User and System Administration

These topics provide information about performing user and system administration tasks and generating diagnostic information for obtaining technical assistance:

- Overview of User Administration Tasks, page 2-1
- Overview of System Administration Tasks, page 2-12
- Setting the NAM System Time, page 2-18
- Generating Diagnostics for Technical Assistance, page 2-19

Overview of User Administration Tasks

When you installed the NAM interface card in the switch or router, you used the NAM CLI to enable the HTTP server and establish a username and password to access the NAM Traffic Analyzer 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.

The User Privileges table (Table 2-1) describes each privilege.

Table 2-1 User Privileges

Privilege	Access Level
Account Mgmt	• Create, delete, and edit user accounts.
System Config	• Edit such basic NAM system parameters as IP address, gateway, HTTP port, and so on.
Capture	• Perform packet capture. • Use the NAM Traffic Analyzer protocol decode.
Alarm Config	• Create, delete, and edit alarms on the switch/router and NAM.
Collection Config	• Create, delete, and edit collections and reports. • Create, delete, and edit protocol directory entries.
Collection View	• View monitoring data (granted to all users) and reports.

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 Catalyst 6000 and 6500 Series NAMs, see the *Catalyst Network Analysis Module Installation and Configuration Note Release 3.1*. For information on resting the NAM passwords on NM-MAN devices, see the *Network Analysis Module (NM-NAM)* feature module.

If you have forgotten NAM Traffic Analyzer admin 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 a Telnet login from 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.

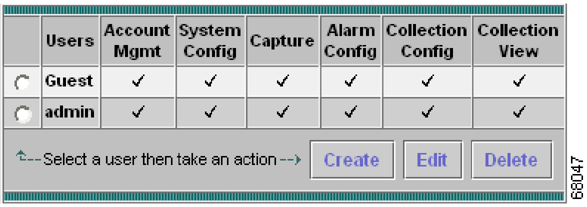
Creating a New User

Step 1 Click the Admin tab.

Step 2 Click **Users**.

The Users Table (Figure 2-1), showing users registered in the local database, is displayed.

Figure 2-1 Users Table

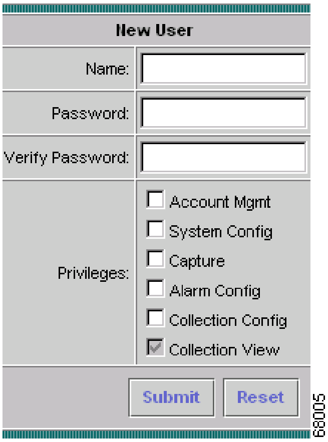


	Users	Account Mgmt	System Config	Capture	Alarm Config	Collection Config	Collection View
○	Guest	✓	✓	✓	✓	✓	✓
○	admin	✓	✓	✓	✓	✓	✓

Step 3 Click **Create**.

The New User Dialog Box (Figure 2-2) is displayed.

Figure 2-2 New User Dialog Box



New User

Name:

Password:

Verify Password:

Privileges:
- ☐ Account Mgmt
- ☐ System Config
- ☐ Capture
- ☐ Alarm Config
- ☐ Collection Config
- ☑ Collection View

Step 4 Enter or select the information described in the New User Dialog Box (Table 2-2):

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.	—
Privileges	Privileges associated with this account.	Select each privilege to grant to the user.

Note User names and passwords cannot exceed 32 characters and must be alphanumeric.

Step 5 Do one of the following:

- To create the user, click **Submit**.
- To cancel, click **Reset**.

Editing a User

Step 1 Click the Admin tab.

Step 2 Click **Users**.

The Users table is displayed.

Step 3 Select the username.

Step 4 Click **Edit**.

Step 5 In the Modify Users dialog box, change whatever information is necessary. See the New User Dialog Box (Figure 2-2) for a description of each field.

Step 6 Do one of the following:

- To submit the changes, click **Submit**.
- To discard the changes, click **Reset**.

Deleting a User

Step 1 Click the Admin tab.

Step 2 Click **Users**.

The Users table is displayed.

Step 3 Select the username.

Step 4 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.

