



Cisco Branch Routers Series Network Analysis Module (NME-NAM-120S) Installation and Configuration Note, 5.1

OL-24402-01

The Cisco Prime Network Analysis Module (NAM) is an integrated module that enables network managers to understand, manage, and improve how applications and services are delivered to end-users.

The Cisco Prime portfolio of enterprise and service provider management offerings supports integrated lifecycle management of Cisco architectures and technologies based on a service-centric framework. Built on an intuitive workflow-oriented user experience, Cisco Prime products help increase IT productivity and reduce operations costs through innovative management solutions for the network services, infrastructure, and endpoints.

The NAM offers flow-based traffic analysis of applications, hosts, and conversations, performance-based measurements on application, server, and network latency, quality of experience metrics for network-based services such as voice over IP (VoIP) and video, and problem analysis using deep, insightful packet captures. NAM includes an embedded, web-based GUI that provides quick access to the configuration menus and presents easy-to-read performance reports on Web, voice, and video traffic.

The NME-NAM-120S is the most recent NAM model offered for the branch routers. The NAM software runs on the NAM and is directly reachable as an end-station and includes its own SNMP agent, HTTP server and command-line interface (CLI). The NAM software communicates with the IOS software on the router.

NAM software supports NME-NAM-120S and NME-NAM-80S modules on branch routers including the 2800, 2900, 3700, 3800, and 3900 series multi-services and integrated services routers.



Note

This document specifically addresses the NAM software installation and configuration with the NME-NAM-120S, but also supports the NME-NAM-80S.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

- [Prerequisites for NME-NAM-120S, page 2](#)
- [Restrictions for the NME-NAM-120S, page 4](#)
- [NAM Software, page 4](#)
- [How to Install, Upgrade, or Downgrade NME-NAM-120S, page 7](#)
- [Configuring the NME-NAM-120S for Management, page 20](#)
- [Managing the NME-NAM-120S, page 45](#)
- [Additional References, page 49](#)
- [Glossary, page 52](#)

Prerequisites for NME-NAM-120S

The following prerequisites are required to use the NME-NAM-120S module with NAM software.

Supported Branch Routers

The NME-NAM-120S (and NME-NAM-80S) can be deployed in any network module slot in the Cisco router platforms listed in [Table 1](#). A Network Module (NM) Adapter Card, SM-NM-ADPTR, is required to successfully integrate the NME-NAM into supported ISR G2 platforms. The NME-NAM supports the router platforms with NAM software version 3.6 or later. Only one Cisco NAM can be installed in a Cisco branch router.

Table 1 NME-NAM Supported Router Platforms

Router Platform	IOS Version (Minimum)	NM Adapter Card Required?
Cisco 3945 ISR	Cisco IOS 15.0(1)M	Yes
Cisco 3925 ISR	Cisco IOS 15.0(1)M	
Cisco 2951 ISR	Cisco IOS 15.0(1)M	
Cisco 2921 ISR	Cisco IOS 15.0(1)M	
Cisco 2911 ISR	Cisco IOS 15.0(1)M	
Cisco 3845 ISR	Cisco IOS 12.4(9)T	No
Cisco 3825 ISR	Cisco IOS 12.4(9)T	
Cisco 2851 ISR	Cisco IOS 12.4(9)T	
Cisco 2821 ISR	Cisco IOS 12.4(9)T	
Cisco 2811 ISR	Cisco IOS 12.4(9)T	
Cisco 3745 MSR	Cisco IOS 12.4(9)T	
Cisco 3725 MSR	Cisco IOS 12.4(9)T	

To determine which IOS release your router is currently running, examine the output of the **show version** command.

Network Modules

To install an NME-NAM-120S network module, see the following:

- *Connecting Cisco NAM Enhanced Network Modules to the Network*
<http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/namnme.html>
- *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*
<http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html>

To install an NME-NAM-120S network module in supported ISR G2 platforms using the NM Adapter Card, see the following:

- *Installing Cisco Network Modules and Service Modules*, section “Using Network Modules in Service Module Slots on Cisco 2900 Series and Cisco 3900 Series Routers”:
<http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/InstNetM.html>

NME-NAM-120S

- The **NME-NAM-120S** ships from the factory with the following:
 - 120 GB hard disk
 - 1 GB memory
 - 64 MB flash memory
- Make a note of the network module location in the host router:
 - *slot*—Number of the router chassis slot for the module. After you install the module, you can get this information from the router’s **show running-config** command output and look for interface Integrated-Service-Engine.



Note You need this information for the “Setting Up Network Module Interfaces” section on page 7 and the “Closing a Session” section on page 11.

File Server

- Verify that your download FTP or TFTP file server is accessible:
 - FTP file server—Use for installations, backups, and restores.
 - TFTP file server—Use (on the FTP-file-server machine) for boothelper operations to recover from a failed installation.

Restrictions for the NME-NAM-120S

The following restrictions currently exist for NAM and the NME-NAM-120S.

- [Upgrade or Downgrade](#)
- [Configuration](#)
- [Monitoring Traffic Through Internal Interface](#)



Warning

The NME-NAM module is not hot swappable. You must shutdown and turn off power to the router before inserting or removing an NME-NAM module.

Upgrade or Downgrade

You can upgrade or downgrade NAM software in a production environment. Although the NAM will not be operational during the upgrade or downgrade procedure, the router should remain fully operational. Downloading the NAM software image will generate some additional network traffic, but should not affect router operations.

Configuration

- You can only configure the NME-NAM-120S initially from a session that is initiated from the router.
- After you configure the NME-NAM-120S network parameters, you can enable access to the software running on the network module using one of the following:
 - The router's Cisco IOS CLI
 - The NME-NAM-120S graphical user interface (GUI), secure-shell (SSH) connection, or telnet connection
 - SNMP

Monitoring Traffic Through Internal Interface



Note

The following restriction applies only to traffic that is monitored through the internal NAM interface.

The NAM (web GUI) provides Layer 3 and higher layer information about the original packets. The Layer 2 header is modified by the router when it forwards the packets to the NAM, so the Layer 2 information that the NAM records is not applicable to the original packets.

NAM Software

The NAM software application resides on a network module that plugs into a host Cisco router running Cisco IOS software.

The network module is a standalone service engine with its own startup and run-time configurations that are independent of the Cisco IOS configuration on the router. The module does not have an external console port. Instead, you launch and configure the module through the router, by means of a configuration session on the module. After the session, you return to the router CLI and clear the session.

This arrangement—host router plus network module (the latter is also sometimes called an appliance or blade or, with installed software, a service or services engine)—provides a router-integrated application platform for accelerating data-intensive applications including the following and more:

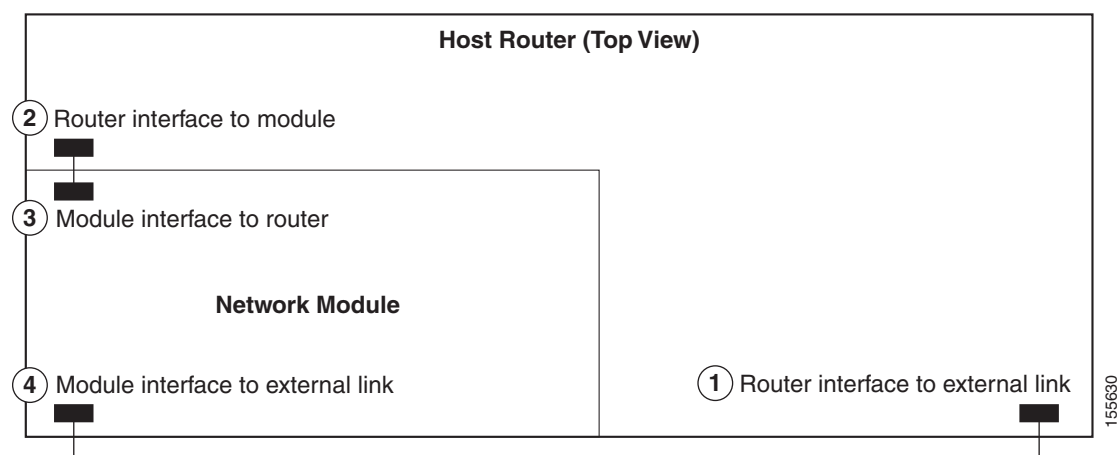
- Application-oriented networking
- Contact centers and interactive-voice-response applications
- Content caching and delivery
- Data and video storage
- Network analysis
- Voice mail and auto-attendant applications

Hardware Interfaces

The host router and network module use several interfaces for internal and external communication (see [Figure 1](#)). Each interface is configurable both from the router by using the Cisco IOS CLI and from the module by using the module's CLI.

The NME-NAM-120S can monitor traffic on both the external and the internal interface at the same time. However, only one can be used for management traffic.

Figure 1 Router and Network Module Interfaces



	On This Hardware Interface...	Configure These Settings...	Using This Configuration Method
1	Router interface (for example, Gig0/0)	Standard router settings	Router's Cisco IOS CLI
2	Router side interface to NME-NAM-120S. This is the <i>integrated-service-engine</i> interface on the router.	Module's IP address and default gateway router	
3	INTERNAL interface of the NME-NAM-120S. This is a Gigabit Ethernet (GE) interface.	All other module and NME-NAM-120S application settings	Module's NME-NAM-120S CLI, GUI, telnet, SSH interface, or SNMP
4	EXTERNAL interface of the NME-NAM-120S. This is a Gigabit Ethernet interface.	Support for data requests and transfers from outside sources	

How to Install, Upgrade, or Downgrade NME-NAM-120S

This section contains the following information:

- [Setting Up Network Module Interfaces, page 7](#)
- [Closing a Session, page 11](#)
- [Upgrading NAM Software, page 12](#)



Note

- If you lose power or connection during any of the following procedures, the system usually detects the interruption and tries to recover. If it fails to do so, fully reinstall the system using the boothelper.
- You can configure the network module by means of either the CLI or the GUI. This document presents CLI configuration instructions. For GUI configuration instructions, see the GUI's online help.

