Getting Started

This chapter describes how to configure the Catalyst 6500 series switch, Catalyst 6000 series switch, or Cisco 7600 series router NAM and includes these sections:

Configuring the NAM

How you configure the NAM on your switch depends on whether you are using Cisco IOS software or the Catalyst operating system software. Several NAM configuration tasks are common to both switch operating systems.

For initial configuration of the NAM. refer to the *Quick Start Guide for the Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module*.

After you set up the NAM initial configuration, you can configure VLAN access control lists (VACLs), either local or remote NetFlow Data Export (NDE), and the switched port analyzer (SPAN) to monitor network traffic. For more information, see the "Configuring Traffic Sources for Capturing NAM Traffic" section on page 3-1.

When you complete configuring the software-dependent attributes for the NAM, you can configure the software-independent attributes. For more information, see the "Operating-System-Independent Configuration" section on page 3-12.

Configuring Traffic Sources for Capturing NAM Traffic

The WS-SVC-NAM-1 platform provides a single destination port for SPAN sessions.

The WS-SVC-NAM-2 platform provides two possible destination ports for VACL and SPAN sessions. The destination ports for use by the SPAN GUI are named data port 1 and data port 2 by default. For the CLI SPAN port names, refer to Table 1-2 on page 1-4.

VACL and SPAN cannot be applied to the same port simultaneously. Table 3-1 shows the SPAN and VACL port configurations that are supported on the NAM.

Table 3-1 NAM SPAN and VACL Port Configurations

NAM-1	NAM-2
One SPAN session only	Two SPAN sessions
One VACL session only	One SPAN session and one VACL session
	Two VACL sessions

For more information about SPAN, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/span.htm

For more information about VACLs, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_82/confg_gd/acc_list.htm#1053650

For more information about NDE, see these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1035105
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/nde.htm

These sections describe how to configure VACLs, either local or remote NDE, and SPAN to monitor network traffic with the NAM:

- Cisco IOS Software, page 3-2
- Catalyst Operating System Software, page 3-8

Cisco IOS Software

You can capture traffic for NAM monitoring from a single VLAN or from multiple VLANs. If you want to monitor traffic from specific VLANs only, you need to clear the VLANs that you do not want to monitor from the capture feature.

Using SPAN as a Traffic Source

You can configure SPAN as a traffic source using both the CLI and the NAM Traffic Analyzer application.

The NAM can analyze Ethernet traffic from Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN source ports. You can also specify an Ethernet VLAN as the SPAN source.

For more information on SPAN, refer to the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm

You cannot use ports on the NAM module as SPAN source ports.

To enable SPAN on the NAM, perform one of these tasks:

Command	Purpose
`Router (config)# monitor session {session_number} {source {interface type slot/port} | {vlan vlan_ID}} [, | - | rx | tx | both]`	Sets the source interfaces and VLANs for the monitor session.
`Router (config)# monitor session {session_number} {destination analysis module NAM module number data-port port}`	Enables port 1 of the NAM as a SPAN destination.
`Router (config)# no monitor session session_number`	Disables the monitor session.
`Router (config)# monitor session {session_number} {filter {vlan_ID} [, | - ]}`	Filters the SPAN session so that only certain VLANs are seen from switch port trunks.
`Router # show monitor session {session_number}`	Shows current monitor sessions.

This example shows how to enable SPAN on the NAM:

```
Router# show monitor
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports:None
Filter VLANs:      None

Session 2
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Destination Ports:None
Filter VLANs:      None

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# monitor session 1 source vlan 1 both
```

Note If you are using the switch CLI to configure SPAN as a traffic source to NAM-1, the SPAN destination port for NAM-1 is data-port 1. The SPAN destination ports for NAM-2 are data-port 1 and data-port 2.

```
Router#
00:21:10:%SYS-5-CONFIG_I:Configured from console by console
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# monitor session 1 destination analysis-module 8 data-port 1
Router# show monitor
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          1
Source RSPAN VLAN:None
Destination Ports:analysis-module 8 data-port 1

Filter VLANs:     None
Dest RSPAN VLAN:  None
Session 2
---------
 Type       :Local Session
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:         None
Source RSPAN VLAN:None
Destination Ports:None
Filter VLANs:     None
Dest RSPAN VLAN:  None
```

Using a VACL as a Traffic Source

This section describes how to configure a VACL for a switch running Cisco IOS Release 12.1(13)E1 or later releases. To configure a LAN VACL on the Catalyst operating system, you can use the security ACL feature to achieve the same result. For more information, see the "Operating-System-Independent Configuration" procedure on page 3-12.