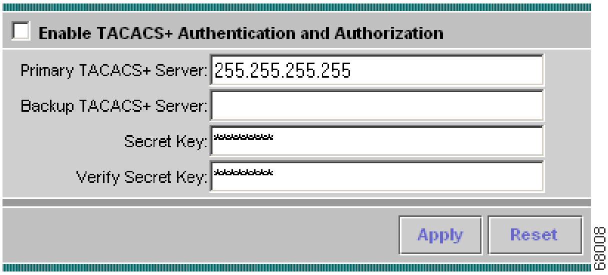
Step 1 Click the Admin tab.

Step 2 Click **Users**.

Step 3 In the contents, click **TACACS+**.

The TACACS+ Authentication and Authorization Dialog Box (Figure 2-3) is displayed.

Figure 2-3 TACACS+ Authentication and Authorization Dialog Box



□ Enable TACACS+ Authentication and Authorization

Primary TACACS+ Server: 255.255.255.255

Backup TACACS+ Server:

Secret Key: ********

Verify Secret Key: ********

Step 4 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 5 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

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

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

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 Access Log

The access log is a historical record of users who logged into the NAM Traffic Analyzer. It includes the login name and time, the originating IP address, and a summary of login activity. It also records logouts, unsuccessful login attempts, and attempts at unauthorized access (denials).

The user access log is checked daily and trimmed when it exceeds 100,000 bytes; trimming deletes the older 50,000 bytes so the most recent log data remains. If the log grows too quickly and reaches 200,000 bytes before the daily check, logging stops until the daily trimming or until you manually clear it.

Step 1 Click the Admin tab.

Step 2 Click **Users**.

Step 3 In the contents, click **Access Log**.

The access log is displayed.

Note To clear the log, click **Clear Log**.

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.

Step 1 Click the Admin tab.

Step 2 Click **Users**.

Step 3 In the contents, click **Current Users**.

The Current User Sessions Table (Table 2-4) is displayed.

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.

Overview of System Administration Tasks

The System option of the Admin tab provides features for:

- Viewing System Resources, page 2-12
- Setting and Viewing Network Parameters, page 2-13
- Setting and Viewing the NAM SNMP System Group, page 2-15
- Working with NAM Community Strings, page 2-16

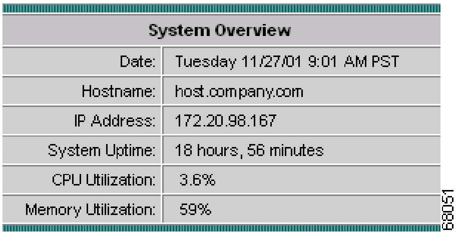
Viewing System Resources

Step 1 Click the Admin tab.

Step 2 Click **System**.

The System Overview Table (Figure 2-4) is displayed.

Figure 2-4 System Overview Table



System Overview	
Date:	Tuesday 11/27/01 9:01 AM PST
Hostname:	host.company.com
IP Address:	172.20.98.167
System Uptime:	18 hours, 56 minutes
CPU Utilization:	3.6%
Memory Utilization:	59%

The System Overview Table (Table 2-5) describes each field.

Table 2-5 System Overview Table

Field	Description
Date	Current date and time, synchronized with the switch or router.
Hostname	NAM hostname.
IP Address	NAM IP address.

Table 2-5 System Overview Table (continued)

Field	Description
System Uptime	Length of time the host has been running uninterrupted.
CPU Utilization	Percentage of CPU resources being consumed by the NAM.
Memory Utilization	Percentage of memory resources being consumed by the NAM.

Setting and Viewing Network Parameters

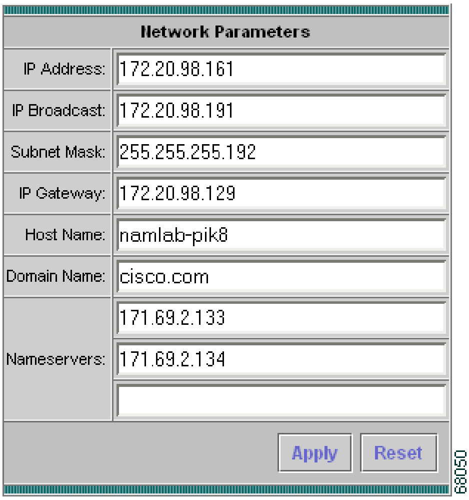
Step 1 Click the Admin tab.

