



CHAPTER 21

Configuring the NME IPS



Note

All IPS platforms allow ten concurrent CLI sessions.

This chapter describes how to configure the NME IPS and get it ready to receive IPS traffic. After that you are ready to configure intrusion prevention. This chapter contains the following sections:

- [NME IPS Configuration Sequence, page 21-1](#)
- [Verifying Installation and Finding the Serial Number, page 21-2](#)
- [Understanding the Hardware Interfaces, page 21-4](#)
- [Setting Up Interfaces on the NME IPS and the Router, page 21-4](#)
- [Establishing Sessions, page 21-8](#)
- [Opening and Closing a Session, page 21-9](#)
- [Displaying the Status of the NME IPS, page 21-10](#)
- [Enabling and Disabling Heartbeat Reset, page 21-11](#)
- [Rebooting, Resetting, and Shutting Down the NME IPS, page 21-12](#)
- [New and Modified Commands, page 21-13](#)

NME IPS Configuration Sequence

Perform the following tasks to configure the NME IPS:

1. Set up the interfaces.
2. Log in to the NME IPS.
3. Initialize the NME IPS.

Run the **setup** command to initialize the NME IPS.

4. Configure the NME IPS to capture traffic for intrusion prevention.
5. Create the service account.

**Caution**

You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

6. Perform the other initial tasks, such as adding users, trusted hosts, and so forth.
7. Configure intrusion prevention.
8. Perform administrative tasks to keep your NME IPS running smoothly.
9. Upgrade the IPS software with new signature updates and service packs.
10. Reimage the boot helper and bootloader when needed.

For More Information

- For the procedure for setting up interfaces, see [Setting Up Interfaces on the NME IPS and the Router, page 21-4](#).
- For the procedure for logging in to the NME IPS, see [Logging In to the NME IPS, page 2-8](#).
- For the procedure for running the **setup** command on the NME IPS, see [Advanced Setup for the NME IPS, page 3-24](#).
- For the procedure for creating the service account, see [Creating the Service Account, page 4-14](#).
- For the procedures for setting up the sensor, see [Chapter 4, “Setting Up the Sensor.”](#)
- For the procedures for configuring intrusion prevention, see [Chapter 9, “Configuring Anomaly Detection,” Chapter 7, “Configuring Event Action Rules,” Chapter 8, “Defining Signatures,” and Chapter 13, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the procedures to keep your sensor running smoothly, see [Chapter 16, “Administrative Tasks for the Sensor.”](#)
- For more information on obtaining Cisco IPS software, see [Chapter 22, “Obtaining Software.”](#)
- For the procedure for reimaging the NME IPS, see [Installing the NME IPS System Image, page 23-40](#).

Verifying Installation and Finding the Serial Number

Use the **show inventory** command in privileged EXEC mode to verify the installation of the NME IPS.

**Note**

You can also use this command to find the serial number of your NME IPS for use in troubleshooting with TAC. The serial number appears in the PID line, for example, SN: FHH1117001R.

To verify the installation of the NME IPS, follow these steps:

- Step 1** Log in to the router.
- Step 2** Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Verify that the NME IPS is part of the router inventory.

```
router# show inventory
NAME: "3845 chassis", DESCR: "3845 chassis"
PID: CISCO3845          , VID: V01 , SN: FTX1002C255

NAME: "c3845 Motherboard with Gigabit Ethernet on Slot 0", DESCR: "c3845 Motherboard with
Gigabit Ethernet"
PID: CISCO3845-MB      , VID: V03 , SN: FOC09514J4Y

NAME: "4 Port FE Switch on Slot 0 SubSlot 0", DESCR: "4 Port FE Switch"
PID: HWIC-4ESW        , VID: V01 , SN: FOC1102394U

NAME: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet on Slot 0 SubSlot
3", DESCR: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet"
PID: HWIC-1GE-SFP     , VID: V01 , SN: FOC10164DAR

NAME: "1000BASE-T SFP", DESCR: "1000BASE-T SFP"
PID: SP7041           , VID: C   , SN: 00000MTC101608RB

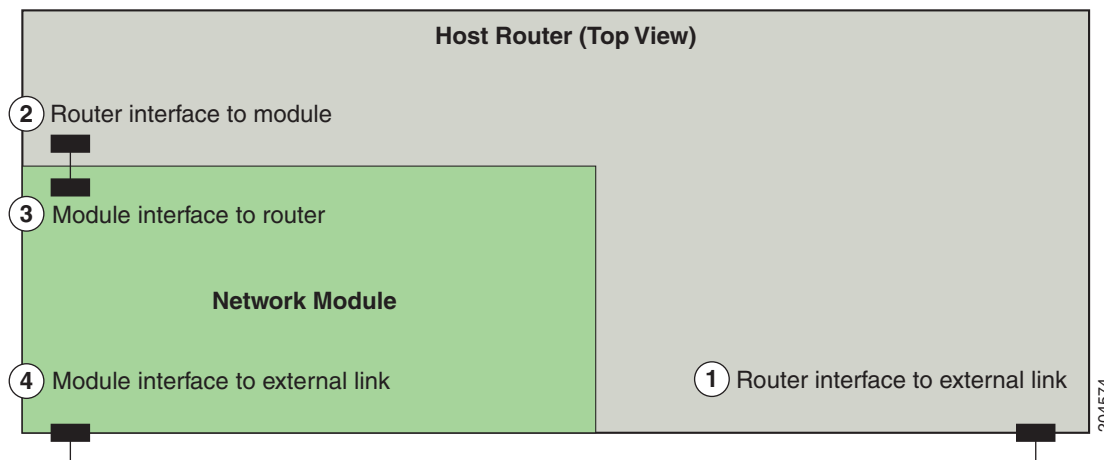
NAME: "Cisco Intrusion Prevention System NM on Slot 2", DESCR: "Cisco Intrusion
Prevention System NM"
PID: NME IPS-K9       , VID: V01 , SN: FHH1117001R

router#
```

Understanding the Hardware Interfaces

Figure 21-1 shows the router and the NME IPS interfaces used for internal and external communication. You can configure the router interfaces through the Cisco IOS CLI and the NME IPS interfaces through the IPS CLI, IDM, IME, or CSM.

Figure 21-1 NME IPS and Router Interfaces



| | |
|----------|---|
| 1 | Router interface to external link Configure the standard router settings using the Cisco IOS CLI. |
| 2 | Router interface to the NME IPS (ids-sensor x/0) Configure the IP address and default gateway router of the NME IPS using the Cisco IOS CLI. |
| 3 | The NME IPS interface to router (GigabitEthernet0/1) Configure the interface as inline or promiscuous using the Cisco IOS CLI. |
| 4 | The NME IPS interface to external link (Management0/1) Configure the command and control interface using the IPS CLI, IDM, IME, or CSM. |

Setting Up Interfaces on the NME IPS and the Router

This section describes how to set up interfaces on the NME IPS and the router, contains the following topics:

- [NME IPS Interface Configuration Sequence, page 21-5](#)
- [ARC and NAT, page 21-5](#)
- [Configuring the IDS-Sensor Interfaces on the Router, page 21-6](#)
- [Configuring Monitoring on the Router Interface, page 21-7](#)

NME IPS Interface Configuration Sequence

Follow this sequence to set up interfaces on the NME IPS and the router:

1. Configure the IPS command and control interface on the router, and the NME IPS IP address, mask, and gateway.
2. Enable the monitoring interface and specify whether it is promiscuous or inline, assign the ACL to the interface, specify how you want the router to handle traffic if the module fails, and create a monitoring ACL (optional).
3. Save the configuration.

For More Information

- For the procedure for configuring an unnumbered IP address on the IDS-Sensor interface, see [Configuring the IDS-Sensor Interfaces on the Router, page 21-6](#).
- For the procedure for enabling the monitoring interface, see [Configuring Monitoring on the Router Interface, page 21-7](#).

Advantages of NAT

NAT has the following advantages:

- You can use private IP addresses on your inside networks. Private IP addresses are not routable on the Internet.
- NAT hides the local IP addresses from other networks, so attackers cannot learn the real IP address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.

For More Information

For information on how ARC and NAT operate together, see [ARC and NAT, page 21-5](#).

ARC and NAT

If you use NAT to establish management access to the NME IPS, ARC on the NME IPS does not know the external IP address of the NME IPS. To make sure that management access to the NME IPS is not interrupted by devices that the NME IPS is managing, you must state the NAT address of the NME IPS every time you add a blocking device.

