CHAPTER 4

Configuring the Cisco NAM 2204 Appliance

This section describes how to configure the Cisco NAM 2204 appliance to establish network connectivity, configure IP parameters, and perform other required administrative tasks using the NAM command line interface (CLI). This chapter also provides information about how to get started with the NAM graphical user interface (GUI) and how to perform various system management tasks.

This chapter contains the following sections:

- Logging In For the First Time, page 4-1
- Establishing Network Connectivity, page 4-3
- Enabling the NAM GUI Web Server, page 4-6
- Additional Configuration Using the NAM GUI, page 4-8
- Managing the Cisco 2204 NAM Appliance, page 4-12

Note For more advanced NAM configuration information, use the NAM web GUI or see the *Cisco Prime Network Analysis Module Command Reference* at the following URL: http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1/command/reference/guide/cmdref.html

Logging In For the First Time

After you turn power on and boot the Cisco NAM 2204 appliance for the first time, the login prompt displays on the attached console. When shipped from the factory, the root user is pre configured on the Cisco NAM 2204 appliance. The default password for the root user is *root*.

Note We require you to change the user root password during the first login session.

The root user has access to the root (read/write) level of NAM and can enter NAM command-line interface (CLI) commands.

To log in to the Cisco NAM 2204 appliance for the first time, open a console session or a serial session with the NAM appliance:

Note After your initial login, you can enable **telnet** and **ssh** connections to the NAM appliance.

Step 1 When the NAM login prompt appears, enter **root** and press **Enter**.

```
nam.localdomain login: root
```

Step 2 When the password prompt appears, enter **root** and press **Enter**.

After you enter the ID and password, you will be prompted to change the root password.

```
Cisco 2200 NAM Appliance (NAM2200)

nam.localdomain login: root
Password: root

Cisco 2200 NAM Appliance (NAM2200) Console, 5.1(1)
Copyright (c) 1999-2011 by Cisco Systems, Inc.

System Alert! Default password has not been changed!
Please enter a new root user password.
Enter new UNIX password:
```

Step 3 Enter the new password for the root user.

We recommend that you make a record of the password, and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies. See Changing the Root Password, page 4-2.

```
Retype new UNIX password:
passwd: password updated successfully
root@nam.localdomain#
```

Changing the Root Password

This section describes how to change the root user password after the initial login session. To change the root password:

Step 1 Open a console session or serial session with the NAM appliance.

Step 2 When prompted for a username, enter **root**.

The Cisco NAM 2204 appliance ships from the factory with default settings for user **root** with a password of **root**.

Step 3 When prompted, enter the password for user root.

After you log in as the root user, you have read and write access to the root level of the NAM appliance, and you can enter and perform CLI commands.

```
root@hostname#
```

Step 4 Enter the following command to change the root user password.

password root

```
New password:

Confirm password:
```

Step 5 Enter the new password for user root and confirm it.

We recommend that you make a record of the password and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies.

Step 6 Enter **exit** to end the session and log out.

Examples

This section provides the following examples:

- Changing the NAM Root Password: Example, page 4-3
- Verifying the NAM Root Password: Example, page 4-3

Changing the NAM Root Password: Example

```
root@nam1.company.com# password root
Changing password for user root
New UNIX password: <rtpswd>
Retype new UNIX password: <rtpswd>
passwd:all authentication tokens updated successfully
root@nam1.company.com#
root@nam1.company.com# exit
```

Verifying the NAM Root Password: Example

```
nam1.company.com login: root
Password: <rtpswd>
Terminal type: vt100

Cisco Network Analysis Module (NAM 2200 Appliance) Console, 5.1
Copyright (c) 2011 by Cisco Systems, Inc.

root@nam1.company.com#
root@nam1.company.com# exit
```

Establishing Network Connectivity

This section describes how to configure the Cisco NAM 2204 appliance to configure IP parameters and establish network connectivity.

