CHAPTER 22

Upgrading, Downgrading, and Installing System Images

This chapter describes how to upgrade, downgrade, and install system images. It contains the following sections:

Upgrades, Downgrades, and System Images

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update, signature engine update, minor version, major version, or recovery partition file. Downgrading removes the last applied service pack or signature update from the sensor.

Caution You cannot use the **downgrade** command to go from Cisco IPS 6.1 to 6.0. To revert to 6.0, you must reimage the sensor.

You can recover the application partition image on your sensor if it becomes unusable. Using the **recover** command lets you retain your host settings while other settings revert to the factory defaults.

To install a new system image on the sensor, use ROMMON, the bootloader file, or the maintenance partition depending on which platform you have.

When you install a new system image on your sensor, all accounts are removed and the default cisco account is reset to use the default password **cisco**. After installing the system image, you must initialize the sensor again.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, signature engine update, minor update, major update, and recovery partition file.

For More Information

- For the procedure for initializing the sensor, see Basic Sensor Setup, page 3-3.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Supported FTP and HTTP/HTTPS Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CMS - Apache Server (Tomcat)
- CMS - Apache Server (JRun)

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for configuring automatic updates, see Configuring Automatic Upgrades, page 22-6.

Upgrading the Sensor

Note For the IDM procedure for upgrading the sensor, refer to Manually Updating the Sensor. For the IME procedure, refer to Manually Updating the Sensor.

This section explains how to use the **upgrade** command to upgrade the software on the sensor. It contains the following topics:

IPS 6.1 Upgrade Files

The following files are part of Cisco IPS 6.1(1)E1:

- Readme
  - IPS-6.1-1-E1.readme.txt
- Minor Version Upgrade File
  - IPS-K9-6.1-1-E1.pkg
  - IPS-AIM-K9-6.1-1-E1.pkg
- System Image Files
  - IPS-4240-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-4255-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-4260-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-4270-K9-sys-1.1-a-6.1-1-E1.img
  - WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.bin.gz
  - IPS-SSM_10-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-SSM_20-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-SSM_40-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-AIM-K9-sys-1.1-a-6.1-1-E1.img
  - IPS-NME-K9-sys-1.1-a-6.1-1-E2.img
- Recovery Image Files
  - IPS-K9-r-1.1-a-6.1-1-E1.pkg
  - IPS-AIM-K9-r-1.1-a-6.1-1-E1.pkg
  - IPS-NME-K9-r-1.1-a-6.1-1-E2.pkg

For More Information

For the procedure for obtaining these files on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

upgrade Command and Options

Note For the IDM procedure for upgrading the sensor, refer to Manually Updating the Sensor. For the IME procedure, refer to Manually Updating the Sensor.

Use the **upgrade** *source-url* command to apply service pack, signature update, engine update, minor version, major version, or recovery partition file upgrades.

The following options apply:

- *source-url*—The location of the source file to be copied.
- ftp:—Source URL for an FTP network server. The syntax for this prefix is:

  ftp://[[username@]location][/relativeDirectory]/filename

  ftp://[[username@]location][//absoluteDirectory]/filename

Note You are prompted for a password.

- scp:—Source URL for the SCP network server. The syntax for this prefix is:

  scp://[[username@]location][/relativeDirectory]/filename

  scp://[[username@]location][//absoluteDirectory]/filename

  Note You are prompted for a password. You must add the remote host to the SSH known hosts list.

- http:—Source URL for the web server. The syntax for this prefix is:

  http://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file.

- https:—Source URL for the web server. The syntax for this prefix is:

  https://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file. The remote host must be a TLS trusted host.

Using the upgrade Command

Note For the IDM procedure for upgrading the sensor, refer to Manually Updating the Sensor. For the IME procedure, refer to Manually Updating the Sensor.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file (for example, IPS-K9-6.1-1-E1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Note You must log in to Cisco.com using an account with cryptographic privileges to download the file. Do not change the filename. You must preserve the original filename for the sensor to accept the update.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-K9-6.1-1-E1.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-K9-6.1-1-E1.pkg
```

Step 5 Enter the password when prompted.

```
Enter password: ********
```

Step 6 Enter **yes** to complete the upgrade.

Note Major updates, minor updates, and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

Note The operating system is reimaged and all files that have been placed on the sensor through the service account are removed.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privileges, see Obtaining Cisco IPS Software, page 21-1.

Upgrading the Recovery Partition

Use the **upgrade** command to upgrade the recovery partition with the most recent version so that it is ready if you need to recover the application partition on your sensor.

Note Recovery partition images are generated for major and minor updates and only in rare situations for service packs or signature updates.

Note The AIM IPS and the NME IPS have unique recovery images (IPS-AIM-K9-r-1.1-a-6.1-1-E1.pkg and IPS-NME-K9-r-1.1-a-6.1-1-E2.pkg) that you must use to upgrade the recovery partition.

To upgrade the recovery partition on your sensor, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-6.1-1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Caution Some browsers add an extension to the filename. The filename of the saved file must match what is displayed on the download page or you cannot use it to upgrade the recovery partition.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the recovery partition.

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-6.1-1-E1.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-6.1-1-E1.pkg
```

Step 5 Enter the server password.