Setting Up Network Module Interfaces

Your first configuration task is to set up network module interfaces to the host router and to its external links. This configuration enables you to access the module to install and configure NME-NAM-120S.



Note

The first few steps open the host-router CLI and access the router's interface to the module. The subsequent steps configure the interface.

SUMMARY STEPS

From the Host-Router CLI

1. **enable**
2. **configure terminal**
3. **interface integrated-service-engine <slot>/0**
4. **ip address** *router-side-ip-address subnet-mask*
or
ip unnumbered *type number*
5. [Optional, but if done, do not do **Step 6**] **service-module ip address** *module-side-ip-address subnet-mask*
6. [Optional, but if done, do not do **Step 5**] **service-module external ip address** *external-ip-address subnet-mask*
7. [Optional] **service-module ip default-gateway** *gateway-ip-address*
8. **end**
9. **copy running-config startup-config**
10. **show running-config**

DETAILED STEPS

Command or Action	Purpose
From the Host-Router CLI	
<p>Step 1 <code>enable</code></p> <p>Example: Router> enable</p>	<p>Enters privileged EXEC mode on the host router. Enter your password if prompted.</p>
<p>Step 2 <code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode on the host router.</p>
<p>Step 3 <code>interface integrated-service-engine slot/0</code></p> <p>Example: Router(config)# interface integrated-service-engine 1/0</p>	<p>Enters interface configuration mode for the slot and port where the network module resides.</p>
<p>Step 4 <code>ip address router-side-ip-address subnet-mask</code></p> <p>or</p> <p><code>ip unnumbered type number</code></p> <p>Example: Router(config-if)# ip address 10.0.0.20 255.255.255.0</p> <p>or</p> <p>Router(config-if)# ip unnumbered ethernet 0/0</p>	<p>Specifies the router interface to the module. Arguments are as follows:</p> <ul style="list-style-type: none"> • <i>router-side-ip-address subnet-mask</i>—IP address and subnet mask for the interface. • <i>type number</i>—Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface. Serial interfaces using High Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered.
<p>Step 5 <code>service-module ip address module-side-ip-address subnet-mask</code></p> <p>Example: Router(config-if)# service-module ip address 172.0.0.20 255.255.255.0</p>	<p>Specifies the IP address for the module interface to the router. Arguments are as follows:</p> <ul style="list-style-type: none"> • <i>module-side-ip-address</i>—IP address for the interface • <i>subnet-mask</i>—Subnet mask to append to the IP address; must be in the same subnet as the host router <p>This command selects and configures the internal interface for management traffic. This command is equivalent to using the commands ip interface internal and ip address <address> <mask> on the NME-NAM-120S CLI.</p> <p>Note If you want to use the external interface for management traffic use the Step 6 instead.</p>

	Command or Action	Purpose
Step 6	<p>service-module external ip address <i>external-ip-address</i> <i>subnet-mask</i></p> <p>Example: Router(config-if)# service-module external ip address 172.0.0.30 255.255.255.0</p>	<p>Specifies the IP address for the external LAN interface on the module. Arguments are as follows:</p> <ul style="list-style-type: none"> <i>external-ip-address</i>—IP address for the interface <i>subnet-mask</i>—Subnet mask to append to the IP address <p>This command selects and configures the external interface for management traffic. This command is equivalent to using the commands ip interface external and ip address <address> <mask> on the NME-NAM-120S CLI.</p> <p>Note If you want to use the internal interface for management traffic, use the Step 5 instead.</p>
Step 7	<p>service-module ip default-gateway <i>gateway-ip-address</i></p> <p>Example: Router(config-if)# service-module ip default-gateway 10.0.0.40</p>	<p>Specifies the IP address for the default gateway router for the module. The argument is as follows:</p> <ul style="list-style-type: none"> <i>gateway-ip-address</i>—IP address for the gateway router <p>Note Use this step only if you used Step 5 or Step 6.</p>
Step 8	<p>end</p> <p>Example: Router(config-if)# exit</p>	<p>Returns to global configuration mode on the host router.</p>
Step 9	<p>copy running-config startup-config</p> <p>Example: Router# copy running-config startup-config</p>	<p>Saves the router's new running configuration.</p>
Step 10	<p>show running-config</p> <p>Example: Router# show running-config</p>	<p>Displays the router's running configuration, so that you can verify address configurations.</p>

Examples

The following partial output from the **show running-config** command shows how the interfaces are configured.

```
interface Integrated-Service-engine1/0
 ip address 10.0.0.20 255.255.255.0
 service-module ip address 10.0.0.21 255.255.255.0
 service-module ip default-gateway 10.0.0.20
```

Opening a Session

This section describes how to open a session on the network module.



Note

- Before you install your application software, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.
- You can conduct only one session at a time.

SUMMARY STEPS

From the Router CLI

1. **enable**
2. **service-module integrated-service-engine slot/0 session clear**
3. **service-module integrated-service-engine slot/0 session**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enters privileged EXEC mode on the host router. Enter your password if prompted.
Step 2	service-module integrated-service-engine slot/0 session clear Example: Router# service-module integrated-Service-Engine 1/0 session clear [confirm] [OK] Router#	Make sure there is not an existing session which will prevent this session to login successfully.
Step 3	service-module integrated-service-engine slot/0 session Example: Router# service-module integrated-Service-Engine 1/0 session Trying 172.20.98.151, 2066 ... Open Cisco Network Analysis Module (NME-NAM-120S) NAM.domain.name login:	Begins a session on the specified module.

Closing a Session

This section describes how to close a session on the network module.



Note

- Before you install your application software, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.
- You can conduct only one session at a time.
- In NAM, the CLI command **exit** automatically closes a session.

SUMMARY STEPS

Use the following steps to close a session:

From the NAM CLI, NAM login, NAM helper, or NAM bootloader prompts

1. **Control-Shift-6 x**

From the Router prompt

2. **disconnect** *<or>*
service-module integrated-service-engine slot/0 session clear

DETAILED STEPS

	Command or Action	Purpose
	From the NAM CLI, NAM login, NAM helper, or NAM bootloader prompts	
Step 1	Press Control-Shift-6 x . Note This key sequence returns you to the router prompt.	Closes the service-module session and returns to the router CLI. Note The service-module session stays up until you clear it in the next step. While it remains up, you can return to it from the router CLI by pressing Enter .
	From the Router CLI	
Step 2	disconnect <i>or</i> service-module integrated-service-engine slot/0 session clear Example: Router# service-module integrated-Service-Engine 1/0 session clear [confirm] [OK] Router#	Disconnects the session connection or clears the service module session for the specified module. When prompted to confirm this command, press Enter .

Upgrading NAM Software

During software upgrades, you use the Bootloader, a small set of system software that runs when the system first powers up. The Bootloader loads and runs the NAM application. The bootloader might optionally load and run the helper image on flash memory.

Upgrading software involves installing, configuring, and starting a helper image. The helper, in turn, starts the NAM installation wizard, which installs the software.

**Note**

Plan software upgrades for times when you can take all applications that run on the host router out of service or offline.

NAM Software Images

The NME-NAM-120S contains three NAM software images:

- Bootloader image in flash memory—Use to specify whether to boot the NAM application image or the helper image
- Helper image in flash memory—Use to recover NAM software images
- NAM application image on the hard drive—Source of the NAM and NAM CLI

Types of NAM Software Upgrades

NAM software upgrades are available in two forms:

- Images—Full image releases that are installed from the helper image. Full image upgrades are typically used to update the NAM application image, and if necessary and recommended by technical support, you can also use the helper image to upgrade the bootloader image or helper image.
- Patches—Incremental updates to software versions that are installed with the **patch** NAM CLI command. Patches are available only for the NAM application image.

Perform one of the following procedures in this section, depending on whether you are adding a patch to your NAM application or are performing a full software image upgrade:

- [Upgrading the NME-NAM-120S Application Image \(Full Image\), page 13](#)
- [Upgrading the NAM Application Image — Patch, page 16](#)

Prerequisites

- Download the NAM software image from Cisco.com
- Copy the image to an FTP server.
- (Optional) Have available the IP address of your TFTP file server.

Upgrading the NME-NAM-120S Application Image (Full Image)

This section provides summary and detailed steps about how to upgrade the full NME-NAM-120S application image.

SUMMARY STEPS

From the Router CLI

1. Download the required software.
2. **service-module integrated-service-engine slot/0 reload**
3. **service-module integrated-service-engine slot/0 session**

From the Service-Module Interface

While the service module reboots, it displays the following prompt:

```
Enter *** to change boot configuration:
```

4. Enter ***.

After you enter ***, the NAM should display the bootloader prompt. From this prompt, you can either boot the NAM helper located at a TFTP server or boot the pre-installed helper image in the NAM flash.

- To boot the NAM helper image from a TFTP server, do Steps 5, 6, and 7. Skip Step 8, then do Steps 9, 10, and 11.
- To boot the pre-installed helper image on the NAM compact flash, skip Steps 5, 6, and 7, then do Steps 8 through 11.

5. **configure**

(and follow the prompts)

6. **show config**

7. boot helper

8. **boot compactflash**

At this point, you should be at the helper image menu.

9. Select either option **1** or option **2**, and follow the prompts.
10. Select **r**.
11. Close the session as described in [Closing a Session, page 11](#).

DETAILED STEPS

-
- Step 1** Download the NME-NAM-120S installation-package files (containing a kernel image, a helper image, and the NME-NAM-120S application software files) as follows:
- a. Go to the NAM page of the Cisco Software Center website.
 - b. Locate the NME-NAM-120S Application Image Release 5.1 for Cisco Branch Routers.
 - c. Download the files to one of the following locations:
 - FTP file server
 - HTTP server

Step 2 Reset the system:

```
Router> enable
Router# service-module integrated-service-engine slot/0 reload
```

Step 3 Session into the NME-NAM-120S console.

```
ServiceEngine boot-loader> service-module integrated-service-engine slot/0 session
```

While the service module reboots, it displays the following prompt:

```
Enter *** to change boot configuration:
```

Step 4 Enter *** to go to the bootloader.