Log into the Cisco NAM 2204 appliance from the management console and enter the following CLI commands with the appropriate information for your site:

Step 1 Use the **ip address** command to configure the NAM appliance IP address. The syntax for this command is as follows:

ip address *ip-address subnet-mask*

Example

```
root@localhost# ip address 172.20.104.126 255.255.255.248
```

Step 2 (Optional) You can use the **ip broadcast** command to configure the NAM appliance broadcast address. The syntax for this command is as follows:

ip broadcast *broadcast-address*

Example

```
root@localhost# ip broadcast 10.255.255.255
```

Step 3 Use the **ip gateway** command to configure the NAM appliance default gateway address. The syntax for this command is as follows:

ip gateway *ip-address*

Example

```
root@localhost# ip gateway 172.20.104.123
```

Step 4 (Optional) You can use the **exsession** command to enable remote login to the NAM appliance using either Telnet or SSH. The **excession on ssh** requires crypto patch to be installed. See Enabling the NAM GUI Web Server, page 4-6, to know how to download and install the software K9 cryptographic patch.

The syntax for this command is as follows:

exsession on *(for Telnet)*

or

exsession on ssh *(for SSH)*

Examples

To configure the NAM appliance to enable Telnet access:

```
root@localhost# exsession on
```

To configure the NAM appliance to enable SSH access:

```
root@localhost# exsession on ssh
```

Note The NAM software K9 cryptographic patch is required to configure the **ssh** option.

Step 5 You can use the **ip domain** command to configure the NAM appliance system domain name. The syntax for this (optional) command is as follows:

ip domain *name*

Example

```
root@localhost# ip domain your_company.com
```

Step 6 You can use the **ip host** command to configure the NAM appliance system hostname.

The syntax for this command is as follows:

ip host *name*

Example

```
root@localhost# ip host nam_machine
```

Step 7 You might (optionally) want to use the **ip nameserver** command to configure one or more name servers for the NAM appliance.

The syntax for this command is as follows:

ip nameserver *ip-address [ip-address] [ip-address}*

Examples

```
root@localhost# ip nameserver 172.20.104.10

root@localhost# ip nameserver 172.20.104.10  172.20.104.20  172.20.104.30
```

Checking Your Configuration

After you finish configuring the NAM appliance for network connectivity, it is a good idea to check your connectivity and verify the IP parameters you have just configured for the NAM appliance.

Step 1 Use the **show ip** command to verify that you have configured the NAM appliance IP parameters the way you want them.

The syntax for this command is as follows:

show ip

```
root@localhost# show ip

root@nam1.company.com# show ip
```

Sample Output for the show ip NAM CLI Command

The following is an example of the **show ip** command output that shows a configured NAM appliance:

```
root@nam1.company.com# show ip

IP address:            172.20.105.215
Subnet mask:           255.255.255.192
IP Broadcast:          10.255.255.255
DNS Name:              nam1.company.com
Default Gateway:       172.20.105.210
Nameserver(s):         209.165.201.29
HTTP server:           Disabled
HTTP secure server:    Disabled
TACACS+ configured:    No
Telnet:                Enabled
SSH:                   Disabled
root@nam1.company.com#
```

Step 2 Use the **ping** command to check connectivity between the NAM appliance and a network device.

The syntax for this command is as follows:

ping *{hostname* | *ip-address}*

Examples

```
root@localhost# ping nam_machine.your_company.com

root@localhost# ping 172.20.104.10
```

The following is an example of the **ping** command showing successful connectivity:

```
root@nam_machine.your_company.com# ping 172.20.104.10
PING 172.20.104.10 (172.20.104.10) 56(84) bytes of data.
64 bytes from 172.20.104.10: icmp_seq=1 ttl=254 time=1.27 ms
64 bytes from 172.20.104.10: icmp_seq=2 ttl=254 time=1.13 ms
64 bytes from 172.20.104.10: icmp_seq=3 ttl=254 time=1.04 ms
64 bytes from 172.20.104.10: icmp_seq=4 ttl=254 time=1.08 ms
64 bytes from 172.20.104.10: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.104.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.043/1.129/1.278/0.090 ms
root@nam_machine.your_company.com#
```

Enabling the NAM GUI Web Server

This section describes how to enable the NAM web server and browser-based access to the NAM graphical user interface (GUI).