Step 2 Click **System**.

Step 3 In the contents, click **Network Parameters**.

The Network Parameters Dialog Box (Figure 2-5) is displayed.

Figure 2-5 Network Parameters Dialog Box



Network Parameters

IP Address:	172.20.98.161
IP Broadcast:	172.20.98.191
Subnet Mask:	255.255.255.192
IP Gateway:	172.20.98.129
Host Name:	namlab-pik8
Domain Name:	cisco.com
Nameservers:	171.69.2.133 171.69.2.134

Step 4 Enter or change the information in the Network Parameters Dialog Box (Table 2-6):

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 5 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

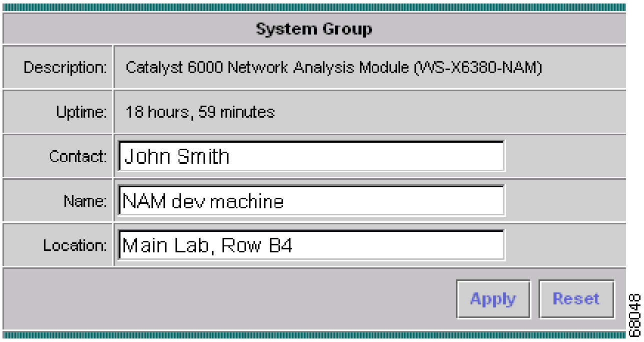
Step 1 Click the Admin tab.

Step 2 Click **System**.

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

At the top of the window, the SNMP System Group Dialog Box (Figure 2-6) and NAM Community Strings Dialog Box (Figure 2-7) are displayed.

Figure 2-6 SNMP System Group Dialog Box



System Group

Description: Catalyst 6000 Network Analysis Module (WS-X6380-NAM)

Uptime: 18 hours, 59 minutes

Contact: John Smith

Name: NAM dev machine

Location: Main Lab, Row B4

Step 4 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 5 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

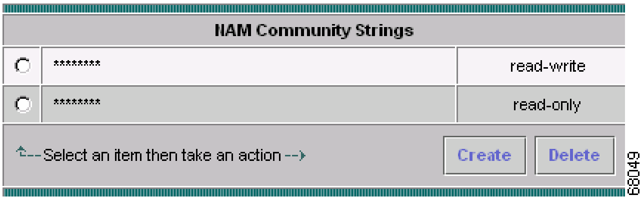
Step 1 Click the Admin tab.

Step 2 Click **System**.

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

At the bottom of the window, the NAM Community Strings Dialog Box is displayed (Figure 2-7).

Figure 2-7 NAM Community Strings Dialog Box

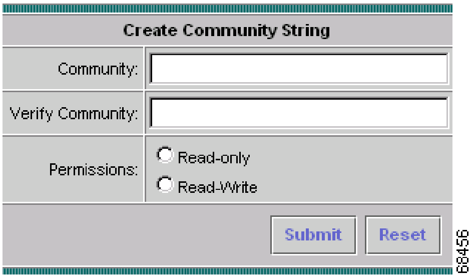


NAM Community Strings		
○	********	read-write
○	********	read-only

Step 4 Select an entry, then click **Create**.

The Create Community String Dialog Box (Figure 2-8) is displayed.

Figure 2-8 Create Community String Dialog Box



Note If you are using NetScout nGenius Real-Time Monitor release 1.3 or earlier, the NAM community string must match the switch or router read-write community strings.

Step 5 Enter the community string (use a meaningful name).

Step 6 Enter the community string again in the Verify Community field.

Step 7 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 8 Do one of the following:

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

Deleting NAM Community Strings

Step 1 Click the Admin tab.

Step 2 Click **System**.

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

At the bottom of the window, the NAM Community Strings Dialog Box is displayed (Figure 2-7).

Step 4 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.