After you enter ***, you will be at the bootloader prompt. From this prompt, you can either boot the NAM helper located at a TFTP server or boot the pre-installed helper image in the NAM flash.

- To boot the NAM helper image from a TFTP server, do Steps 5, 6, and 7. Skip Step 8, then do Steps 9, 10, and 11.
- To boot the pre-installed helper image on the NAM compact flash, skip Steps 5, 6, and 7, then do Steps 8 through 11.

Step 5 Configure the bootloader to load and launch the helper:

```
ServiceEngine bootloader> config
```

Prompts for the following appear in the order listed. For each, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.

- NME-NAM-120S IP address and subnet mask
- TFTP file-server IP address
- Default gateway of NME-NAM-120S (normally the IP address for the ISR)
- Default helper image filename
- Ethernet interface: internal or external of NME-NAM-120S
- Default boot option is to boot the NAM 5.1 image from disk.
- Default bootloader file to be used on subsequent boot: primary or secondary

**Note**

Primary causes the application to launch normally.
Secondary causes the application to start the primary bootloader; the primary bootloader then checks the secondary bootloader location and, if it finds the secondary bootloader and if the checksum is correct, uses the secondary bootloader.

Example:

```
ServiceEngine bootloader> config
IP Address [10.100.20.81] >
Subnet mask [255.255.255.0] >
TFTP server [10.107.150.30] >
Gateway [10.100.20.80] >
Default Helper-file [cue-installer.10.2.0.13] >
Ethernet interface [internal] >
Default Boot [none|disk] >
Default bootloader [primary|secondary] [primary] >
ServiceEngine bootloader>
```

Step 6 (Optional) Verify your bootloader configuration settings:

```
ServiceEngine bootloader> show config
```

Example:

```
ServiceEngine boot-loader> show config
IP addr:                172.20.98.152
Netmask:                255.255.255.192
TFTP server :          172.20.98.175
GW IP addr:            172.20.98.129
eth int:               internal
Default boot:         disk
Bootloader Version:   2.1.12
Bootloader Name:     DEV_BOOTLOADER
Default Helper-file:  nme-nam-helper.bin
Default bootloader:  secondary
External i/f media:  copper
```

```
ServiceEngine boot-loader>
```

Step 7 Enter **boot helper**.

```
ServiceEngine bootloader> boot helper
```

Step 8 Enter **boot flash**.

```
ServiceEngine bootloader> boot compactflash
```

Step 9 Using helper menu install the application image. Use option 2 to reformat the HDD and install the application image. Using Option 2 is useful if the HDD image is corrupted, but all configuration will be lost.

Example:

```
Cisco Systems, Inc.
Services engine helper utility for NME-NAM-120S
Version 1.1(0.5)
```

```
-----
```

```
Main menu
```

```
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Download bootloader and write to flash
4 - Download helper and write to Compact Flash
5 - Display software versions
6 - Reset application image CLI passwords to default
7 - Change file transfer method (currently ftp/http)
8 - Show upgrade log
9 - Send Ping
f - Format the Compact Flash
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine
```

```
Selection [123456789frh]:
```

Step 10 Reboot the NME-NAM-120S using helper menu option *r*.

Step 11 Close the session as described in [Closing a Session, page 11](#).

Upgrading the NAM Application Image — Patch

This section describes how to add a patch to your NAM application image from the NAM CLI.

SUMMARY STEPS

1. Access the NME-NAM-120S console by following the steps described in [Opening a Session, page 10](#).



Note Depending on the previous state of the session, you might be prompted to log in to the NAM CLI.

2. At the NME-NAM-120S prompt, enter one of:
patch *ftp://user:passwd@host/full-path/filename*
 or
patch *ftp://user@host/full-path/filename*
3. **show patches**
4. Close the session as described in [Closing a Session, page 11](#).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Follow the steps described in Opening a Session, page 10 to close the NAM console session.	Initiate a console connection in the NME-NAM-120S. Log in to the NAM CLI.
Step 2	patch <i>ftp://user:password@host/full-path/filename</i> or patch <i>ftp://user@host/full-path/filename</i>	Downloads and installs a software patch. <ul style="list-style-type: none"> • Use the first option, which includes the password, if the FTP server does not allow anonymous users. • If you use the second option, enter your password when prompted.
Step 3	show patches Example: root@nam1.company.com# show patches	Displays all installed patches. Verify that your patch was successfully installed.
Step 4	Follow the steps described in Closing a Session, page 11 to close the NAM console session.	Close the NAM console session.

Upgrading the NAM Helper Image (NAM CLI)

This section describes how to upgrade the NAM helper image stored on the NAM compact flash. The NAM must be running its application image for these steps to work.

SUMMARY STEPS

1. Download the NAM helper image from Cisco.com and load it to an FTP server.
2. Open a session to the NAM CLI by following the steps in [Opening a Session, page 10](#). (Login if prompted).
3. **upgrade** <ftp-URL>
4. **exit**
5. Close the NAM session as described in [Closing a Session, page 11](#).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Download the NME-NAM-120S helper image from Cisco.com and load it to a FTP server.	Note The FTP server must be reachable from NAM CLI.
Step 2	Follow the steps described in Opening a Session, page 10 to close the NAM console session. Example: Router# service-module integrated-Service-Engine 1/0 session clear [confirm] [OK] Router# service-module integrated-Service-Engine 1/0 session Trying 172.20.98.151, 2066 ... Open Cisco Network Analysis Module (NME-NAM-120S) NAM.domain.name login: root Password: Last login: Tue July 2 22:04:43 2009 on ttyS0 Linux NAM.domain.name 2.6.10-nam #1 SMP Mon Dec 11 10:44:04 PST 2009 i68 6 GNU/Linux Cisco Network Analysis Module (NME-NAM-120S) Console, 5.1 Copyright (c) 1999-2011 by cisco Systems, Inc. WARNING! Default password has not been changed! root@NAM.domain.com#	Initiate a console connection in the NME-NAM-120S. Log in to the NAM CLI.

	Command or Action	Purpose
Step 3	Upgrade <ftp-url>, then follow the prompt.	Download and save the NAM helper image to the NAM flash.
Step 4	<p><code>exit</code></p> <p>Example:</p> <pre>root@NAM.domain.name# exit Cisco Network Analysis Module (NME-NAM-120S) NAM.domain.com login:</pre>	Exit the NAM CLI prompt and get to the NAM login prompt.

Upgrading the NAM Helper Image

This section describes how to upgrade the NAM helper image.

SUMMARY STEPS

1. Download the NAM helper image from Cisco.com and store it on an FTP server.

From the Router Enable (exec) Mode Prompt

2. `service-module integrated-service-engine slot/0 reload`
3. `service-module integrated-service-engine slot/0 session`



Note This will open a connection to the NAM console.

From the Service Module Interface

While the service module reboots, it displays the following prompt:

```
Enter *** to change boot configuration:
```

4. **Enter ***.**

After you enter *** in Step 4 above, you will be at the bootloader prompt. From this prompt, you can either boot the NAM helper located at a TFTP server or boot the pre-installed helper image in the NAM flash.

- To boot the NAM helper image that is located at a TFTP server, do Steps 5, 6, and 7. Skip Step 8.
- To boot the pre-installed helper image on the NAM compact flash, skip Steps 5, 6 and 7, then do Steps 8-11.

5. `configure`
6. `show config`
7. `boot helper`
8. `boot compactflash`
9. Select 4, and follow the prompts.
10. Select r, and confirm the reboot the NAM.
11. Close the NAM console connection as described in [Closing a Session, page 11](#).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Download the NME-NAM-120S helper image from Cisco.com and load it to an FTP server.	Note The FTP server must be reachable from NAM CLI.
Step 2	From the router exec prompt, apply the IOS command: <code>service-module integrated-service-engine slot/0 reload</code> Example: Router# <code>service-module integrated-Service-Engine 1/0 reload</code> Use reset only to recover from shutdown or failed state Warning: May lose data on the hard disc! Do you want to reset?[confirm] Trying to reset Service Module Integrated-Service-Engine1/0.	Reboot the NAM.
Step 3	<code>service-module integrated-Service-Engine slot/0 session</code> Example: Router# <code>service-module integrated-Service-Engine 1/0 session</code> Trying 172.20.98.151, 2066 ... Open	Open a connection to the NAM console. Note Pay attention to the messages that scroll up the screen. When prompted to enter ***, do so.
Step 4	Enter *** Note If you want to boot the pre-installed helper image, skip Steps 5, 6 and 7. Note If you do Steps 5, 6, and 7, skip Step 8. Note Step 5, 6, and 7 are useful in case the pre-installed helper image on the NAM flash has been corrupted. These steps reinstall the helper image.	Break to the NAM bootloader prompt.
Step 5	<code>configure</code>	Configure the bootloader to load and launch the helper. Note Follow the prompts to enter NME address, subnet mask, TFTP server address, NAM default gateway address, helper image filename. Press Enter to accept the previously store input that appears inside the square brackets.
Step 6	<code>show config</code>	Verify the bootloader configuration.
Step 7	<code>boot helper</code>	Boot the NAM helper image that is located on the TFTP server.
Step 8	<code>boot compactflash</code> Note Skip this step if you performed Steps 5, 6, and 7.	Boot the helper image located on the NAM flash. Note NAM is shipped with a helper image on its flash memory.

	Command or Action	Purpose
Step 9	<p>Select 4, and follow the prompt to enter a FTP URL</p> <pre>Main menu 1 - Download application image and write to HDD 2 - Download application image and reformat HDD 3 - Download bootloader and write to flash 4 - Download helper and write to Compact Flash 5 - Display software versions 6 - Reset application image CLI passwords to default 7 - Change file transfer method (currently ftp/http) 8 - Show upgrade log 9 - Send Ping f - Format the Flash r - Exit and reset Services Engine h - Exit and shutdown Services Engine Selection [123456789frh]: 4</pre>	Download helper image from FTP server and write to NAM flash.
Step 10	Select r and confirm to reboot the NAM	Reboot the NAM. By default the NAM will boot to the NAM application image.
Step 11	Follow the steps described in Closing a Session, page 11 to close the NAM console session.	Close the NAM console session.