To enable the NAM web server and provide browser-based access, the following prerequisites must be met:

- If you plan to use the HTTP secure server (HTTPs), you must first download and install the NAM software K9 cryptographic patch. You can download the NAM software K9 cryptographic patch from Cisco.com.

  After downloading the software, install the patch using the following command:

  patch <ftp url>

  <ftp url>: *ftp://<username>@<host>/<path>/<filename>*. The username is optional based on the ftp server setting.

  For example: **patch ftp://10.1.1.2/patch/nam-5-0-k9.patch**

Note The **ip http secure** commands remain disabled until you install the patch.

- Ensure that your web browser supports your NAM software release. For a list of supported browsers, see the NAM software release notes at the following URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html

To enable the NAM web server:

Step 1 Open a Telnet or SSH session to the NAM appliance and at the password prompt, enter your password.

telnet {ip-address | hostname}

or

ssh {ip-address | hostname}

Step 2 Enter one of the following commands to enable either an HTTP server or an HTTPS secure server:

To enable the NAM HTTP web server:

ip http server enable

To enable the NAM HTTPS secure web server:

ip http secure server enable

The NAM requests a web administrator user name.

```
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]: <CR>
```

The NAM web server requires at least one properly-configured web administrator. If the NAM does not prompt you for a web username and password, then at least one web administrator was previously configured.

Step 3 Enter the username of the web administrator. Otherwise, press **Enter** to use the default web administrator username *admin*.

The NAM requests a password for the web administrator, then requests the password to be entered again to ensure accuracy.

```
New password: <adminpswd>

Confirm password: <adminpswd>
```

Step 4 Enter the password for the web administrator and confirm it. Otherwise, press **Enter** to use the default web administrator password *adminpswd*.

Note Because this document is available to the public by way of Cisco.com, it is a good idea to change this and all default passwords as soon as possible.

Enabling the Web Server Summary

The following summarizes the steps or interaction when you enable the NAM web server and access to it.

```
root@localhost# ip http server enable

No web users are configured.
Please enter a web administrator user name [admin]: <CR>
New password: <admin-passwd>
Confirm password: <admin-passwd>

User admin added.
Starting httpd
```

Checking the NAM GUI Web Server

After you have configured the NAM web server and enabled access to it, you should check that the web server is working by launching a browser and trying to log in to the NAM.

To check the NAM web server functionality, launch an approved internet browser and enter the IP address or host and domain name in the browser address field.

Note For a list of supported browsers, see the NAM software release notes at: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html

If the Cisco NAM 2204 Appliance web server is properly configured, you should be able to access the NAM. At this point, the only user able to log into the NAM web server is the administrative user you configured when you enabled the web server.

Additional Configuration Using the NAM GUI

After you log in through the NAM login window, you have access to the NAM graphical user interface (GUI). The NAM GUI is a web-based interface that uses five main tabs for you to set up and use the NAM. The five main tabs are:

- Monitor
- Analyze
- Capture
- Setup
- Administration

For detailed information on the NAM GUI, see the User Guide for your NAM software release. You can find a PDF file of the user guide in the online help of the NAM GUI and on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_user_guide_list.html