Configuring a VACL on a WAN Interface

Because WAN interfaces do not support SPAN if you want to monitor traffic on a WAN interface using a NAM, you need to manually configure a VACL on the switch using the switch CLI. This feature only works for IP traffic over the WAN interface. You can apply additional filtering rules to target specific data flows.

In addition, you can use a VACL if there are no available SPAN sessions to direct traffic to the NAM. In this scenario, you can set up a VACL instead of SPAN for monitoring VLAN traffic.

The following examples describe the steps to configure a VACL for a switch running Cisco IOS Release 12.1(13)E1 or higher. To configure a LAN VACL on a switch running the Catalyst operating system, use the ACL feature to achieve the same result.

This example shows how to configure a VACL on an ATM WAN interface and forward both ingress and egress traffic to the NAM:

```
Cat6500# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface ATM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

When monitoring only egress traffic, you can obtain the VLAN ID that is associated with the WAN interface command as follows:

```
Cat6509# show cwan vlan
Hidden VLAN  swidb->if_number   Interface
-----------------------------------------------
1017          94               ATM6/0/0.1
```

After the VLAN ID is obtained, configure the NAM data port capture as follows:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017
```

For monitoring ingress traffic, you should replace VLAN 1017 in the previous capture configuration with the VLAN ID that carries the ingress traffic. For example, this configuration allows the NAM to monitor only ingress traffic on a WAN interface:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
```

Configuring a VACL on a LAN VLAN Interface

To monitor VLAN traffic on the LAN, you can forward the traffic to the NAM by using SPAN. However, in some rare circumstances, if the spanned traffic exceeds the NAM's monitoring capability, you can prefilter the LAN traffic before it is forwarded to the NAM.

This example shows how to configure a VACL for the LAN VLAN interfaces. In this example, all traffic that is directed to the server 172.20.122.226 on VLAN 1 is captured and forwarded to the NAM that is located in slot 3:

```
Cat6500# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cat6500(config)# access-list 100 permit ip any any
Cat6500(config)# access-list 110 permit ip any host 172.20.122.226
Cat6500(config)# vlan access-map lan 100
Cat6500(config-access-map)# match ip address 110
Cat6500(config-access-map)# action forward capture
Cat6500(config-access-map)# exit
Cat6500(config)# vlan access-map lan 200
Cat6500(config-access-map)# match ip address 100
Cat6500(config-access-map)# action forward
Cat6500(config-access-map)# exit
Cat6500(config)# vlan filter lan vlan-list 1
Cat6500(config)# analysis module 3 data-port 1 capture allowed-vlan 1
Cat6500(config)# analysis module 3 data-port 1 capture
Cat6500(config)# exit
```

Using NetFlow Data Export as a Traffic Source

NDE makes traffic statistics available for analysis by an external data collector. You can use NDE to monitor all Layer 3-switched and all routed IP unicast traffic. To use NDE as a traffic source for the NAM, enable the NetFlow Monitor option to allow the NAM to receive the NDE stream. The statistics are presented on reserved ifIndex.3000.

Configuring NDE for a NetFlow device so that it exports NDE packets to the NAM is platform specific and version specific to the sending device. Refer to the device NDE configuration guidelines for more information.

NDE Configuration

To configure NDE for the Cisco IOS software for both local and remote NDE devices, follow these steps:

Step 1 Configure NDE as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface type slot/port
```

Step 2 Enable NetFlow for the interface.

```
Router(config)# ip route-cache flow
```

Step 3 Export the routed flow cache entries to the NAM UDP port 3000.

```
Router(config)# ip flow-export destination NAM-address 3000
```

Note The UDP port number must be set at 3000.

When you configure a NAM module as an NDE collector, you should use the IP address of the NAM (set up by sessioning into the NAM module).

This example shows how to set up a basic NDE configuration:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan 2
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router(config)# exit
```

NDE Configuration from MLS Cache

To configure NDE from the PFC (multilayer switching cache), follow these steps:

Step 1 Enter configuration mode.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2 Select the version of NDE.