Configuring the NME-NAM-120S for Management

NME-NAM-120S has an internal Gigabit Ethernet interface and an external interface. You can use either interface for NAM management traffic such as the NAM web GUI, **telnet** or **ssh**, but not both. You can configure the NAM internal interface to use either IP unnumbered or a routable subnet.

See the following sections for information about how to configure the NME-NAM-120S internal interfaces for management:

- [Configuring the Internal Interface for Management—IP Unnumbered, page 20](#)
- [Configuring the Internal Interface for Management—Routable Subnet, page 24](#)
- [Configuring the External Interface for Management, page 27](#)

Configuring the Internal Interface for Management—IP Unnumbered

This section describes how to configure the NME-NAM-120S internal interface for IP unnumbered.



Note

The addresses used for the interface address (Step 4), the NAM-Address (Steps 6 and 9), and the NAM-Default-Gateway-Address (Step 7) must all be in the same subnet.

SUMMARY STEPS

From the Router Prompt

1. **enable**
2. **configure terminal**
3. `interface integrated-service-engine slot/0`
4. `ip unnumbered interface number`
5. **no shutdown**
6. `service-module ip address NAM-Address subnetmask`
7. `service-module ip default-gateway NAM-Default-Gateway-Address`
8. **exit**
9. `ip route NAM-Address 255.255.255.255 integrated-service-engine slot/0`
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enter IOS exec mode.
Step 2	<code>configure terminal</code>	Enter IOS configuration from terminal mode.
Step 3	<code>interface integrated-service-engine slot/0</code>	Enter IOS interface configuration mode for the integrated-service-engine interface.
Step 4	<code>ip unnumbered <interface> <number></code> Example: Router (config-if)# <code>ip unnumbered gigabitethernet 0/1</code>	Borrow the address that was set at <interface>. In the example, interface integrated-service-engine 1/0 borrows the address set in gigabitethernet0/1 interface.
Step 5	<code>no shutdown</code>	Enable the integrated-service-engine interface.
Step 6	<code>service-module ip address <NAM-Address> <subnetmask></code> Router (config-if)# <code>service-module ip address 209.165.200.226 255.255.255.224</code>	Set <NAM-Address> to the NAM Internal interface.
Step 7	<code>service-module ip default-gateway <NAM-Default-Gateway-Address></code> Example: Router (config-if)# <code>service-module ip default-gateway 209.165.200.225</code>	Setup the NAM default gateway address.
Step 8	<code>exit</code>	Exit from the router interface configuration mode to the router global configuration mode.

	Command or Action	Purpose
Step 9	<pre>ip route <NAM-Address> 255.255.255.255 integrated-service-engine slot/0</pre> <p>Example: Router(config)# <code>ip route 209.165.200.226 255.255.255.255 integrated-service-engine 1/0</code></p>	Setup a full 32-bit static route for the NAM management address.
Step 10	<code>end</code>	Exit the router configuration mode.

Configuration Example

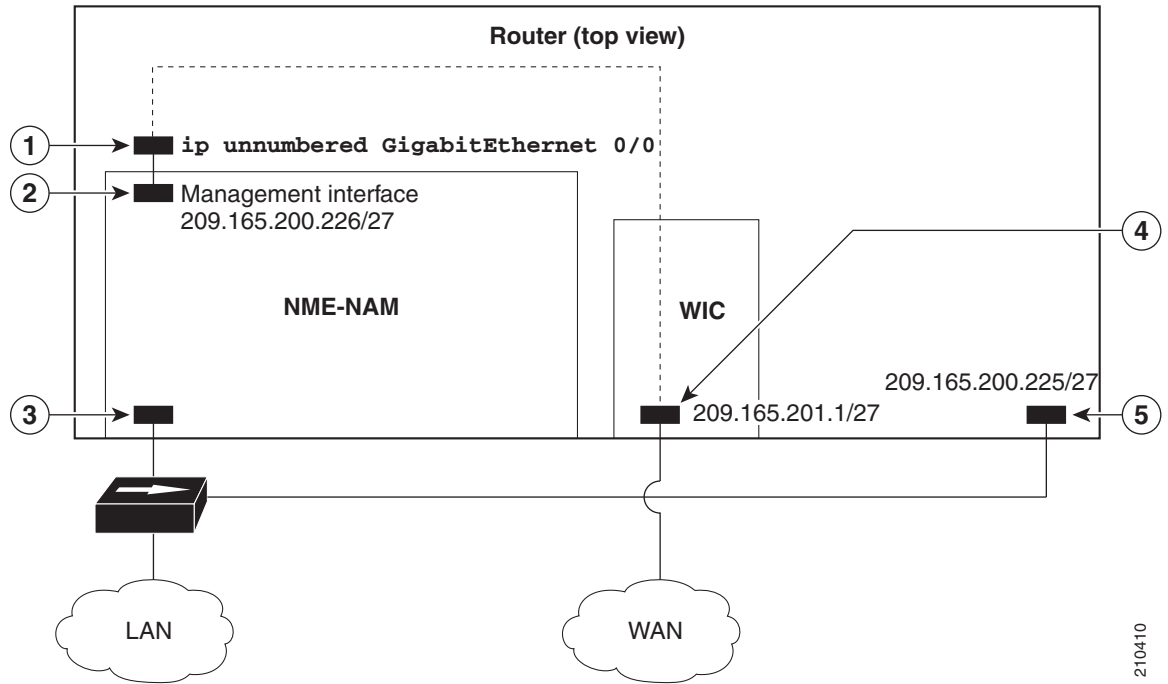
In this configuration example:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Integrated-Service-Engine interface and the NAM system
- To conserve IP address space, the Integrated-Service-Engine interface is configured as IP unnumbered to borrow the IP address of the Gigabit Ethernet interface.
- A static route to the NAM through the Integrated-Service-Engine interface is configured.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Gigabit Ethernet 0/0.
- The NME-NAM-120S is installed in router slot 2.

Figure 2 shows the topology used in the example, and the following sections show the router and NAM configurations:

- [Router Configuration \(Cisco IOS Software\), page 23](#)
- [NAM Configuration \(NAM Software\), page 24](#)

Figure 2 NAM Management Interface Is Internal and Integrated-Service-Engine Interface Is Unnumbered: Sample Topology



210410

Callout	Interface	Location
1	Integrated-Service-Engine interface	Router internal
2	Internal NAM interface (Management)	NME-NAM-120S internal
3	External NAM interface	NME-NAM-120S faceplate
4	Serial interface	WAN interface card (WIC)
5	GigabitEthernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```

!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.224
 duplex auto
 speed auto
 analysis-module monitoring
!
interface Integrated-Service-Engine2/0
 ip unnumbered GigabitEthernet0/0
 ip nbar protocol-discovery
 no keepalive
!
!
ip route 209.165.200.226 255.255.255.255 Integrated-Service-Engine2/0
!
!

```

NAM Configuration (NAM Software)

```

root@myNAM.company.com# show ip
IP address:                209.165.200.226
Subnet mask:               255.255.255.224
IP Broadcast:             209.165.200.255
IP Interface:             Internal
DNS Name:                 myNAM.company.com
Default Gateway:          209.165.200.225
Nameserver(s):           171.69.2.133
HTTP server:              Enabled
HTTP secure server:      Disabled
HTTP port:                80
HTTP secure port:        443
TACACS+ configured:      No
Telnet:                   Enabled
SSH:                      Disabled
    