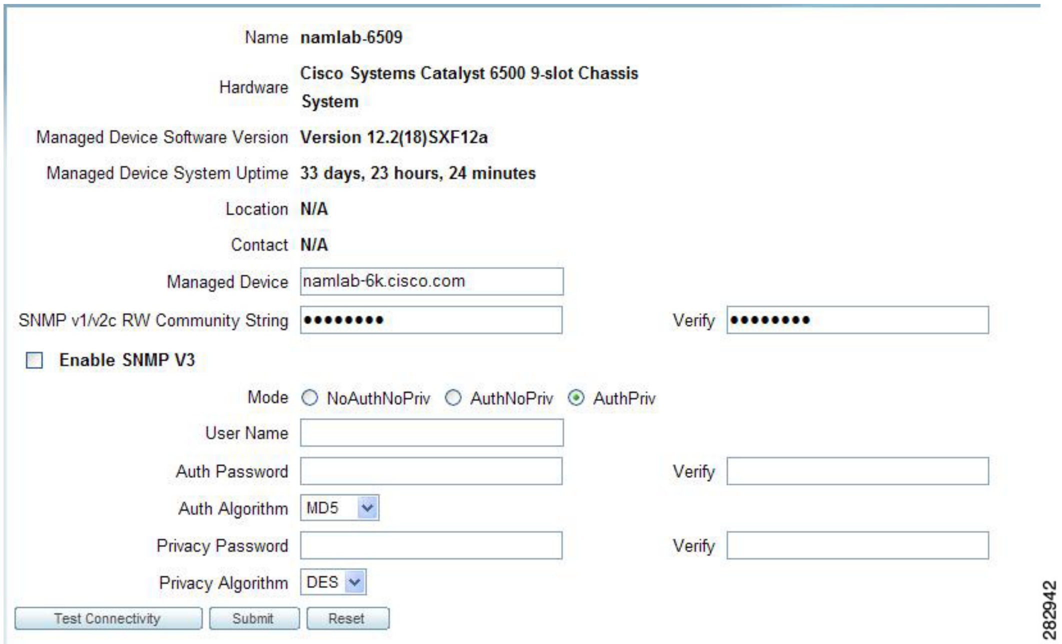
After you log in to the NAM GUI, perform the following tasks:

Step 1 Go to the **Setup** > **Managed Device> Device Information** window, and enter the parameters for your managed device in the Managed Device Information window.

Figure 4-1 shows the Managed Device Information window.

For more detailed information about the parameters required to set up a managed device, see Chapter 3 of the User Guide at http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_user_guide_list.html

Figure 4-1 *Managed Device Information Window*

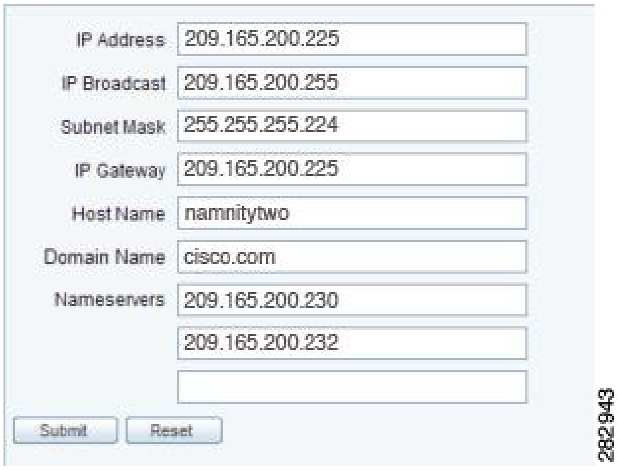


Name	namlab-6509		
Hardware	Cisco Systems Catalyst 6500 9-slot Chassis System		
Managed Device Software Version	Version 12.2(18)SXF12a		
Managed Device System Uptime	33 days, 23 hours, 24 minutes		
Location	N/A		
Contact	N/A		
Managed Device	namlab-6k.cisco.com		
SNMP v1/v2c RW Community String	••••••••	Verify	••••••••
□ Enable SNMP V3			
Mode	○ NoAuthNoPriv ○ AuthNoPriv ● AuthPriv		
User Name			
Auth Password		Verify	
Auth Algorithm	MD5		
Privacy Password		Verify	
Privacy Algorithm	DES		

Step 2 Go to the **Administration** > **System** window, and click Network Parameters in the content menu.

Figure 4-2 shows an example of the Network Parameters window. Use this window to enter additional network connectivity parameters such as your site's name servers.

