**.

The Audit Trail Window (Figure 2-18) displays.

The Audit Trail window provides a way to view the user access log and filter entries based on time, user, (IP address) from or activity. The internal log files are rotated after reaching certain size limit.

Figure 2-18 Audit Trail Window



Time	User	From	Activity
29 Dec 2005, 15:33:49	admin	10.21.122.224	User login
29 Dec 2005, 14:09:22	admin	10.82.208.159	User login
29 Dec 2005, 12:34:50	admin	10.82.208.159	User login
29 Dec 2005, 10:14:29	admin	10.82.208.159	User login
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor NBAR stats enabled
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor VLAN stats enabled
29 Dec 2005, 09:40:40	-	10.82.208.159	Supervisor ether stats enabled
29 Dec 2005, 09:39:34	admin	10.24.2.108	User login
29 Dec 2005, 09:36:10	admin	10.82.208.159	User login
28 Dec 2005, 15:36:35	admin	10.21.122.224	User login
28 Dec 2005, 15:32:36	admin	10.82.208.159	User login
28 Dec 2005, 15:23:52	admin	10.82.208.159	User login
28 Dec 2005, 15:18:24	admin	10.82.208.159	User login
28 Dec 2005, 15:06:57	-	10.82.208.159	Application statistics disabled on datasource ALL SPAN
28 Dec 2005, 15:02:05	admin	10.82.208.159	User login
28 Dec 2005, 14:16:19	-	10.82.208.159	Address Mapping enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	Host Conversation statistics enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	MAC Hosts statistics enabled on datasource ALL SPAN
28 Dec 2005, 14:16:19	-	10.82.208.159	Network Conversation statistics enabled on datasource ALL SPAN

Monitor and Capture Configuration Information

The Monitor and Capture Configuration window contains information about NAM data collections configured by NAM Traffic Analyzer and other management applications. To view the Monitoring and Capturing Configuration information window:

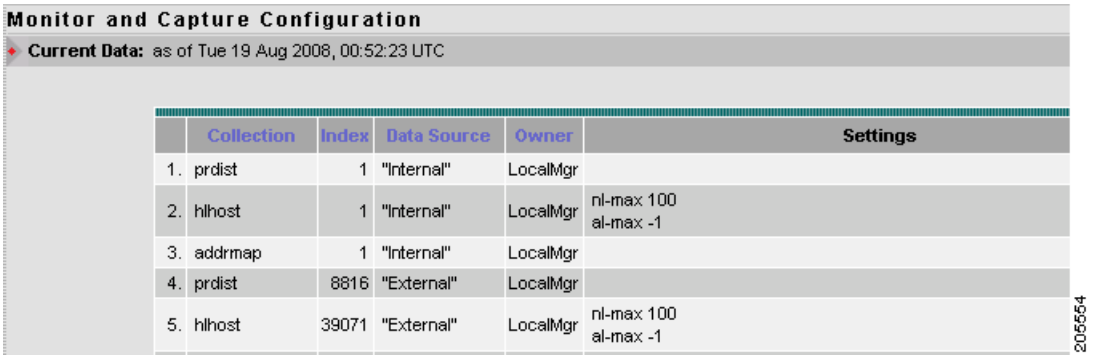
Step 1 Choose **Admin > Diagnostics**.

Step 2 In the contents menu, click **Monitor and Capture Configuration**.

The NAM displays the Monitor and Capture Configuration Window (Figure 2-19). Each line in the Monitor and Capture Configuration window represents an internal configuration statement for NAM collections, captures, filters, data sources, and alarms. Your configuration might have dozens of statements like these.

Note This information does not mean much to the casual user, but it is valuable when you consult with Cisco TAC personnel or when you require technical support.

Figure 2-19 Monitor and Capture Configuration Window



Step 3 To save the information, choose **File > Save As...** from your browser menu.

Step 4 Select an output destination, filename, and format, then click **Save**.

If the name LocalMgr is displayed in the Owner column, the collection was configured by the NAM Traffic Analyzer.

Viewing Technical Support

The NAM syslog records NAM system alerts that contain event descriptions and date and timestamps, indicating unexpected or potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs.

This information is unlikely to be meaningful to the average user. It is intended to be used by the Cisco TAC for debugging purposes. You are not expected to understand this information; instead, you should save the information and attach it to an email message to the Cisco TAC.

Before you can view the Tech-Support page, you must enable the System Config user privilege on the **Admin > Users** page. For more information on editing user privileges, see the "Editing a User" section on page 2-5.

Note You can also view this information from the NAM CLI. For information on using the NAM CLI, see *Cisco Network Analysis Module Command Reference,* for NM-NAM or NME-NAM devices, the *Network Analysis Module (NM-NAM or NME-NAM)* feature module.

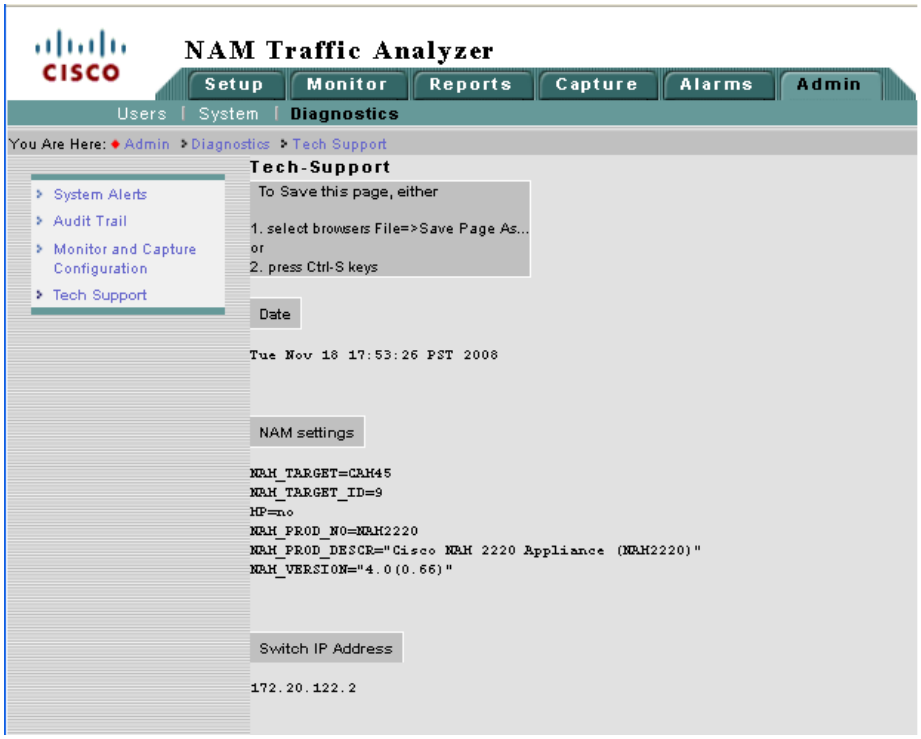
To view tech support:

Step 1 Choose **Admin > Diagnostics**.

Step 2 In the contents, click **Tech Support**.

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window (Figure 2-20).

Figure 2-20 Diagnostics Tech Support Window



Step 3 To save the information, select **File>Save As...** from the browser menu.

If you are using Internet Explorer, you can click the **Save This Page** button at the top of the page to download the Tech-Support page as a text file.

Step 4 Select an output destination, filename, and file format, then click **Save**.

Downloading Core Files

To download core files from the Tech-Support page, scroll down to the Core Files section and click on the filename.