```

Configuring the Internal Interface for Management—Routable Subnet

This section describes how to configure the NME-NAM-120S internal interface for management using a routable subnet method.

SUMMARY STEPS

From the Router Prompt

1. **enable**
2. **configure terminal**
3. **interface integrated-service-engine slot/0**
4. **ip address <router-side-address> <subnetmask>**
5. **no shutdown**
6. **service-module ip address <NAM-Address> <subnetmask>**
7. **service-module ip default-gateway <router-side-address>**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enter IOS exec mode.
Step 2	configure terminal	Enter IOS configuration from terminal mode.
Step 3	interface integrated-service-engine slot/0	Enter the IOS interface configuration mode for the integrated-service-engine interface.

	Command or Action	Purpose
Step 4	<pre>ip address <router-side-address> <subnetmask></pre> <p>Example: Router (config-if)# <code>ip address 209.165.200.225 255.255.255.224</code></p>	Set a routable address to the integrated-service-engine interface.
Step 5	<pre>no shutdown</pre>	Bring up the integrated-service-engine interface.
Step 6	<pre>service-module ip address <NAM-Address> <subnetmask></pre> <p>Example: Router (config-if)# <code>service-module ip address 209.165.200.226 255.255.255.224</code></p>	Set NAM-Address to the NAM Internal interface. Note The NAM-Address must be in the same subnet as router-side-address.
Step 7	<pre>service-module ip default-gateway <router-side-address></pre> <p>Example: Router (config-if)# <code>service-module ip default-gateway 209.165.200.225</code></p>	Setup NAM default gateway address to be the integrated-service-engine interface address, which is router-side-address.
Step 8	<pre>end</pre>	Exit the router configuration mode.

Configuration Example

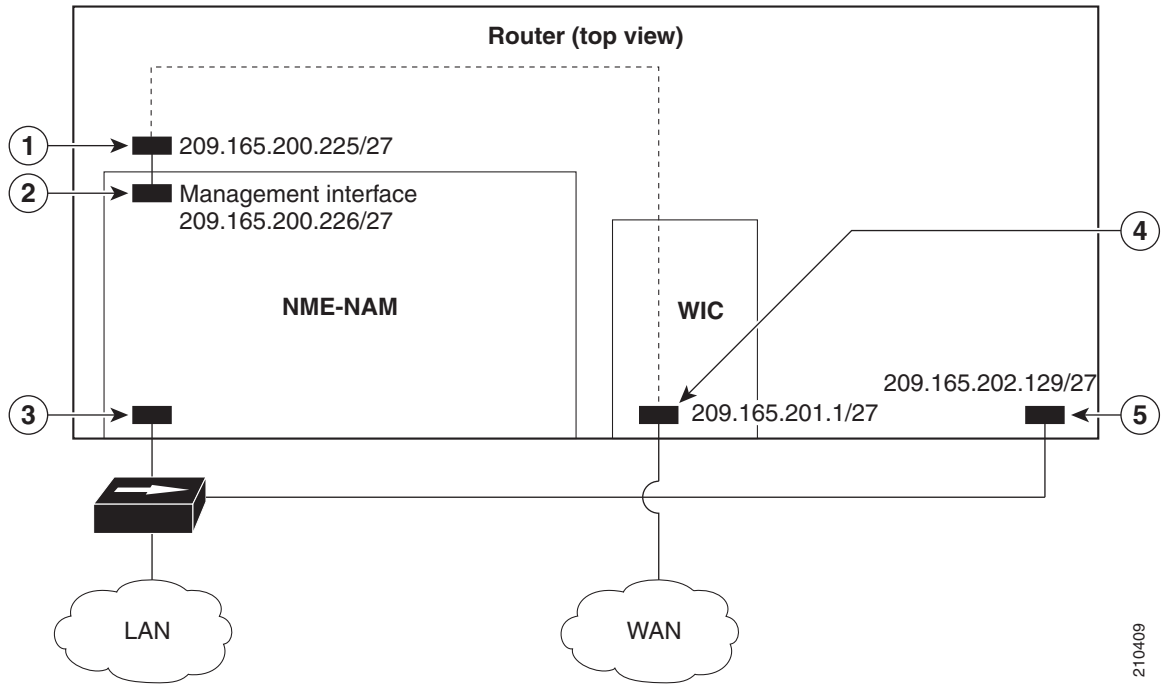
In this configuration example:

- The internal NAM interface is used for management traffic.
- IP addresses from the same routable subnet are assigned to the Integrated-Service-Engine interface and the NAM system.
- A static route to the NAM through the Integrated-Service-Engine interface is configured.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Fast Ethernet 0/0.
- The NME-NAM-120S is installed in router slot 2.

Figure 3 shows the topology used in the example, and the following sections show the router and NAM configurations:

- [Router Configuration \(Cisco IOS Software\), page 26](#)
- [NAM Configuration \(NAM Software\), page 26](#)

Figure 3 *NAM Management Interface Is Internal and Integrated-Service-Engine Interface Is Assigned an IP Address: Sample Topology*



210409

Callout	Interface	Location
1	Integrated-Service-Engine interface	Router internal
2	Internal NAM interface (Management)	NME-NAM-120S internal
3	External NAM interface	NME-NAM-120S faceplate
4	Serial interface	WAN interface card (WIC)
5	Fast Ethernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```
!
interface Integrated-Service-Engine2/0
 ip address 209.165.200.225 255.255.255.224

ip route 209.165.200.226 255.255.255.255 Integrated-Service-Engine1/0
```

NAM Configuration (NAM Software)

```
root@myNAM.company.com# show ip
IP address:          209.165.200.226
Subnet mask:         255.255.255.224
IP Broadcast:        209.165.200.255
```

```

IP Interface:           Internal
DNS Name:              myNAM.company.com
Default Gateway:      209.165.200.225
Nameserver(s):       171.69.2.133
HTTP server:         Enabled
HTTP secure server:  Disabled
HTTP port:           80
HTTP secure port:    443
TACACS+ configured:  No
Telnet:              Enabled
SSH:                 Disabled

```

Configuring the External Interface for Management

This section describes how to configure the NME-NAM-120S to use its external interface for NAM management traffic.

SUMMARY STEPS

From the Router Prompt

1. **enable**
2. **configure terminal**
3. **interface loopback** *loopback-number*
4. **ip address** *bogus-address subnetmask*
5. **no shutdown**
6. **exit**
7. **interface integrated-service-engine** *slot/0*
8. **ip unnumbered loopback** *loopback-number*
9. **no shutdown**
10. **service-module external ip address** *NAM-Address subnetmask*
11. **service-module ip default-gateway** *NAM-Default-Gateway-Address*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enter IOS exec mode.
Step 2	configure terminal	Enter IOS configuration from terminal mode.
Step 3	interface loopback <loopback-number> Router (config)# interface loopback 0 Router (config-if)#	Create a loopback interface 0 on the router.

	Command or Action	Purpose
Step 4	<pre>ip address <bogus-address> <subnetmask></pre> <p>Example: Router(config-if)# ip address 10.1.1.1 255.255.255.0</p>	Set a bogus address on the loopback interface. In the example, interface loopback0 is assigned with an address 10.1.1.1/24.
Step 5	<pre>no shutdown</pre>	Enable the loopback interface.
Step 6	<pre>exit</pre> <p>Example: Router(config-if)# exit Router(config)#</p>	Exit from interface configuration mode to the global configuration mode.
Step 7	<pre>interface integrated-service-engine slot/0</pre>	Enter the IOS interface configuration mode for the integrated-service-engine interface.
Step 8	<pre>ip unnumbered loopback <number></pre> <p>Example: Router (config-if)# ip unnumbered loopback 0</p>	Borrow the address that was set to the loopback interface in Step 4 .
Step 9	<pre>no shutdown</pre>	Bring up the integrated-service-engine interface.
Step 10	<pre>service-module external ip address <NAM-Address> <subnetmask></pre> <p>Example: Router (config-if)# service-module external ip address 209.165.201.2 255.255.255.224</p>	Set <NAM-Address> to the NAM External interface.
Step 11	<pre>service-module ip default-gateway <NAM-Default-Gateway-Address></pre> <p>Router (config-if)# service-module ip default-gateway 209.165.201.222</p>	Setup the NAM default gateway address.
Step 12	<pre>end</pre>	Exit the router configuration mode.

Configuration Example

In this configuration example:

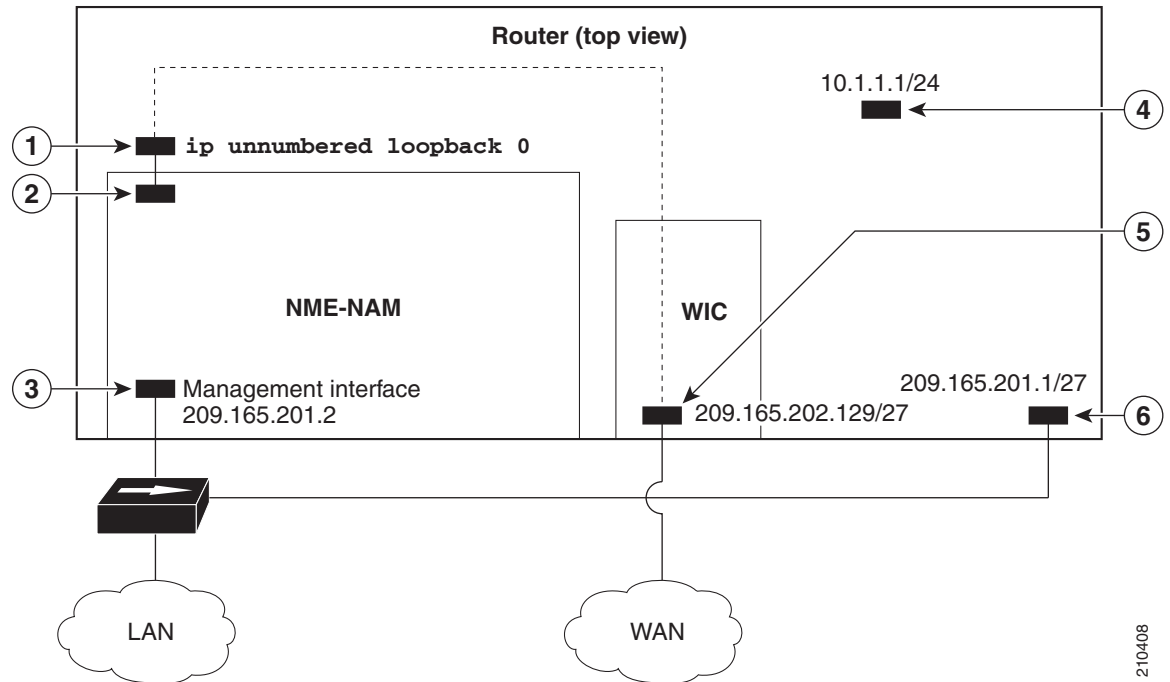
- The external NAM interface is used for management traffic.
- The Integrated-Service-Engine interface is configured as IP unnumbered to borrow the IP address of the loopback interface.
- The borrowed loopback interface IP address is not routable.
- The NAM system is configured with an IP address from the LAN subnet that is connected to the external NAM interface.
- The internal NAM interface is used to monitor WAN traffic on interface Serial 0/0, and the external NAM interface is used to monitor LAN traffic on interface Fast Ethernet 0/0.

- The NME-NAM-120S is installed in router slot 3.

Figure 4 shows the topology used in the example, and the following sections show the router and NAM configurations:

- Router Configuration (Cisco IOS Software), page 29
- NAM Configuration (NAM software), page 30

Figure 4 NAM Management Interface Is External and Integrated-Service-Engine Interface Is IP Unnumbered: Sample Topology



Callout	Interface	Location
1	Integrated-Service-Engine interface	Router internal
2	Internal NAM interface	NME-NAM-120S internal
3	External NAM interface (Management)	NME-NAM-120S faceplate
4	Loopback interface	Router internal
5	Serial interface	WAN interface card (WIC)
6	Fast Ethernet interface	Router rear panel

Router Configuration (Cisco IOS Software)

```
!
interface loopback 0
 ip address 10.1.1.1 255.255.255.0
!
!
interface Integrated-Service-Engine3/0
 ip unnumbered loopback 0
```

```
no shutdown
!
```

NAM Configuration (NAM software)

```
root@myNAM.company.com# show ip
IP address:                209.165.201.2
Subnet mask:               255.255.255.224
IP Broadcast:             209.165.201.223
IP Interface:             External
DNS Name:                  myNAM.company.com
Default Gateway:          209.165.201.222
Nameserver(s):            171.69.2.133
HTTP server:              Enabled
HTTP secure server:       Disabled
HTTP port:                80
HTTP secure port:         443
TACACS+ configured:       No
Telnet:                   Enabled
SSH:                      Disabled
```

Disabling AAA Login Authentication on the NAM Console Line

If you configured authentication, authorization, and accounting (AAA) on your router, then you might have to log in twice to open a NAM console session from the router: first with your AAA username and password, and second with the NAM login and password.