Figure 4-2 *Network Parameters Window*

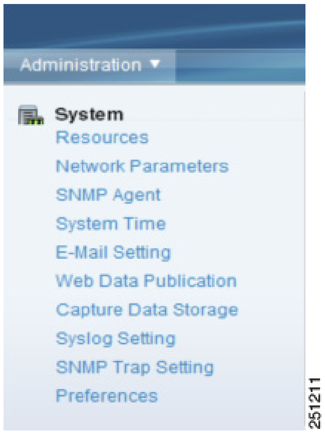


IP Address	209.165.200.225
IP Broadcast	209.165.200.255
Subnet Mask	255.255.255.224
IP Gateway	209.165.200.225
Host Name	namnitytwo
Domain Name	cisco.com
Nameservers	209.165.200.230
	209.165.200.232

Step 3 Continue with each option in the content menu of the **Administration** > **System** window.

Figure 4-3 shows the content menu of the **Administration** > **System** window. The default view of that window is the System Overview window.

Figure 4-3 Administration > System Content Menu



You can find detailed information about the options in the **Administration** > **System** window content menu in the User and System Administration chapter of the *Cisco Prime Network Analysis Module User Guide.*

Step 4 If you plan to use SNMP, go to the **Administration** > **System** > **SNMP Agent** window. Set the community strings for the NAM SNMP agent and enter the administrative contact information.

Step 5 Go to the **Administration** > **System** > **System Time** window, and configure the NAM system time to synchronize with either the local managed device or an external network time protocol (NTP) server.

The default setting is to synchronize with the local managed device. If NTP is used for time synchronization, enter at least one NTP server name or IP address.

Note You must configure the NAM local time zone regardless of the time synchronization method.

Step 6 Go to the **Administration** > **System** > **E-Mail Setting** window, and enter the POP or external mail server for your organization. Also enter a complete E-mail address to receive a test message when you have completed the E-mail configuration.

Step 7 Go to the **Administration > System > Web Data Publication** window, and check each item you want to make available for Web Data Publishing. The publication code, if required, must be present in the URL address or cookie to enable access to published data.

Step 8 Go to the **Administration** > **System** > **Capture Data Storage** window, and enter the parameters required to set up capture storage to remote disks using either iSCSI or NFS storage systems.

Step 9 Go to the **Administration** > **System** > **Syslog Setting** window, and specify optional remote syslog server names (up to five) to receive syslog messages from NAM. NAM syslogs are created for alarm threshold events, voice threshold events, or system alerts. You can use the NAM to view the local NAM syslogs.

Step 10 Go to the **Administration** > **System** > **SNMP Trap Setting** window**,** and enter the parameters required to configure traps.

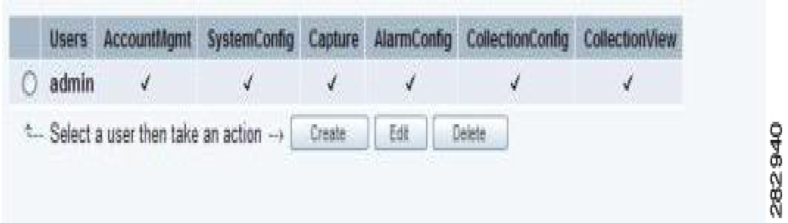
Step 11 Go to the **Administration** > **System** > **Preferences** window**,** and enter the prefered parameters.

If you plan to use the local user database, continue with the next step. If you plan to use a TACACS+ database, proceed to **Step 13**.

Step 12 Go to the **Administration** > **Users** > **Local Database** window, and click **Create** to add any administrative users who require access. Click **Edit** to make any changes to the privilege each administrative user require for the functions they might perform, and **Delete** to remove the user access.

Figure 4-4 shows an example of the default local user database window.