```
Router(config)# mls nde sender version version-number
```

Note NAM supports NDE version 1, 5, 6, 7, 8, and version 8 aggregation caches. Refer to the Cisco IOS documentation for NDE versions that are supported by the switch software to determine which NDE versions are available to the NAM.

Step 3 Select the NDE flow mask.

```
Router(config)# mls flow ip [interface-full | full]
```

Note Use the full keyword to include additional details of the collection data in the flow mask.

Step 4 Enable NetFlow export.

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

Step 5 Export NetFlow packets to the NAM UDP port 3000.

```
Router(config)# ip flow-export destination NAM-Address 3000
```

This example shows how to set up an NDE configuration from the Multilayer Switch Feature Card (MSFC):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls nde sender version 5
Router(config)# mls flow ip full
Router(config)# mls nde sender
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router# show ip cache flow
Router# show ip flow export
```

Note For more information on configuring NDE on the Policy Feature Card (PFC), see this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/nde.htm - xtocid14

NDE Configuration for Version 8 Aggregation

Note Although the NAM supports NDE aggregation, the information that you receive for a specified aggregation type is limited to that aggregation, and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode.

If the NetFlow device supports NDE version 8 aggregations, flows from one or more of the version 8 aggregation caches may be exported to the NAM. To export flows from the aggregation caches, perform these steps:

Step 1 Select an NDE version 8 aggregation.

```
Router(config)# ip flow-aggregation cache aggregation-type
```

The supported aggregation types are as follows:

- Destination-prefix
- Source-prefix
- Protocol-port
- Prefix

Step 2 Enable the aggregation cache.

```
Router(config-flow-cache)# enable
```

Step 3 Export the flow entries in the aggregation cache to NAM UDP port 3000.

```
Router(config-flow-cache)# export destination NAM-Address 3000
```

Step 4 Verify NDE.

```
Router# show ip cache flow-aggregation aggregation-type
```

This example shows how to set up an NDE version 8 aggregation configuration:

```
Router(config)# ip flow-aggregation cache prefix
Router(config-flow-cache)# enable
Router(config-flow-cache)# export destination 172.20.104.74 3000
Router(config-flow-cache)# exit
Router(config)# show ip cache flow-aggregation prefix
```

Catalyst Operating System Software

You can capture traffic for NAM monitoring from a single VLAN or from multiple VLANs. If you want to monitor traffic from specific VLANs only, you need to clear the VLANs that you do not want to monitor from the capture feature.

Using SPAN as a Traffic Source

You can configure Remote SPAN (SPAN) as a traffic source using both the NAM Traffic Analyzer application and the switch CLI. We recommend that you use NAM Traffic Analyzer.

For more information about SPAN and RSPAN, refer to the “Configuring SPAN and RSPAN” chapter in the *Catalyst 6500 Series Switch Software Configuration Guide*.

You can use RSPAN traffic as a SPAN source for the NAM. Verify that the SPAN source is set to the same VLAN ID that is used for RSPAN. The SPAN destination should be set to *nam_module/port*.

Note If you are using the switch CLI to configure SPAN as a traffic source to NAM-1, set the destination port to 3. If you are configuring SPAN as a traffic source to NAM-2, set the SPAN port to destination port 7. Destination port 8 is not available in this NAM release although switch and hardware support is available.

Note You cannot use NAM ports as SPAN source ports.

The NAM can analyze Ethernet traffic from Ethernet, Fast Ethernet, Gigabit Ethernet, trunk ports, or Fast EtherChannel SPAN source ports. You also can specify an Ethernet VLAN as the SPAN source.

For more information on configuring SPAN and RSPAN, refer to the switch software configuration guide.

To set the NAM as a SPAN destination port, perform this task in privileged mode:

Task	Command
Set the NAM as a SPAN destination port.	**set span** {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod* | *dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]

This example shows how to set SPAN VLAN 1 to a NAM-2 that is located in slot 5:

```
Console> (enable) set span 1 5/7
```

Using a LAN VACL as a Traffic Source

Unlike WAN VACLs, which can be used to capture inbound or outbound VLAN packets, Catalyst operating system VACLs can only be used to capture VLAN packets as they are initially routed or bridged into the VLAN on the switch.