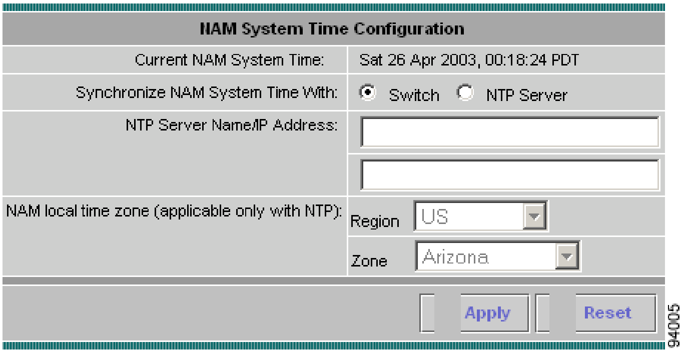
Setting the NAM System Time

The NAM gets the UTC (GMT) time from one of two sources—the switch./router or an NTP server. 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 2-19
- Configuring the NAM System Time with an NTP Server, page 2-19

After the NAM system time has been configured, you can set the local time zone using the NAM System Time configuration screen.

Figure 2-9 NAM System Time Configuration Screen



NAM System Time Configuration

Current NAM System Time:	Sat 26 Apr 2003, 00:18:24 PDT
Synchronize NAM System Time With:	● Switch ○ NTP Server
NTP Server Name/IP Address:	
NAM local time zone (applicable only with NTP):	Region US
	Zone Arizona

Synchronizing the NAM System Time with 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**.

Configuring the NAM System Time with an NTP Server

Step 1 Click the NTP Server radio button.

Step 2 Enter up to two NTP server names or switch IP address in the NTP sever name/IP Address text boxes.

Step 3 Select the Region and local time zone from the lists.

Step 4 Do one of the following:

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

Generating Diagnostics for Technical Assistance

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
- Monitoring and Capturing Configuration Information
- Viewing Technical Support

Viewing System Alerts

You can view any failures or problems that the NAM Traffic Analyzer has during normal operations.

Step 1 Click the Admin tab.

Step 2 Click **Diagnostics**.

Step 3 In the contents, click **System Alerts**.

The Tech Support System Alerts table is displayed.

Step 4 To clear the alert, click **Clear Table**.

Monitoring and Capturing Configuration Information

The Monitor and Capture Configuration option contains information about NAM data collections configured by NAM Traffic Analyzer and other management applications (such as NetScout nGenius Real-Time Monitor). If the name LocalMgr is displayed in the Owner column, the collection was configured by the NAM Traffic Analyzer.

You can save this information when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC).

Some common collections are:

Table 2-8 Collection Types

Collection Type	Created by
host, hlhost	Host Monitor
matrix, hlmatrix	Conversation Monitor
art	Response Time Monitor
buffer, channel, filter	Capture
ds-	DiffServ Monitor

Table 2-8 Collection Types (continued)

Collection Type	Created by
h323-voice-coll sccp-voice-coll	Voice Monitor
vlanstat, priostat	VLAN Monitor
prdist	Apps Monitor
nde-path	Custom NetFlow data sources

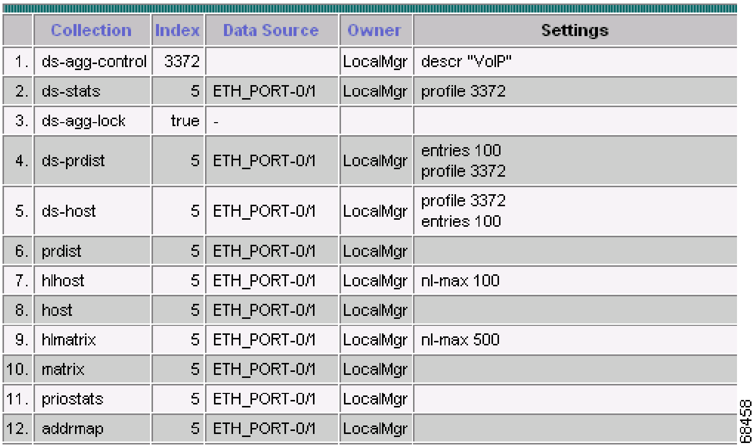
Step 1 Click the Admin tab.