Figure 4-4 Administration > Users > Local Database Window



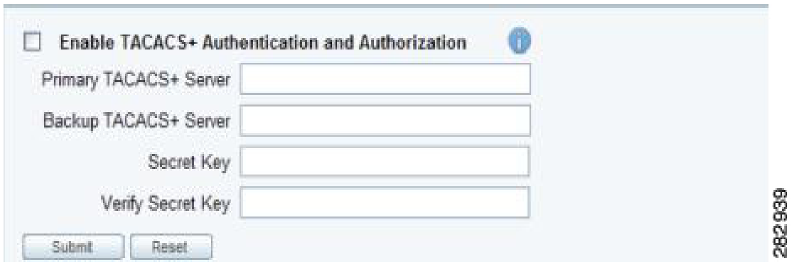
	Users	AccountMgmt	SystemConfig	Capture	AlarmConfig	CollectionConfig	CollectionView
○	admin	✓	✓	✓	✓	✓	✓

Step 13 If you plan to use a TACACS+ server for authentication and authorization (AA), go to the **Administration** > **Users > TACACS+** window, and enter the parameters required to access the TACACS+ server for authentication and authorization.

Enter the IP address of the TACACS+ server and the secret key to communicate with the server. The secret key must be the same as the one configured in the TACACS+ server.

Figure 4-5 shows an example of the **Administration** > **Users > TACACS+** window.

Figure 4-5 Administration > Users > TACACS+ Window



□ Enable TACACS+ Authentication and Authorization

Primary TACACS+ Server	
Backup TACACS+ Server	
Secret Key	
Verify Secret Key	

Managing the Cisco 2204 NAM Appliance

This section contains the following information:

- Shutting Down and Starting Up Cisco NAM 2204 appliance, page 4-12
- Verifying System Status, page 4-12
- Configuring Logging Options and Generating Diagnostics, page 4-13
- Opening and Closing a Telnet or SSH Session to the NAM, page 4-13

Note

- The tables in these sections show only common managed device and network module commands.
  - To view a complete list of available commands, type **?** at the prompt (Example: `user@nam_host.domain# ?`).
  - To view a complete list of command keyword options, type **?** at the end of the command (Example: `nam_host.domain# ip ?`).
- The tables group commands by the configuration mode in which they are available. If the same command is available in more than one mode, it might act differently in each mode.

Shutting Down and Starting Up Cisco NAM 2204 appliance

To shut down the Cisco NAM 2204 appliance, issue the **shutdown** command.

The Cisco NAM 2204 appliance reboots after you press the Power button.

Verifying System Status

To verify the status of an installation, upgrade, or downgrade or to troubleshoot problems, use commands from those listed in Table 4-1, Common diagnostic and Show Commands.

Note Among keyword options for many **show** commands is provision to display diagnostic output on your screen or to pipe it to a file or a URL.

Table 4-1 Common diagnostic and Show Commands

Command	Purpose
show audit-trail	Displays the web GUI logins and CLI access settings
show configuration	Displays the current bootloader configuration as entered using the **configure** command
show ip	Displays the IP parameters
show patches	Displays any installed patches
show tech-support	Displays general information about the host router that is useful to Cisco technical support for problem diagnosis

Table 4-1 Common diagnostic and Show Commands (continued)

Command	Purpose
show time	Displays the NAM system time settings
show version	Displays information about the loaded router, software, or network module bootloader version, and also hardware and device information.

Configuring Logging Options and Generating Diagnostics

To configure logging options for Cisco NAM 2204 appliance, use commands as needed from the list of common network module commands shown in Table 4-2.

Note Some keyword options for many of the **log** and **trace** commands is provision to display diagnostic output on your screen or to pipe it to a file or a URL.

Table 4-2 Common System Log Commands

Configuration Mode	Command	Purpose
`host.domain#`	**show log**	Displays the contents of the specified log.
	copy log	Saves the system log to a destination of your choice.
	show logs	Displays a list of available log files.

What to Do Next

Verify that the default root password of *root* is accepted by performing the steps described in the "Opening and Closing a Telnet or SSH Session to the NAM" section on page 4-13.