This example shows how to create a VACL that captures all the IP packets that are bridged or routed into VLAN 1 on the switch to the NAM-1 data port 6/3:

```
Console> (enable) set security acl ip LANCAPTURE permit ip any any capture
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

This example shows how to create a VACL that captures a specific VLAN 1 conversation:

```
Console> (enable) set sec acl ip LANCAPTURE permit ip host 172.20.122.70 host
172.20.122.226 capture
Console> (enable) set security acl ip LANCAPTURE permit ip any any
Console> (enable) commit
Console> (enable) set security acl map LANCAPTURE 1
Console> (enable) set security acl capture 6/3
```

Using NetFlow Data Export as a Traffic Source

To use NetFlow Data Export (NDE) as a traffic source for the NAM, you must enable the NetFlow Monitor option to allow the NAM to receive the NDE stream. For a local switch, the statistics are presented on reserved ifIndex.3000 as in previous NAM releases. The remote switch uses ifIndex.50000 and greater.

Note You need to configure the Multilayer Switch Function Card (MSFC) to use NetFlow. For more information, refer to the *Catalyst 6500 Series Switch Software Configuration Guide*.

Note There are no CLI commands for creating NetFlow custom data sources. To create a NetFlow custom data source, you must use the NAM Traffic Analyzer GUI.

NDE Configuration

To enable the NetFlow Monitor for the Catalyst operating system, perform this task:

	Task	Command
Step 1	Select the NDE version. **Note** The NAM supports NDE versions 1, 5, 6, 7, 8, and version 8 aggregation caches. Refer to the Cisco IOS documentation for NDE versions supported by the switch software to determine which NDE versions are available to the NAM.	**set mls nde version** *nde-version-number*
Step 2	Set the NDE flow mask to full. **Note** Although the NAM supports NDE aggregation, the information you receive for a specified aggregation type is limited to that aggregation and other NDE details are not available. To receive more information about your NDE configuration, use the full flow mode.	**set mls flow full**
Step 3	Direct NDE packets to the NAM.	**set snmp extendedrmon netflow** [**enable** | **disable**] *mod* **set mls nde** *NAM-address* **3000**
Step 4	Enable NDE export.	**set mls nde enable**

	Task	Command
Step 5	(Optional) Make sure that the device exports if-index. **Note** Use this step if you want to break out NetFlow data by interface and direction at the NAM.	**set mls nde destination-ifindex enable** **set mls nde source-ifindex enable**
Step 6	Verify NDE export. On the local device: On the remote device:	 **show snmp and show mls nde** **show mls nde**

This example shows how to enable the NetFlow Monitor option and verify that it is enabled:

```
Console> (enable) set snmp extendedrmon netflow enable 2
Snmp extended RMON netflow enabled
Console> (enable) show snmp
RMON: Enabled
Extended RMON NetFlow Enabled : Module 2
Traps Enabled:
None
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                            Trap-Rec-Community
------------------------------------------  --------------------
<...output truncated...>
```

Note If a NAM is installed, you do not need to specify an external data collector with the **set mls nde** *collector_ip* [*udp_port_number*] command as described in the *Catalyst 6500 Series Software Configuration Guide*. Ignore any messages that indicate that the host and port are not set.

Exporting NDE From Bridged Flow Statistics

If the switch supports exporting NDE from bridged-flow statistics, you can use bridged-flow statistics to export NDE to the NAM.

To configure bridged-flow statistics export for NDE, perform this task:

	Task	Command
Step 1	Enable bridged-flow statistics on the VLANs.	**set mls bridged-flow-statistics enable** *vlan-list*
Step 2	Export NDE packets to UDP port 3000 of the NAM.	**set mls nde** *NAM-address* **3000**

Operating-System-Independent Configuration

These sections describe the NAM configurations that are not dependent on the switch operating system.

Configuring Automatic RMON Collections

RMON collections can be configured explicitly through SNMP by a management station on some data sources. Collections that are explicitly configured through SNMP take precedence over autostart collections, so if both collections are configured, only the explicitly configured collections are started on each data source when the NAM initializes.

You can specify that some collections are automatically configured on every available data source (including all known VLANs) whenever the NAM is initialized by using the **autostart** command.

Note We recommend that you explicitly configure those collections that you require instead of using autostart to reduce the possibility of performance degradation due to many collections being started for each data source.

Note When you enter the **autostart** command, you must reboot the NAM for that command to take effect.

The following collection types can be started automatically:

- addressMap—addressMapTable from RMON2-MIB (RFC 2021)

  If the NMS never sets the addressMapMaxDesiredEntries scalar, then the NAM uses the value -1 (for no limit).
- art—artControlTable from draft-warth-rmon2-artmib-01.txt
- etherStat—etherStatsTable from RMON-MIB (RFC 1757)
- prioStats—smonPrioStatsControlTable from SMON-MIB (RFC 2613)
- vlanStats—smonVlanStatsControlTable from SMON-MIB (RFC 2613)

For example, each dataSource (interface or VLAN) is configured with an etherStatsEntry (from RMON-1) after you enter the **autostart etherstats enable** command and reboot the NAM. The etherStatsOwner field is set to the *monitor* value.

The automatic start process occurs after you set up any collections that were explicitly created through SNMP by a management station and stored in the NVRAM in the NAM. Automatic start collections are not configured on data sources that already have a collection of that type configured through SNMP.

To enable collections for the automatic start process, do the following:

- Enable the etherStat collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart etherstat enable
  ```
- Enable the addressMap collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart addressmap enable
  ```
- Enable the prioStats collection type by entering this command from the root account of the NAM:

  ```
  root@localhost# autostart priostats enable
  ```

- Enable the vlanStats collection type by entering this command from the root account of the NAM:

```
root@localhost# autostart vlanstats enable
```

- Disable the vlanStats collection type by entering this command from the root account of the NAM:

```
root@localhost# autostart vlanstats disable
```

After enabling or disabling one or more collection types, you must reboot the NAM before the configuration takes effect.

Configuring the HTTP or HTTP Secure Server

Before you can access the NAM through a web browser (HTTP or HTTPS), you must enable the NAM Traffic Analyzer application from the NAM CLI. For HTTP, use the **ip http server enable** command. For HTTPS, use the **ip http secure server enable** command. You also can optionally configure the HTTP (or HTTPS) servers to run on a different TCP port from the default.

Note You can use the HTTP server or the HTTP secure server, but not both.

Note The **ip http** secure commands are all disabled by default, and you must first download and install the NAM strong crypto patch from http://www.Cisco.com before you can enable them.

Configuring the HTTP Server

To configure the HTTP server parameters for the NAM, follow these steps:

Step 1 (Optional) Configure the HTTP port as follows:

```
root@localhost# ip http port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

The port number range is from 1 to 65535.

Note Web users are different from the CLI users. Usernames and passwords for web users and CLI users are administered separately. For changing the usernames and passwords on the NAM CLI, see the "Cisco IOS Software" section on page 4-1 and the "Catalyst Operating System Software" section on page 4-11. To change usernames and passwords through the web interface, refer to the NAM Traffic Analyzer application online help and the *User Guide for the Network Analysis Module NAM Traffic Analyzer Release 3.3.*

Step 2 Enable the HTTP server as follows:

```
root@localhost# ip http server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]:admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

Configuring the HTTP Secure Server

The **ip http secure** commands are all disabled by default, and you must enable the HTTP secure server by installing a strong crypto patch. If you prefer to use SSH instead of Telnet, you also must install a strong crypto patch.

To install a strong crypto patch, follow these steps:

Step 1 Download the patch from http://www.Cisco.com and publish the patch in an FTP server.

Step 2 Install the patch as follows:

```
root@localhost# patch ftp-url
```

where **ftp-url** is the FTP location and the name of the strong crypto patch.

This example shows how to install a patch:

```
root@localhost# patch ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin

Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.

Downloading c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
ftp://host/path/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin (1K)
-                         [########################]       1K |  228.92K/s
1891 bytes transferred in 0.01 sec (225.40k/sec)

Verifying c6nam- 3.3-strong-cryptoK9-patch-1-0.bin. Please wait...
Patch c6nam- 3.3-strong-cryptoK9-patch-1-0.bin verified.