If you do not want to log in twice to open a NAM console session from the router, then disable AAA login authentication on the router's NAM console line by performing this procedure.

Note, however, that if your router contains both the NME-NAM-120S and the NM-CIDS, the Cisco intrusion detection system network module, then AAA can be a useful tool for centrally controlling access to both network modules. For information about AAA, see the [Cisco IOS Security Configuration Guide](#) for your Cisco IOS release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login *list-name* none**
4. **line *number***
5. **login authentication *list-name***
6. **end**
7. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa authentication login list-name none</p> <p>Example: Router(config)# aaa authentication login name none</p>	<p>Creates a local authentication list.</p> <ul style="list-style-type: none"> The none keyword specifies no authentication for this list.
Step 4	<p>line number</p> <p>Example: Router(config)# line 33</p>	<p>Enters line configuration mode for the line to which you want to apply the authentication list.</p> <ul style="list-style-type: none"> The <i>number</i> value is determined by the slot number in which the NME-NAM-120S is installed: $number = (32 \times slot) + 1$ (for Cisco 3700 series) $number = (32 \times slot) + 1 \times 2$ (for Cisco 2800 and Cisco 3800 series)
Step 5	<p>login authentication list-name</p> <p>Example: Router(config-line)# login authentication name</p>	<p>Applies the authentication list to the line.</p> <ul style="list-style-type: none"> Specify the authentication list name that you configured in Step 3.
Step 6	<p>end</p> <p>Example: Router(config-line)# end</p>	<p>Returns to privileged EXEC mode.</p>
Step 7	<p>show running-config</p> <p>Example: Router# show running-config</p>	<p>Displays the contents of the currently running configuration file.</p> <ul style="list-style-type: none"> Verify that you configured the local authentication list and applied it to the line associated with the NME-NAM-120S.

Configuring the NME-NAM-120S For Network Connectivity

This section describes how to configure the NME-NAM-120S to establish network connectivity and configure IP parameters. This task must be performed from the NAM CLI. For more advanced NAM configuration, use the NAM (web GUI) or see the *Network Analysis Module Command Reference* for your NAM software release.

Prerequisites

Before doing this procedure, access the NAM console. See “Opening a Session” section on page 10.

SUMMARY STEPS



Note

You might have already done Steps 1 and 2 if you have configured the NME-NAM-120S for management using either [Configuring the Internal Interface for Management—IP Unnumbered, page -20](#) or [Configuring the External Interface for Management, page -27](#).

1. **ip interface** { **internal** | **external** }
2. **ip address** *ip-address subnet-mask*
3. [Optional] **ip broadcast** *broadcast-address*
4. **ip gateway** *ip-address*
5. **exsession on**
or
exsession on ssh
6. **ip domain** *name*
7. **ip host** *name*
8. **ip nameserver** *ip-address [ip-address][ip-address]*
9. **ping** { *host* | *ip-address* }
10. **show ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>ip interface {internal external}</p> <p>Example: root@localhost# ip interface internal</p> <p>Example: root@localhost# ip interface external</p>	Specifies which NAM interface will handle management traffic.
Step 2	<p>ip address <i>ip-address subnet-mask</i></p> <p>Example: root@localhost# ip address 172.20.104.126 255.255.255.248</p>	Configures the NAM system IP address.
Step 3	<p>ip broadcast <i>broadcast-address</i></p> <p>Example: root@localhost# ip broadcast 10.255.255.255</p>	(Optional) Configures the NAM system broadcast address.
Step 4	<p>ip gateway <i>ip-address</i></p> <p>Example: root@localhost# ip gateway 172.20.104.125</p>	Configures the NAM system default gateway address.
Step 5	<p>exsession on</p> <p>or</p> <p>exsession on ssh</p> <p>Example: root@localhost# exsession on</p> <p>Example: root@localhost# exsession on ssh</p>	<p>(Optional) Enables outside logins.</p> <ul style="list-style-type: none"> • exsession on enables Telnet access. • exsession on ssh enables SSH access. <p>Note The NAM software K9 cryptographic patch is required to configure the ssh option. See http://www.cisco.com/en/US/products/products_security_advisory09186a00801c110e.shtml for details.</p>
Step 6	<p>ip domain <i>name</i></p> <p>Example: root@localhost# ip domain company.com</p>	(Optional) Sets the NAM system domain name.

	Command or Action	Purpose
Step 7	<p>ip host <i>name</i></p> <p>Example: root@localhost# ip host nam1</p>	(Optional) Sets the NAM system hostname.
Step 8	<p>ip nameserver <i>ip-address</i> [<i>ip-address</i>] [<i>ip-address</i>]</p> <p>Example: root@nam1# ip nameserver 209.165.201.1</p>	(Optional) Sets one or more NAM system name servers. <ul style="list-style-type: none"> We recommend that you configure a name server for the NAM system to resolve Domain Name System (DNS) requests.
Step 9	<p>ping {<i>host</i> <i>ip-address</i>}</p> <p>Example: root@nam1# ping 10.20.30.40</p>	Checks connectivity to a network device. <ul style="list-style-type: none"> Verify connectivity to the router or another known host.
Step 10	<p>show ip</p> <p>Example: root@nam1# show ip</p>	Displays the NAM IP parameters. <ul style="list-style-type: none"> Verify that you properly configured the NME-NAM-120S.

Examples

This section provides the following examples:

- [Configuring the NME-NAM-120S, page 34](#)
- [Checking Network Connectivity with Ping, page 35](#)
- [Sample Output for the show ip NAM CLI Command, page 35](#)

Configuring the NME-NAM-120S

In the following example, the external NAM interface is used for management traffic. The HTTP server and Telnet access are enabled. The resulting NAM CLI prompt is `root@nam1.company.com#`.

```

root@nam.domain.name# ip interface external

root@nam.domain.name# ip address 172.20.105.215 255.255.255.192
root@nam.domain.name# ip domain company.com
root@nam.company.com# ip host myNAM
root@myNAM.company.com# ip nameserver 209.165.201.29
root@myNAM.company.com# ip gateway 172.20.105.210
root@myNAM.company.com# exsession on
root@myNAM.company.com# ip http server enable
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]:
New password:
Confirm password:

User admin added.
Successfully enabled HTTP server.
    
```

Checking Network Connectivity with Ping

```

root@myNAM.company.com# ping 172.20.98.129
PING 172.20.98.129 (172.20.98.129) 56(84) bytes of data.
64 bytes from 172.20.98.129: icmp_seq=1 ttl=254 time=1.27 ms
64 bytes from 172.20.98.129: icmp_seq=2 ttl=254 time=1.13 ms
64 bytes from 172.20.98.129: icmp_seq=3 ttl=254 time=1.04 ms
64 bytes from 172.20.98.129: icmp_seq=4 ttl=254 time=1.08 ms
64 bytes from 172.20.98.129: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.98.129 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@myNAM.company.com#

```

Sample Output for the show ip NAM CLI Command

```

root@nam1.company.com# show ip

IP address:          172.20.105.215
Subnet mask:         255.255.255.192
IP Broadcast:        10.255.255.255
IP Interface:        External
DNS Name:            nam1.company.com
Default Gateway:     172.20.105.210
Nameserver(s):       209.165.201.29
HTTP server:         Enabled
HTTP secure server:  Disabled
HTTP port:           80
HTTP secure port:    443
TACACS+ configured:  No
Telnet:              Enabled
SSH:                 Disabled
root@nam1.company.com#

```

What to Do Next

If you plan to monitor traffic through the internal NAM interface, then proceed to the [“Enabling NAM Packet Monitoring”](#) section on page 35.

If you do not plan to monitor traffic through the internal NAM interface, then proceed to the [“Enabling and Accessing the NAM”](#) section on page 38.

Enabling NAM Packet Monitoring

This section describes how to enable NAM packet monitoring on router interfaces that you want to monitor through the internal NAM interface.

When you enable NAM packet monitoring on an interface, Cisco Express Forwarding sends an extra copy of each IP packet that is received from or sent out on that interface to the NAM through the Integrated-Service-Engine interface on the router and the internal NAM interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **interface** *type slot/port*
or
interface *type slot/wic-slot/port*
5. **analysis-module monitoring**
6. Repeat [Step 4](#) and [Step 5](#) for each interface that you want the NAM to monitor.
7. **end**
8. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip cef Example: Router(config)# ip cef	Enables the Cisco Express Forwarding switching path.
Step 4	interface <i>type slot/port</i> or interface <i>type slot/wic-slot/port</i> Example: Router(config)# interface serial 0/0	Selects an interface for configuration.
Step 5	analysis-module monitoring Example: Router(config-if)# analysis-module monitoring	Enables NAM packet monitoring on the interface.
Step 6	Repeat Step 4 and Step 5 for each interface that you want the NAM to monitor through the internal NAM interface.	—

	Command or Action	Purpose
Step 7	end Example: Router(config-if)# end Router#	Returns to privileged EXEC mode.
Step 8	show running-config Example: Router# show running-config	Displays the contents of the currently running configuration file. <ul style="list-style-type: none"> Verify that you enabled the Cisco Express Forwarding switching path and enabled packet monitoring on the correct interfaces.