To change the NAM root password, see the "Changing the Root Password" section on page 4-2.

Opening and Closing a Telnet or SSH Session to the NAM

This procedure opens and closes a Telnet or SSH session to the NAM. This procedure is not commonly performed, because you would typically use the NAM (web GUI) to monitor and maintain the NAM. If, however, you cannot access the NAM, then you might want to use Telnet or SSH to troubleshoot from the NAM CLI.

If your Cisco NAM 2204 appliance is not properly configured for Telnet or SSH access (see the following Prerequisites, page 4-13 section), then you can open a Telnet session to the managed device to which the Cisco NAM 2204 appliance is connected, then open a NAM console session from the managed device.

Prerequisites

- Configure the NAM system IP address. Optionally, set the NAM system hostname.
- Verify NAM network connectivity by performing one of the following ping tests:

  - From a host beyond the gateway, ping the NAM system IP address.
  - From the NAM CLI, ping the NAM system default gateway.

Telnet Prerequisites

- Enter the **exsession on** NAM CLI command.

SSH Prerequisites

- Install the NAM software K9 cryptographic patch, which you can download from Cisco.com.
- Enter the **exsession on ssh** NAM CLI command.

SUMMARY STEPS

1. **telnet** {*ip-address* | *hostname*}
   or
   ssh {*ip-address* | *hostname*}
2. At the login prompt, enter **root**.
3. At the password prompt, enter your password.
   or
   If you have not changed the password from the factory-set default, enter **root** as the root password.
4. Perform the tasks that you need to perform in the NAM CLI. When you want to end the Telnet or SSH session to the NAM and return to the Cisco IOS CLI, complete Step 5 and Step 6.
5. **exit**
6. **logout**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`telnet {ip-address | hostname}`
	or
	`ssh {ip-address | hostname}`
	Example:
	`host.domain# telnet 10.20.30.40`
	Example:
	`host.domain# ssh 10.20.30.40`
		Logs into a host that supports Telnet.
		or
		Starts an encrypted session with a remote networking device.
		• Use the NAM system IP address or NAM system hostname.

Step 2	At the login prompt, enter **root**. **Example:** `login: root`	Accesses the root (read/write) level of NAM.

	Command or Action	Purpose
Step 3	At the password prompt, enter your password. or If you have not changed the password from the factory-set default, enter **root** as the root password. **Example:** `Password: root`	—
Step 4	Perform the tasks that you need to perform in the NAM CLI. When you want to end the Telnet or SSH session to the NAM and return to the Cisco IOS CLI, complete Step 5 and Step 6.	For help using NAM CLI commands.

Step 5	**`exit`**
	Example:
	`root@localhost(sub-custom-filter-capture)# exit`
	`root@localhost#`
		Leaves a subcommand mode.
		• Return to command mode.

Step 6	**`logout`**
	Example:
	`root@localhost# logout`
	`Connection closed by foreign host.`
		Logs out of the NAM system.

Examples

Opening and Closing a Telnet Session to the NAM Using the NAM System IP Address: Example

```
nam_host> telnet 172.20.105.215
Trying 172.20.105.215 ... Open

Cisco Network Analysis Module (NAM 2200 Appliance)

login: root
Password: <password>
Terminal type: vt100

Cisco Network Analysis Module (NAM 2200 Appliance) Console, 5.1
Copyright (c) 2011 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nam.company.com#
root@nam.company.com# logout

[Connection to 172.20.105.215 closed by foreign host]
nam_host>
```

Opening and Closing an SSH Session to the NAM Using the NAM System Hostname: Example

```
host [/home/user] ssh -l root namappl
root@namappl's password: <password>
Terminal type: vt100
```

```
Cisco Network Analysis Module (NAM 2200 Appliance) Console, 5.1
Copyright (c) 2011 by cisco Systems, Inc.

WARNING! Default password has not been changed!
root@namappl.company.com#
root@namappl.company.com# logout

Connection to namappl closed.
host [/home/user]
```