For More Information

- For more information on ARC, see [Chapter 13, “Configuring Attack Response Controller for Blocking and Rate Limiting.”](#)
- For the procedures for configuring the NME IPS NAT address every time you add a blocking device, see the following procedures:
 - [Configuring the Sensor to Manage Cisco Routers, page 13-23](#)
 - [Configuring the Sensor to Manage Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 13-26](#)
 - [Configuring the Sensor to Manage Cisco Firewalls, page 13-28](#)

Configuring the IDS-Sensor Interfaces on the Router

To configure the NME IPS interfaces, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

Step 4 Enable the CEF switching path.

```
router> configuration terminal
router(config)# ip cef
router(config)#
```

Step 5 Create a loopback interface.

```
router(config)# interface loopback 0
router(config-if)#
```

Step 6 Assign an IP address and netmask to the loopback interface.

```
router(config-if)# ip address 10.99.99.99 255.255.255.255
router(config-if)# exit
router(config)#
```



Note You must assign an IP address to the internal interface of the NME IPS to session in to the NME IPS. Choose a network that does not overlap with any networks assigned to the other interfaces in the router.

Step 7 Assign an unnumbered loopback interface to the IDS-Sensor interface. Use slot 1 for the following example:

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered Loopback 0
router(config-if)#
```

Step 8 Activate the port.

```
router(config-if)# no shutdown
router(config-if)#
```

Step 9 Exit configuration mode.

```
router(config-if)# end
```

Step 10 Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

You are now ready to initialize the NME IPS and configure intrusion prevention.

For More Information

- For more information on sessioning from the router to the NME IPS and exiting sessions, see [Establishing Sessions, page 21-8](#).
- For the procedure for using the **setup** command to initialize the NME IPS, see [Advanced Setup for the NME IPS, page 3-24](#).

Configuring Monitoring on the Router Interface

To configure the router interface to be monitored, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 (Optional) Configure a monitoring access list on the router.

```
router(config)# access-list 101 permit tcp any eq www any
```

You can set up a standard access list and apply it to filter what type of traffic you want to inspect. A matched ACL causes traffic not to be inspected for that ACL. This example bypasses inspection of HTTP traffic only. Refer to your Cisco IOS Command Reference for more information on the options for the **access-list** command.

Step 4 Enable monitoring on the interface in either inline or promiscuous mode and associate the access list.

```
router(config)# interface monitored_interface
router(config-if)# ids-service-module monitoring {inline | promiscuous} access-list 101
router(config-if)# exit
router(config)#
```



Note Associating the access list with the interface further controls what traffic is sent to the NME IPS.

Step 5 (For inline mode) Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

Step 6 (For inline mode) Specify how the router handles traffic inspection during a module failure.

```
router(config)# interface ids-sensor 1/0
router(config-if)# service-module {fail-close | fail-open}
router(config-if)#
```

The default is fail-open.

**Note**

The **fail-close** option means that if the NME IPS fails, then the router does not let traffic pass. The **fail-open** option means if the NME IPS fails, the router lets traffic pass, but it is not inspected by the IPS.

Step 7 Exit configuration mode.

```
router(config-if)# exit
router(config)# exit
router#
```

Step 8 Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

For More Information

- For more information on promiscuous mode, see [Promiscuous Mode, page 5-15](#).
- For more information on inline interface mode, see [Inline Interface Mode, page 5-17](#).

Establishing Sessions

Because the NME IPS does not have an external console port, console access to the NME IPS is enabled when you issue the **service-module ids-sensor slot/port session** command on the router, or when you initiate a Telnet connection into the router with the slot number corresponding to the NME IPS port number. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor slot/port session** command, you create a console session with the NME IPS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the IDS-Sensor interface. The IDS-Sensor interface is an interface between the NME IPS and the router. You must assign an IP address to the IDS-Sensor interface before invoking the **session** command. Assigning a routable IP address can make the IDS-Sensor interface itself vulnerable to attacks, because the NME IPS is visible on the network through that routable IP address, meaning you can communicate with the NME IPS outside the router. To counter this vulnerability, assign an unnumbered IP address to the IDS-Sensor interface. Then the NME IPS IP address is only used locally between the router and the NME IPS, and is isolated for the purposes of sessioning in to the NME IPS.

**Note**

Before you install your application software or reimage the module, opening a session brings up the bootloader. After you install the software, opening a session brings up the application.

**Caution**

If you session to the module and perform large console transfers, character traffic may be lost unless the host console interface speed is set to 115200/bps or higher. Use the **show running config** command to check that the speed is set to 115200/bps.

For More Information

For the procedure for configuring the IDS-Sensor interfaces, see [Configuring the IDS-Sensor Interfaces on the Router](#), page 21-6.

Opening and Closing a Session

**Note**

You must initialize the NME IPS (run the **setup** command) from the router. After networking is configured, SSH and Telnet are available.

Use the **service-module ids-sensor slot/port session** command to establish a session from the NME IPS to the module. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the NME IPS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, which is also the router prompt. You should only suspend a session to the router if you will be returning to the session after executing router commands. If you do not plan on returning to the NME IPS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the NME IPS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

**Note**

Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as **^^**, **Ctrl-^**, or ASCII value 30 (hex 1E).

**Caution**

If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Check the status of the NME IPS to make sure it is running.

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..
```

```
Cisco Systems Intrusion Prevention System Network Module
  Software version: 6.2(1)E3
  Model:           NME IPS
  Memory:         443508 KB
  Mgmt IP addr:   10.89.148.195
  Mgmt web ports: 443
  Mgmt TLS enabled: true
```

```
router#
```