Examples

This section provides the following example:

- [Enabling NAM Packet Monitoring, page 37](#)

Enabling NAM Packet Monitoring

In the following example, NAM packet monitoring is enabled on the serial interfaces:

```
interface Serial 0/0
 ip address 172.20.105.213 255.255.255.240
 ip route-cache flow
 speed auto
 full-duplex
 analysis-module monitoring
 no mop enabled
!
interface Serial 0/1
 ip address 172.20.105.53 255.255.255.252
 ip route-cache flow
 duplex auto
 speed auto
 analysis-module monitoring
!
interface Integrated-Service-Engine 2/0
 ip address 10.1.1.1 255.255.255.0
 hold-queue 60 out
!
```

What to Do Next

Proceed to the [“Enabling and Accessing the NAM”](#) section on page 38.

Enabling and Accessing the NAM

This section describes how to enable and access the NAM (web GUI).

Prerequisites

- Ensure that your web browser supports your NAM software release. For a list of supported browsers, see the *Release Notes for the Network Analysis Module Software* at the following location:
http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1/release/notes/nam51note.html
- If you plan to use the HTTP secure server (HTTPs), then you must first download and install the NAM software K9 cryptographic patch. Until you install the patch, the ip http secure commands are disabled. 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**

SUMMARY STEPS

1. Open a NAM console session from the router. See the “Opening a Session” section on page 10.
or
Open a Telnet or SSH session to the NAM. See the “Opening and Closing a Telnet or SSH Session to the NAM” section on page 43.
2. **ip http server enable**
or
ip http secure server enable
3. Enter a web username.
or
Press **Return** to enter the default web username “admin”.
4. Enter a password.
5. Enter the password again.
6. On your PC, open a web browser.
7. In the web browser, enter the NAM system IP address or hostname as the URL.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>Open a NAM console session from the router. See the “Closing a Session” section on page 11.</p> <p>or</p> <p>Open a Telnet or SSH session to the NAM. See the “Opening and Closing a Telnet or SSH Session to the NAM” section on page 43.</p>	Accesses the NAM CLI.
Step 2	<pre>ip http server enable</pre> <p>or</p> <pre>ip http secure server enable</pre> <p>Example: root@localhost# ip http server enable</p> <p>Example: root@localhost# ip http secure server enable</p>	<p>Enables the HTTP server.</p> <p>or</p> <p>Enables the HTTP secure server (HTTPS).</p>
Step 3	<p>Enter a web username.</p> <p>or</p> <p>Press Return to enter the default web username <i>admin</i></p> <p>Example: Please enter a web administrator user name [admin]: joeadmin</p> <p>Example: Please enter a web administrator user name [admin]: <CR></p>	<p>Configures a web username.</p> <ul style="list-style-type: none"> The NAM requires at least one web username and password configuration. If NAM does not prompt you for a web username and password, then at least one web username and password combination was previously configured.
Step 4	<p>Enter a password.</p> <p>Example: New password: <adminpswd></p>	Configures a password for the web username.
Step 5	<p>Enter the password again.</p> <p>Example: Confirm password: <adminpswd></p>	Confirms the password for the web username.

	Command or Action	Purpose
Step 6	On your PC, open a web browser.	—
Step 7	<p>In the web browser, enter the NAM system IP address or hostname as the URL.</p> <p>Example: http://172.20.105.215/</p> <p>Example: https://172.20.105.215/</p> <p>Example: http://nam1/</p>	<p>Opens the NAM GUI in your web browser.</p> <ul style="list-style-type: none"> You are automatically redirected to the NAM login page.

Examples

This section provides the following examples:

- [Enabling the NAM, page 40](#)
- [Accessing the NAM, page 40](#)

Enabling the NAM

```
root@nam1# ip http server enable
Enabling HTTP server...
```

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

```
User admin added.
Successfully enabled HTTP server.
root@nam1#
```

Accessing the NAM

When you enter the Cisco Prime NAM system IP address or hostname as the URL in a web browser, the NAM login window appears. You must enter the username and password, and click the login button to enter into the system.

What to Do Next

For information on the NAM GUI, see the User Guide for your NAM software release. This document is available as online help within the NAM application and on Cisco.com at the following URL:

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

Changing the NAM Root Password

This procedure sets a new password to access the root (read/write) level of NAM, where you can enter NAM CLI commands. The factory-set default root password is *root*.

Prerequisites

Before performing this task, access the NAM console by performing the steps described in the “Closing a Session” section on page 11.

SUMMARY STEPS

1. **password root**
2. Enter the new password.
3. Enter the new password again.
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	password root Example: root@localhost.company.com# password root	Starts the process of changing the NAM root (read/write) level password.
Step 2	Enter the new password. Example: New UNIX password: <password>	Enters the new password.
Step 3	Enter the new password again. Example: Retype new UNIX password: <password>	Confirms the new password.
Step 4	exit Example: root@localhost# exit	Logs out of the NAM system.

Examples

This section provides the following examples:

- [Changing the NAM Root Password, page 41](#)
- [Verifying the NAM Root Password, page 42](#)

Changing the NAM Root Password

```
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

```
nam1.company.com login: root
Password: <rtpsrd>
Terminal type: vt100
Cisco Network Analysis Module (NME-NAM-120S) Console, 5.1
Copyright (c) 2007-2010 by Cisco Systems, Inc.

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

Troubleshooting Tips

If you forget the NAM root password, see the [“Resetting the NAM Root Password to the Default Value” section on page 42](#).

Resetting the NAM Root Password to the Default Value

This procedure resets the NAM root password to the default value of *root*. Use this procedure when you cannot remember the NAM root password and need to access the NAM CLI.

SUMMARY STEPS

1. **enable**
2. **service-module integrated-service-engine *slot/0* password-reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	service-module integrated-service-engine <i>slot/0</i> password-reset Example: Router# service-module integrated-service-engine 1/0 password-reset	Reloads the software on the NME-NAM-120S.

Troubleshooting Tips

If you have trouble opening a NAM console session from the router, ensure that the NAM console line is clear by entering the **service-module analysis-module *slot/0* session clear** command in privileged EXEC mode.

What to Do Next

Verify that the default root password of *root* is accepted by performing the steps described in the [“Closing a Session” section on page 11](#).

To change the NAM root password, see the [“Changing the NAM Root Password” section on page 40](#).

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 NME-NAM-120S is not properly configured for Telnet or SSH access (see the following [Prerequisites, page 43](#) section), then you can open a Telnet session to the router in which the NME-NAM-120S is installed, and then open a NAM console session from the router. See the [“Opening a Session” section on page 10](#).

Prerequisites

- Configure the NAM system IP address. Optionally, set the NAM system hostname. See the [“Configuring the NME-NAM-120S For Network Connectivity” section on page 32](#).
- 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. See [Step 5](#) of the [“Configuring the NME-NAM-120S For Network Connectivity” section on page 32](#).

SSH Prerequisites

- Install the NAM software K9 cryptographic patch, which you can download from Cisco.com.
- Enter the **exsession on ssh** NAM CLI command. See [Step 5](#) of the [“Configuring the NME-NAM-120S For Network Connectivity” section on page 32](#).

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	<p>telnet {ip-address hostname} or ssh {ip-address hostname}</p> <p>Example: Router# telnet 10.20.30.40</p> <p>Example: Router# ssh 10.20.30.40</p>	<p>Logs in to a host that supports Telnet.</p> <p>or</p> <p>Starts an encrypted session with a remote networking device.</p> <ul style="list-style-type: none"> Use the NAM system IP address or NAM system hostname.
Step 2	<p>At the login prompt, enter root.</p> <p>Example: login: root</p>	Accesses the root (read/write) level of NAM.
Step 3	<p>At the password prompt, enter your password.</p> <p>or</p> <p>If you have not changed the password from the factory-set default, enter root as the root password.</p> <p>Example: Password: root</p>	—
Step 4	<p>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.</p>	For help using NAM CLI commands, see the “Configuring the NME-NAM-120S for Management” section on page 20.
Step 5	<p>exit</p> <p>Example: root@localhost(sub-custom-filter-capture)# exit root@localhost#</p>	<p>Leaves a subcommand mode.</p> <ul style="list-style-type: none"> Return to command mode.
Step 6	<p>logout</p> <p>Example: root@localhost# logout</p> <p>Connection closed by foreign host.</p>	Logs out of the NAM system.

Examples

This section provides the following examples:

- [Opening and Closing a Telnet Session to the NAM Using the NAM System IP Address, page 45](#)

- [Opening and Closing an SSH Session to the NAM Using the NAM System Hostname, page 45](#)

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

```
Router> telnet 172.20.105.215
Trying 172.20.105.215 ... Open

Cisco Network Analysis Module (NME-NAM-120S)

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

Cisco Network Analysis Module (NME-NAM-120S) Console, 5.1
Copyright (c) 1999-2010 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]
Router>
```

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

```
host [/home/user] ssh -l root nmnam2
root@nmnam2's password: <password>
Terminal type: vt100

Cisco Network Analysis Module (NME-NAM-120S) Console, 5.1
Copyright (c) 1999-2010 by Cisco Systems, Inc.

WARNING! Default password has not been changed!
root@nmnam2.company.com#
root@nmnam2.company.com# logout

Connection to nmnam2 closed.
host [/home/user]
```

Managing the NME-NAM-120S

This section contains the following information:

- [Shutting Down and Starting Up NME-NAM-120S, page 46](#)
- [Verifying System Status, page 47](#)
- [Configuring Logging Options and Generating Diagnostics, page 48](#)



Note

- The tables in these sections show only common router and network module commands.
 - To view a complete list of available commands, type `?` at the prompt (Example: Router(config-if)# `?`).
 - To view a complete list of command keyword options, type `?` at the end of the command (Example: Router# `service-module integrated-service-engine ?`).
- 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 NME-NAM-120S

To shut down or start up the network module or the NME-NAM-120S application that runs on the module, use commands as needed from the following list of common router and network module commands (Table 2).