Step 2 Click **Diagnostics**.

Step 3 In the contents, click **Monitor and Capture Configuration**.

The Monitor and Capture Configuration Table is displayed (Figure 2-10).

Figure 2-10 Monitor and Capture Configuration Table



	Collection	Index	Data Source	Owner	Settings
1.	ds-agg-control	3372		LocalMgr	descr "VoIP"
2.	ds-stats	5	ETH_PORT-0/1	LocalMgr	profile 3372
3.	ds-agg-lock	true	-		
4.	ds-prdist	5	ETH_PORT-0/1	LocalMgr	entries 100 profile 3372
5.	ds-host	5	ETH_PORT-0/1	LocalMgr	profile 3372 entries 100
6.	prdist	5	ETH_PORT-0/1	LocalMgr	
7.	hlhost	5	ETH_PORT-0/1	LocalMgr	nl-max 100
8.	host	5	ETH_PORT-0/1	LocalMgr	
9.	hlmatrix	5	ETH_PORT-0/1	LocalMgr	nl-max 500
10.	matrix	5	ETH_PORT-0/1	LocalMgr	
11.	priostats	5	ETH_PORT-0/1	LocalMgr	
12.	addrmap	5	ETH_PORT-0/1	LocalMgr	

Step 4 To save the information, select **File>Save As...** from your browser menu.

Step 5 Select an output destination, filename, and format, then click **Save**.

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.

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* or *Network Analysis Module (NM-NAM)* feature module.

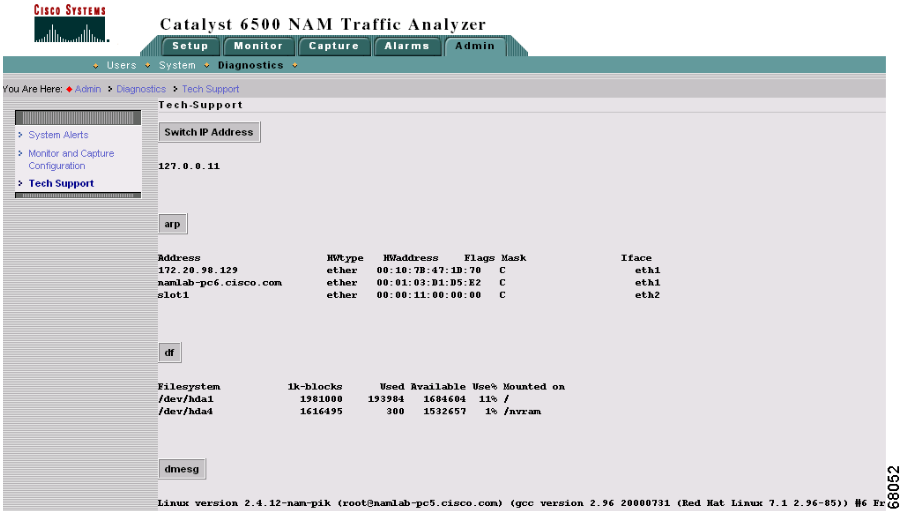
Step 1 Click the Admin tab.

Step 2 Click **Diagnostics**.

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

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window (Figure 2-11).

Figure 2-11 Diagnostics Tech Support Window



```
127.0.0.11
```

```
Address                  HWtype   HWaddress          Flags Mask            Iface
172.20.98.129            ether    00:10:7B:47:1D:70   C                     eth1
namlab-pc6.cisco.com     ether    00:01:03:D1:D5:E2   C                     eth1
slot1                    ether    00:00:11:00:00:00   C                     eth2
```

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda1              1981000    193984   1684604  11% /
/dev/hda4              1616495       300   1532657   1% /nvram
```

```
Linux version 2.4.12-nam-pik (root@namlab-pc5.cisco.com) (gcc version 2.96 20000731 (Red Hat Linux 7.1 2.96-85)) #6 Fr
```

Step 4 To save the information, select **File>Save As...** from the browser menu.

Step 5 Select an output destination, filename, and file format, then click **Save**.