Applying /usr/local/nam/patch/workdir/c6nam- 3.3-strong-cryptoK9-patch-1-0.bin.
Please wait...
########################################### [100%]
########################################### [100%]

Patch applied successfully.
```

Step 3 (Optional) Configure the HTTPS server as follows:

Note If you specify a port other than the default (443), add :*port_number.*

```
root@localhost# ip http secure port 8080
The HTTP server is enabled now. You must restart the
server to change HTTP port. Continue [y/n]? y
```

The port number range is from 1 to 65535.

Note Web users are different from the CLI users.

Step 4 Enable the HTTPS server as follows:

```
root@localhost# ip http secure server enable
Enabling HTTP server...
No web users configured!
Please enter a web administrator username [admin]:admin
New password:
Confirm password
User admin added.
Successfully enabled HTTP server.
```

Generating Certificates

Certificates are used to validate the secure server connection. You can generate a self-signed certificate or obtain and install a certificate from a certification authority.

This example shows how to generate a self-signed certificate:

```
root@localhost# ip http secure generate self-signed-certificate

The HTTP secure server is enabled now. You must restart
to generate the certificate. Continue [y/n]? y
5243 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
..........++++++
.....++++++
e is 65537 (0x10001)
Using configuration from /usr/local/nam/defaults/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems, Inc.
Organizational Unit Name (eg, section) []:NAM
Common Name (eg, your name or your server's hostname) [r2d2-186.cisco.com]:
Email Address []:kjchen@cisco.com
Using configuration from /usr/local/nam/defaults/openssl.cnf
-----BEGIN CERTIFICATE-----
MIIDlTCCAv6gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBlDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28g
U3lzdGVtcywgSW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5j
aXNjby5jb20xHDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wHhcNMDQwMjI0
MDAwNDAxWhcNMDUwMjIzMDAwNDAxWjCBlDELMAkGA1UEBhMCVVMxCzAJBgNVBAgT
AkNBMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywg
SW5jLjEMMAoGA1UECxMDTkFNMRswGQYDVQQDExJyMmQyLTE4Ni5jaXNjby5jb20x
HDAaBgkqhkiG9w0BCQEWDW5hbUBjaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMDrGqhw2Kt8fimI+b11bk6+z9nTEQago1Qfoo8DehBLZ10eoJ/0
YAWlCqx3fnW3csSmGiHj6aEjJhm0WO5GvJRbzzbxeSPadDv7IdbIhXTLtPklW11g
```

```
byhUzvi5R8UFGSmerbbnc7qkTDXQdrQ2vETAfxK4oysq+HF55qVjY2KpAgMBAAGj
gfQwgfEwHQYDVR0OBBYEFEjcj4+vFJmLAo1NjnO9MYE/Hn9eMIHBBgNVHSMEgbkw
gbaAFEjcj4+vFJmLAo1NjnO9MYE/Hn9eoYGapIGXMIGUMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQKExNDaXNjbyBT
eXN0ZW1zLCBJbmMuMQwwCgYDVQQLEwNOQU0xGzAZBgNVBAMTEnIyZDItMTg2LmNp
c2NvLmNvbTEcMBoGCSqGSIb3DQEJARYNbmFtQGNpc2NvLmNvbYIBADAMBgNVHRME
BTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAHwBnz9OALHWkyK4qYTTbBno2MFbmI49
gU4IIpFSgWjoqdiXXGJs7c1q0dMPzdmDIG1TjmkLx2HC1+dVuq/2X4RrOFaoog/s
K9GmULi8OtgRkDhXJHT/gDfv+L7gQpQCCpq1TUFMVlzxzAHSsBGnlQ8oTysXScEJ
nSr0tR/OKB0t
-----END CERTIFICATE-----
Disabling HTTP secure server...
Successfully disabled HTTP secure server.
Enabling HTTP secure server...
Successfully enabled HTTP secure server.
root@localhost#
```

To obtain a certificate from a certification authority, you need to first generate a certificate-signing request and then submit the certificate-signing request manually to the certification authority. After obtaining the certificate from the certification authority, install the certificate.

Installing Certificates

To install a certificate from a certification authority, follow these steps:

Step 1 Generate a certificate signing request as follows:

```
root@localhost# ip http secure generate certificate-request
A certificate-signing request already exists. Generating a
new one will invalidate the existing one and any certificates
already generated from the existing request. Do you still
want to generate a new one? [y/n] y
5244 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.++++++
e is 65537 (0x10001)
Using configuration from /usr/local/nam/defaults/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Tamil Nadu
Locality Name (eg, city) []:Chennai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [hostname.Cisco.com]:
Email Address []:xxx@Cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAklOMRMwEQYDVQQIEwpUYW1pbCBOYWR1
MRAwDgYDVQQHEwdDaGVubmFpMRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMR4wHAYD
VQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20xIDAeBgkqhkiG9w0BCQEWEXNla2Fy
YmNAY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8+SR503gS
ygkf6pnHuh0LelNf6LqJjzwFfjqjS8vpkFq/QVbwqTNDIggUfbvRAIRWEKVWhpRf
rr+II2o/Xzb0RLpV2J2p3HGgoRrKC3nArIFFiSqXniEU+g2mPqsFNcOyxHNXIxEj
iBQf80DxbmvWFOpunmOQ/pGuEysNfU/46wIDAQABoAAwDQYJKoZIhvcNAQEEBQAD
```

```
gYEAVAX89pCAcRDOqPgaBEMQCmWD+wqZPnALovr7C81OLBYTgLLqdwPqoSjSYosE
w/pFnIxWN1sJ7MC8+hjnJJLjoCwbyrEyvoiAvzpsGsnAZgWUVaUpR7jlNbf8x2A1
hAOH9KchS0TpSNy13OyhuAkv0pUcM2AJqB/93u4YvuHfNOA=
-----END CERTIFICATE REQUEST-----
```

Step 2 Install a certificate obtained from a certification authority as follows:

```
root@localhost# ip http secure install certificate
The HTTP server is enabled now. You must restart the
server to install certificate. Continue [y/n]? y

Cut and paste the certificate you received from
Certificate Authority. Enter a period (.), then
press enter to indicate the end of the certificate.
-----BEGIN CERTIFICATE-----
MIIDAzCCAmygAwIBAgIBADANBgkqhkiG9w0BAQQFADBlMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wHhcNMDExMDMw
MTAxMDI4WhcNMDIxMDMwMTAxMDI4WjBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMK
U29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMR4w
HAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANsO1T5ayA6pvkJad413V+N/ibvND0XRyXfFycTQRzeA8F4A+etV
s0Iq0muFfiL9mDr/es9TkyfIM+T2F6+NE13DxJ53ZBbh7ndb6WOnzeHLKh9EDfSI
cy2s7751CPCjfLcMsWQLWSU7XUbi/ExDpb9e2wQQgi6QBED/YRkr73KNAgMBAAGj
gcIwgb8wHQYDVR0OBBYEFIHsyecd8AW4cvt7voCFeZMarXIqMIGPBgNVHSMEgYcw
gYSAFIHsyecd8AW4cvt7voCFeZMarXIqoWmkZzBlMQswCQYDVQQGEwJBVTETMBEG
A1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkg
THRkMR4wHAYDVQQDExVuYW1sYWItcGlrMy5jaXNjby5jb22CAQAwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQQFAAOBgQACDyWhULAUeSIXyt9tuUrdPfF97hrpFkKy
nj1yEU4piuc9qQtxG9yCGsofAm+CiGFg6P4qJZtBF47mq81qF+48JTYwi68CGCye
suZgw0iCPQVv4KDirHBKFc0Vr/2SMrXcJImczoV2WGcxWxsVaXwpkBKF8pcMFFYd
iOULMcvFxg==
-----END CERTIFICATE-----
.
Disabling HTTP server...
Successfully disabled HTTP server.
Enabling HTTP server...
Successfully enabled HTTP server.
```

Using a TACACS+ Server

TACACS+ is a Cisco Systems authentication protocol that provides remote access authentication and related services. With TACACS+, user passwords are administered in a central database instead of individual routers.

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

Before you can use the NAM with TACACS+, you must configure both the NAM and the TACACS+ server.

To configure the NAM for TACACS+, follow these steps:

Step 1 Start the NAM Traffic Analyzer application.

Step 2 Click the **Admin** tab.

Step 3 Choose **Users**.

Step 4 Choose **TACACS+**.

Step 5 Click the Enable TACACS+ Administration and Authentication box.

Step 6 Follow the instructions in the online help.