Step 3 Open a session from the router to the NME IPS.

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

Step 4 Exit, or suspend and close the module session:

- sensor# **exit**



Note If you are in submodes of the IPS CLI, you must exit all submodes. Enter **exit** until the sensor login prompt appears.



Caution

Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to enter **exit** at the `router#` prompt to close the Cisco IOS session completely.

- To suspend and close the session to the NME IPS, press **Ctrl-Shift** and press **6**. Release all keys, and then press **x**.



Note When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 5 Disconnect from the router.

```
router# disconnect
```

Step 6 Press **Enter** to confirm the disconnection.

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

For More Information

For the procedure for initializing the NME IPS, see [Advanced Setup for the NME IPS, page 3-24](#).

Displaying the Status of the NME IPS

Use the `service-module ids-sensor slot/port status` command in privileged EXEC mode to display the status and statistics of the NME IPS.

To display the status of the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Display the status of the NME IPS.

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
```

```

Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version: 6.2(1)E3
  Model:           NME IPS
  Memory:          443508 KB
  Mgmt IP addr:    10.89.148.195
  Mgmt web ports: 443
  Mgmt TLS enabled: true

router#

```

Enabling and Disabling Heartbeat Reset

Use the **service-module ids-sensor *slot/port* heartbeat reset {enable | disable}** command in privileged EXEC mode to reset the heartbeat of the NME IPS.

When the NME IPS is booted in failsafe mode or is undergoing an upgrade, you can use the **service-module ids heartbeat-reset** command to prevent a reboot during the process. If you leave the heartbeat reset enabled during an upgrade, you may lose the NME IPS heartbeat.

When the NME IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the NME IPS and stops sending traffic to the NME IPS, and sets the NME IPS to error state. The router performs a hardware reset on the NME IPS and monitors the NME IPS until the heartbeat is reestablished.



Note

Disabling the heartbeat reset prevents the router from resetting the module during system image installation if the process takes too long.

To reset the heartbeat of the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Verify the status of heartbeat reset.

```

router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled

```

Step 4 To disable the heartbeat on the NME IPS:

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

Step 5 To reenabling the heartbeat on the NME IPS:

```
router# service-module ids-sensor 1/0 heartbeat-reset enable
```

Rebooting, Resetting, and Shutting Down the NME IPS

This section describes when and how the NME IPS shuts down. It contains the following topics:

- [NME IPS Status Monitoring](#), page 21-12
- [Rebooting, Resetting, and Shutting Down the NME IPS](#), page 21-12

NME IPS Status Monitoring

The NME IPS uses RBCP to monitor its status. RBCP is monitored by the main application on the NME IPS, not by SensorApp. If the main application on the NME IPS fails, the RBCP heartbeat responses do not return from the NME IPS. When the router determines that the NME IPS has failed, a **reload** command is issued through RBCP to reboot the Linux kernel on the NME IPS. In the period during the attempt to bring the NME IPS back up, the router works in the mode determined by the failover operation configured.

In some cases, SensorApp may stop processing, but the main application on the NME IPS continues to process RBCP packets. In this case, packets are processed according to the bypass settings set for the NME IPS by the IPS CLI, IDM, or IME.

There are two situations in which the NME IPS shuts down:

- A hardware or software error forces it to fail. The router can detect this through the loss of the RBCP heartbeat.
- **Reload** or **shutdown** command.

For More Information

- For more information on SensorApp, see [SensorApp](#), page A-22.
- For more information on software bypass, see [Inline Bypass Mode](#), page 5-35.

Rebooting, Resetting, and Shutting Down the NME IPS

Use the **service-module ids-sensor slot/port {reload | reset | shutdown}** command in privileged EXEC mode to reboot, reset, and shut down the NME IPS.

To reboot, reset, and shut down the NME IPS, follow these steps:

-
- Step 1** Log in to the router.
- Step 2** Enter privileged EXEC mode on the router.
- ```
router> enable
```
- Step 3** To gracefully halt and reboot the operating system on the NME IPS:
- ```
router# service-module ids-sensor 1/0 reload
Do you want to proceed with the reload? [confirm]
```
- Step 4** To reset the hardware on the NME IPS:
- ```
router# service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

**Note**

The NME IPS has a compact flash device that functions as a permanent storage device rather than a hard-disk drive.

**Caution**

Data loss occurs only if you issue the **reset** command without first shutting down the NME IPS. You can use the **reset** command safely in other situations.

**Step 5**

To shut down applications running on the NME IPS:

```
router# service-module ids-sensor 1/0 shutdown
Trying 10.10.10.1, 2129 . . . Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

## New and Modified Commands

**Note**

All other Cisco IOS software commands are documented in the Cisco IOS Release 12.4(20)T command reference at Cisco.com, <http://www.cisco.com/en/US/products/ps6441/index.html>.

This section describes the following new and modified Cisco IOS commands, and specific commands that are used to configure the NME IPS. It contains the following topics:

- [interface ids-sensor, page 21-13](#)
- [interface interface\\_name, page 21-15](#)
- [service-module ids-sensor, page 21-16](#)
- [service-module ids-sensor bootmode, page 21-18](#)

### interface ids-sensor

To configure the IPS sensor interface and enter config-if mode, use the **interface ids-sensor** command in config mode. To specify how the router handles traffic inspection during a module failure, use the **service-module** command in config-if mode. The default is fail open.

```
interface ids-sensor slot/port

ip {address | unnumbered}

service-module {fail-close | fail-open}
```

**Syntax Description**

|              |                                                                                           |
|--------------|-------------------------------------------------------------------------------------------|
| <i>slot</i>  | Number of the router chassis slot for the NME IPS.                                        |
| <i>lport</i> | Port number of the NME IPS.                                                               |
| <b>Note</b>  | The slash mark is required between the <i>slot</i> argument and the <i>unit</i> argument. |

|                                  |                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------|
| <b>ids-sensor</b>                | The IPS interface for the sensor.                                                             |
| <b>ip address</b>                | Sets the IP address of an interface.                                                          |
| <b>ip unnumbered</b>             | Enables IP address processing without an explicit IP address.                                 |
| <b>service-module fail-close</b> | The NME IPS drops all the traffic.                                                            |
| <b>service-module fail-open</b>  | The NME IPS passes all the traffic through, but does not perform traffic inspection (default) |

**Caution**

Although there are 57 subcommands associated with the **ip** command, the only two supported for the modules are **ip address** and **ip unnumbered**. Enabling any of the other subcommands can result in unpredictable behavior.

**Command Defaults****Command Modes**

Config  
Config-if

**Command History**

| Release   | Modification                 |
|-----------|------------------------------|
| 12.4(20)T | This command was introduced. |

**Usage Guidelines**

The **interface ids-sensor slot/port** command lets you enter config-if mode and configure the IPS sensor slot and port. On the NME IPS, the slot value is specified by identifying the physical location where the module is installed on the router and the port number is 0.

**Examples**

The following example demonstrates how to use the **interface IDS-Sensor** command to enter config-if mode on an NME IPS in slot 1, port 0:

```
router(config)# interface ids-sensor 1/0
router(config-if)#
```

The following example demonstrates how to use the **interface ids-sensor** command with the **ip unnumbered** subcommand to specify the router command and control interface:

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered router_command_and_control_interface
router(config-if)#
```