Note

- Some shutdown commands can potentially disrupt service. If command output for such a command displays a confirmation prompt, confirm by pressing **Enter** or cancel by entering **n** and pressing **Enter**. Alternatively, prevent the prompt from displaying by using the **no-confirm** keyword.
- Some commands shut the module or application down and then immediately restart it.

Table 2 Common Shutdown and Startup Commands


Configuration Mode	Command	Purpose
Router#	service-module integrated-service-engine slot/0 reload	Shuts down the network module operating system gracefully, then restarts it from the bootloader.
Router#	service-module integrated-service-engines slot/0 reset	Resets the hardware on a module. Use only to recover from shutdown or a failed state.  Caution Use this command with caution. It does <i>not</i> provide an orderly software shutdown and consequently might impact file operations that are in progress.
Router#	service-module integrated-service-engine slot/0 session	Accesses the specified service engine and begins a network module configuration session.
Router#	service-module integrated-service-engines slot/0 shutdown	Shuts down the network module operating system gracefully. Use when removing or replacing a hot-swappable module during online insertion and removal (OIR).
Router#	service-module integrated-service-engine slot/0 status	Displays configuration and status information for the network module hardware and software.
Router (config)#	shutdown	Shuts down the entire system (host router plus network module) gracefully.
ServiceEngine bootloader>	boot	Starts the helper or application.
ServiceEngine bootloader>	reboot	Shuts down NME-NAM-120S without first saving configuration changes, then reboots it from the bootloader.

Table 2 Common Shutdown and Startup Commands (continued)

Configuration Mode	Command	Purpose
root@hostname .domain	reboot	Gracefully reboots NME-NAM-120S from the NAM CLI.
root@hostname .domain	shutdown	Shuts down the NME-NAM-120S application gracefully, then shuts down the module.

Verifying System Status

To verify the status of an installation, upgrade, or downgrade or to troubleshoot problems, use commands as needed from the following list of common router and network module commands (Table 3).



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 3 Common Verification and Troubleshooting Commands

Configuration Mode	Command	Purpose
Router#	ping	Pings a specified IP address to check network connectivity (does not accept a hostname as destination).
Router#	show arp	Displays the current Address Resolution Protocol (ARP) table.
Router#	show clock	Displays the current date and time.
Router#	show configuration	Displays the current bootloader configuration as entered by means of the configure command.
Router#	show controllers service-engine	Displays interface debug information.
Router#	show diag	Displays standard Cisco IOS diagnostics information, including information about NME-NAM-120S.
Router#	show hardware	Displays information about network module and host-router hardware.
Router#	show hosts	Displays the default domain name, style of name lookup, list of name-server hosts, and cached list of hostnames and addresses
Router#	show interfaces	Displays information about all hardware interfaces, including network and disk.
Router#	show interfaces service-engine	Displays information about the module side of the router-module interface.

Table 3 Common Verification and Troubleshooting Commands (continued)

Configuration Mode	Command	Purpose
Router#	show ntp status	Displays information about Network Time Protocol (NTP).
Router#	show processes	Displays a list of the running application processes.
Router#	show running-config	Displays the configuration commands that are in effect.
Router#	show startup-config	Displays the startup configuration.
Router#	show tech-support	Displays general information about the host router that is useful to Cisco technical support for problem diagnosis.
Router#	show version	Displays information about the loaded router, software or network module bootloader version, and also hardware and device information.
Router#	test scp ping	Pings the network module to check network connectivity.
Router#	verify	Displays version information for installed hardware and software.
SE-Module>	ping	Pings a specified IP address to check network connectivity (does not accept a hostname as destination).

Configuring Logging Options and Generating Diagnostics

To configure logging options for NME-NAM-120S, use commands as needed from the list of common network module commands shown in [Table 4](#) and [Table 5](#).


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 Common Syslog Commands

Configuration Mode	Command	Purpose
Router#	show log	Displays the contents of the specified log.
	show logs	Displays a list of available log files.
	copy log	Saves the syslog to a destination of your choice.

Table 5 Common Trace Commands

Command	Purpose
clear trace	Clears logged trace events for specified modules.
log trace	Logs configured traces to the network module (can be done locally or remotely).
no trace	Disables tracing for specified modules, entities, or activities.
show errors	Displays error statistics by module, entity, or activity.
show trace	Displays trace settings.
show trace buffer	Displays the contents of the trace buffer.
show trace store	Displays the contents of the traced messages that are stored.
trace	Enables tracing (that is, generates error reports) for specified modules, entities, or activities.

Additional References

The following sections provide references related to the NME-NAM-120S features.

Table 6 Related Documentation

Related Topic	Document Title
Links to software downloads, product documentation, and technical documentation	<i>Cisco Network Analysis Module (NAM) Software</i> at http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html
Network modules	<i>Installing Cisco Network Modules in Cisco Access Routers</i> at http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/InstNetM.html
Installing and cabling network modules	<i>Connecting Cisco NAM Enhanced Network Modules to the Network</i> at http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/namme.pdf
Advanced Integration Modules (AIMs)	<i>Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers</i> at http://www.cisco.com/en/US/docs/routers/access/2600/hardware/module/installation/guide/aims_ins.html
Installing Cisco Integrated Services Routers Generation Two.	<i>Cisco 2900 and 3900 Series Hardware Installation</i> at http://www.cisco.com/en/US/partner/docs/routers/access/2900/hardware/installation/guide/Install_Connect.html
Safety and compliance	<i>Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information</i> at http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html

Related Topic	Document Title
Accessing the ROM monitor and issuing commands.	<i>ROM Monitor Download Procedures for Cisco 2691, Cisco, 3631, Cisco 3725, and Cisco 3745 Routers</i> at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/sw_conf/piperrom.htm
Cisco IOS interface commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Interface and Hardware Component Command Reference</i> at http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.html
Configure a switch port analyzer (SPAN) session on Cisco series routers.	<i>16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series</i> at http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ft1636nm.html <i>Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards</i> at http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html
IP unnumbered interfaces	<i>Understanding and Configuring the ip unnumbered Command</i> at http://www.cisco.com/application/pdf/paws/13786/20.pdf
Authentication, authorization, and accounting (AAA)	<i>Cisco IOS Security Configuration Guide</i> at http://www.cisco.com/en/US/products/ps6441/products_installation_and_configuration_guides_list.html
Cisco IOS software	<i>Cisco IOS Software Releases 12.4 T</i> at http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.html

MIBs

Description	Source
MIB-II: All groups except Exterior Gateway Protocol (EGP) and transmission	RFC 1213
RMON-MIB: Alarm and Event groups only	RFC 2819
RMON2: trapDestTable only	RFC 2021
CDP-MIB: Cisco Discovery Protocol	
EntityMIB	RFC 2737

RFCs

RFCs	Title
RFC 768	User Datagram Protocol
RFC 793	Transmission Control Protocol
RFC 826	<i>Ethernet Address Resolution Protocol</i>

RFCs	Title
RFC 959	<i>File Transfer Protocol</i>
RFC 1165	Network Time Protocol
RFC 1213	<i>Remote Network Monitoring Management Information Base Version 2 using SMIPv2</i>
RFC 1350	The TFTP Protocol
RFC 2074	<i>Remote Network Monitoring MIB Protocol Identifiers</i>
RFC 2613	<i>Remote Network Monitoring MIB Extensions for Switch Networks Version 1.0</i>
RFC 2896	<i>Remote Network Monitoring Management Information Base</i>
RFC 3164	The BSD Syslog Protocol
RFC 3273	<i>Remote Network Monitoring Management Information Base for High Capacity Networks</i>
RFC 3287	<i>Remote Monitoring MIB Extensions for Differentiated Services</i>

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Network Analysis Module

For information on a feature in this technology that is not documented here, see the product documentation at the following URL:

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

For release information about a specific command, see the command reference documentation. Not all commands might be available in your Cisco IOS software release.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport
Cisco Feature Navigator website	http://www.cisco.com/go/cfn Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. An account on Cisco.com is not required.
Cisco Software Center website	http://www.cisco.com/cisco/web/download/index.html

Glossary

AAA	Authentication, authorization, and accounting, pronounced <i>triple A</i> .
access list	A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
AIM	Asynchronous interface module. Type of network module.
appliance	Alternate term for network module.
ARP	Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address.
blade	Alternate term for network module.
boothelper	See <i>helper</i> .
bootloader	A small set of system software that runs when the system first powers up. It loads the operating system (from the disk, network, external flash, or external USB flash), which loads and runs the NME-NAM-120S application. The bootloader might optionally load and run the boothelper.
CEF	Cisco Express Forwarding
Flooding	Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.
FTP	File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.

GRE	Generic routing encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.
GUI	Graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.
helper (previously known as boothelper)	A small subset of the system software that runs on the module. It boots the module from the network and assists in software installation and upgrades, disaster recovery, and other operations when the module cannot access its software.
IP Multicast	Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address.
MIB	Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as <i>Network Address Translator</i> .
NetFlow	A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.
network module	Type of network module.
NTP	Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
PCI	Peripheral Component Interconnect. An industry local bus standard.
QoS	Quality of Service. Cisco IOS QoS technology lets complex networks control and predictably service a variety of networked applications and traffic types.
Service engine	Content-networking product (hardware plus software) that accelerates content delivery, ensuring maximum scalability and availability of content.

Service (or services) engine	Alternate term for network module with installed application software.
service module	Standalone content engine with its own startup and run-time configurations that are independent of the Cisco IOS configuration on the router.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. SNMPv2c supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.
SSH	Secure Shell Connection protocol is a protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.
syslog	Industry-standard protocol for capturing log information for devices on a network.
TCP	Transmission Control Protocol. Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
telnet	Network protocol used to make unsecure internet connections to the application server.
UDP	User Datagram Protocol. Connectionless transport-layer protocol in the TCP/IP protocol stack that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the digital signal processor (DSP) segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

**Note**

For terms not included in this glossary, see a reference like the *Cisco IOS Voice Configuration Library Glossary* at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/VCLgloss.html

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2011 Cisco Systems, Inc. All rights reserved.