The following example demonstrates how to use the **service-module fail-open** command to configure the module to pass all traffic through the module when the hardware fails, but not to perform traffic inspection:

```
router(config)# interface ids-sensor 1/0
router(config-if)# service-module fail-open
router(config-if)#
```

| Related Commands | Command                                | Description                                           |
|------------------|----------------------------------------|-------------------------------------------------------|
|                  | <b>interface</b> <i>interface_name</i> | Lets you specify which interface should be monitored. |

## interface *interface\_name*

To enter config-if mode, configure the interface for monitoring in promiscuous or inline mode, and apply a standard or extended ACL to inline monitoring, use the **interface** *interface\_name* command in config mode.

```
interface interface_name
```

```
ids-service-module monitoring {promiscuous | inline} access-list number
```

| Syntax Description | Parameter                 | Description                                                                            |
|--------------------|---------------------------|----------------------------------------------------------------------------------------|
|                    | <i>interface_name</i>     | The name of the router interface to be monitored.                                      |
|                    | <b>ids-service-module</b> | Configures IPS on the interface.                                                       |
|                    | <b>monitoring</b>         | Specifies how the NME IPS inspects traffic.                                            |
|                    | <b>promiscuous</b>        | Specifies whether the NME IPS inspects traffic in promiscuous mode.                    |
|                    | <b>inline</b>             | Specifies whether the NME IPS inspects traffic in inline mode.                         |
|                    | <b>access-list</b>        | Specifies that you are applying a numbered or extended ACL to the inspected interface. |
|                    | <i>number</i>             | Number of the ACL.                                                                     |

### Command Defaults

**Command Modes**

Config  
Config-if

| Command History | Release   | Modification                 |
|-----------------|-----------|------------------------------|
|                 | 12.4(20)T | This command was introduced. |

**Usage Guidelines**

The **interface** *interface\_name* command lets you enter config-if mode and configure the router to operate in inline or promiscuous mode for that interface.

**Examples**

The following example demonstrates how to use the **interface** command to enter config-if mode and configure monitoring for GigabitEthernet0/0 using ACL 101:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# ids-service-module monitoring inline access-list 101
router(config-if)#
```

| Related Commands | Command                           | Description                   |
|------------------|-----------------------------------|-------------------------------|
|                  | <code>interface ids-sensor</code> | Configures the IPS interface. |

## service-module ids-sensor



### Caution

When you reload the router, the NME IPS also reloads. To ensure that there is no loss of data on the NME IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.

To prevent the Cisco IOS software from rebooting the NME IPS when the heartbeat is lost, to reboot, reset, enable console access to, shut down, see the statistics, and monitor the status of a module, use the **service-module ids-sensor** command in privileged EXEC mode.

```
service-module ids-sensor slot/port {heartbeat-reset {enable | disable} reload | reset | session |
shutdown | status}
```

| Syntax                 | Description                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>slot</i>            | Number of the router chassis slot for the module.                                                                                                                                                                            |
| <i>port</i>            | Port number of the NME IPS.<br><b>Note</b> The slash mark is required between the <i>slot</i> argument and the <i>unit</i> argument.                                                                                         |
| <b>heartbeat-reset</b> | Enables or disables the heartbeat reset. The default is enabled.<br><b>Note</b> Disabling the heartbeat reset prevents the router from resetting the NME IPS during system image installation if the process takes too long. |
| <b>reload</b>          | Performs a graceful halt and reboot of the operating system on the NME IPS.                                                                                                                                                  |
| <b>reset</b>           | Resets the hardware on the NME IPS. This command is usually used to recover from a shutdown.                                                                                                                                 |
| <b>session</b>         | Enables console access to the NME IPS from the router.                                                                                                                                                                       |
| <b>shutdown</b>        | Shuts down the IPS application running on the module.                                                                                                                                                                        |
| <b>statistics</b>      | Provides NME IPS statistics.                                                                                                                                                                                                 |
| <b>status</b>          | Provides information about the status of the IPS software.                                                                                                                                                                   |

### Defaults

**Command Modes** Privileged EXEC

| Command History | Release   | Modification                 |
|-----------------|-----------|------------------------------|
|                 | 12.4(20)T | This command was introduced. |



**Usage Guidelines**

When the NME IPS is booted in failsafe mode or is undergoing an upgrade, you can use the **service-module ids heartbeat-reset** command to prevent a reboot during the process. If you leave the heartbeat reset enabled during an upgrade, you may lose the AIM IPS heartbeat.

When the NME IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the NME IPS and stops sending traffic to the NME IPS, and sets the NME IPS to error state. The router performs a hardware reset on the NME IPS and monitors the NME IPS until the heartbeat is reestablished.

If a confirmation prompt is displayed, press **Enter** to confirm the action or **n** to cancel.

**Examples**

The following example demonstrates how to disable or enable the reset action when the heartbeat is lost on an NME IPS in slot 1, port 0:

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

The following example demonstrates how to enable the IDS heartbeat on the NME IPS:

```
router# service-module ids-sensor 1/0 heartbeat-reset enable
```

The following example demonstrates how to display the status of the heartbeat reset by using the **service-module ids slot/port status** command:

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled
```

The following example demonstrates how to gracefully halt and reboot the operating system on the NME IPS:

```
router# service-module ids-sensor 1/0 reload
```

```
Do you want to proceed with reload?[confirm]
```

The following example demonstrates how to reset the hardware on an NME IPS. A warning is displayed:

```
router# service-module ids-sensor 1/0 reset
```

```
Use reset only to recover from shutdown or failed state
Warning: May lose data on the NVRAM, nonvolatile file system or unsaved configuration!
```

```
Do you want to reset?[confirm]
```

The following example enables console access to the NME IPS operating system:

```
router# service-module ids-sensor 1/0 session
```

The following example demonstrates how to shut down IPS applications running on the NME IPS:

```
router# service-module ids-sensor 1/0 shutdown
```

```
Trying 10.10.10.1, 2129 ... Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor 1/0 shutdown complete
```

The following example demonstrates how to display IPS software statistics:

```
router# service-module ids-sensor 1/0 statistics
Module Reset Statistics:
 CLI reset count = 1
 CLI reload count = 0
 Registration request timeout reset count = 1
```

```
Error recovery timeout reset count = 1
Module registration count = 7
```

The last IOS initiated event was a cli reset at 20:18:36.038 UTC Tue Jan 16 2007

The following example demonstrates how to display the status of the IPS software on the NME IPS:

```
router# service-module ids-sensor 1/0 status

Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait...
Service Module Version information received, Major ver = 1, Minor ver= 1

Cisco Systems Intrusion Prevention System Network Module
Software version: 6.1(1)E1
Model: NME IPS
Memory: 890996 KB
Mgmt IP addr: 10.1.9.201
Mgmt web ports: 443
Mgmt TLS enabled: true
```

| Related Commands | Command                              | Description                                      |
|------------------|--------------------------------------|--------------------------------------------------|
|                  | <b>ids-service-module monitoring</b> | Enables IPS monitoring on a specified interface. |

## service-module ids-sensor bootmode

To enter failsafe or normal boot mode for the NME IPS, use the **service-module ids-sensor bootmode** command in privileged EXEC mode.

```
service-module ids-sensor slot/port bootmode {failsafe | normal}
```

| Syntax Description | Parameter       | Description                                                                                                                                      |
|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <i>slot</i>     | Number of the router chassis slot for the NME IPS. The slash mark (/) is required between the <i>slot</i> argument and the <i>port</i> argument. |
|                    | <i>port</i>     | Port number of the NME IPS.                                                                                                                      |
|                    | <b>failsafe</b> | Enters failsafe boot mode on the NME IPS                                                                                                         |
|                    | <b>normal</b>   | Enters normal boot mode on the NME IPS.                                                                                                          |

**Defaults** None

**Command Modes** Privileged EXEC (#)

| Command History | Release   | Modification                                                  |
|-----------------|-----------|---------------------------------------------------------------|
|                 | 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

---

**Usage Guidelines**

If a confirmation prompt is displayed, press **Enter** to confirm the action, or press **n** to cancel.

---

**Examples**

The following example demonstrates how to enter failsafe boot mode on an NME IPS in slot 1, port 0:

```
router# service-module ids-sensor 1/0 bootmode failsafe
```

The following example demonstrates how to enter normal boot mode on the NME IPS:

```
router# service-module ids-sensor 1/0 bootmode normal
```

---

**Related Commands**

| <b>Command</b>                       | <b>Description</b>                               |
|--------------------------------------|--------------------------------------------------|
| <b>ids-service-module monitoring</b> | Enables IDS monitoring on a specified interface. |

---