The upgrade process begins.

Note This procedure only reimages the recovery partition. The application partition is not modified by this upgrade. To reimage the application partition after the recovery partition, use the **recover application-partition** command.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for using the **recover** command, see Using the recover Command, page 22-11.

Configuring Automatic Upgrades

Note For the IDM procedure for automatically upgrading the sensor, refer to Configuring Automatic Update. For the IME procedure, refer to Configuring Automatic Update.

This section describes how to configure the sensor to automatically look for upgrades in the upgrade directory. It contains the following topics:

Automatic Upgrades

You can configure the sensor to look for new upgrade files in your upgrade directory automatically. For example, several sensors can point to the same remote FTP server directory with different update schedules, such as every 24 hours, or Monday, Wednesday, and Friday at 11:00 pm.

You specify the following information to schedule automatic upgrades:

- Server IP address
- Path of the directory on the file server where the sensor checks for upgrade files

- File copy protocol (SCP or FTP)
- Username and password
- Upgrade schedule

You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades.

For More Information

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

auto-upgrade Command and Options

Note For the IDM procedure for automatically upgrading the sensor, refer to Configuring Automatic Update. For the IME procedure, refer to Configuring Automatic Update.

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

The following options apply:

- **cisco-server**—Enables automatic signature and engine updates from Cisco.com.
- **cisco-url**—The Cisco server locator service.

  You do not need to change this unless the www.cisco.com IP address changes.
- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

  A leading '/' indicates an absolute path.
- **file-copy-protocol**— File copy protocol used to download files from the file server. The valid values are **ftp** or **scp**.

  Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.
- **ip-address**— IP address of the file server.
- **password**— User password for Cisco server authentication.
- **schedule-option**—Schedules when Cisco server automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.
  - **calendar-schedule**—Configure the days of the week and times of day that automatic upgrades will be performed.

    days-of-week—Days of the week on which auto-upgrades will be performed. You can select multiple days: *sunday* through *saturday* are the valid values.

    no—Removes an entry or selection setting.

    times-of-day—Times of day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.

  - **periodic-schedule**—Configure the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.

    interval—The number of hours to wait between automatic upgrades. Valid values are 0 to 8760.

    start-time—The time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.

- **user-name**—Username for server authentication.
- **user-server**—Enables automatic upgrades from a user-defined server.

For More Information

For the CLI procedure for adding the SCP server to the SSH known hosts list, see Adding Hosts to the SSH Known Hosts List, page 4-42.

Using the auto-upgrade Command

Note For the IDM procedure for automatically upgrading the sensor, refer to Configuring Automatic Update. For the IME procedure, refer to Configuring Automatic Update.

Note If you get an unauthorized error message while configuring an automatic update, make sure you have the correct ports open on any firewalls between the sensor and Cisco.com. For example, you need 198.133.219.25 port 443 for the initial automatic update connection to www.cisco.com, and you need 198.133.219.243 port 80 to download the chosen package from a Cisco file server. The IP address may change for the Cisco file server, but you can find it in the lastDownloadAttempt section in the output of the **show statistics host** command.

Note To check the status of the last automatic update or the next scheduled automatic update, run the **show statistics host** command and check the Auto Update Statistics section.

To schedule automatic upgrades, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter automatic upgrade submode.

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade
sensor(config-hos-aut)#
```

Step 3 Configure the sensor to automatically look for new upgrades either on Cisco.com or on your file server:

a. On Cisco.com:

```
sensor(config-hos-aut)# cisco-server enabled
```

Continue with Step 4.

b. From your server:

```
sensor(config-hos-aut)# user-server enabled
```

c. Specify the IP address of the file server.

```
sensor(config-hos-ena)# ip-address 10.1.1.1
```

d. Specify the directory where the upgrade files are located on the file server.

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

e. Specify the file server protocol.

```
sensor(config-hos-ena)# file-copy-protocol ftp
```

Note If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the sensor can communicate with it through SSH.

Step 4 Specify the username for authentication.

```
sensor(config-hos-ena)# user-name tester
```

Step 5 Specify the password of the user.

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

Step 6 Specify the scheduling:

a. For calendar scheduling, which starts upgrades at specific times on specific day:

```
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal)# days-of-week sunday
sensor(config-hos-ena-cal)# times-of-day 12:00:00
```

b. For periodic scheduling, which starts upgrades at specific periodic intervals:

```
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
sensor(config-hos-ena-per)# start-time 13:00:00
```

Step 7 Verify the settings.

```
sensor(config-hos-ena)# show settings
   enabled
   -----------------------------------------------
      schedule-option
      -----------------------------------------------
         periodic-schedule
         -----------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
         -----------------------------------------------
      -----------------------------------------------
      ip-address: 10.1.1.1
      directory: /tftpboot/update/6.1_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   -----------------------------------------------
sensor(config-hos-ena)#
```

Step 8 Exit automatic upgrade submode.

```
sensor(config-hos-ena)# exit
```

```
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

Step 9 Press **Enter** to apply the changes or type **no** to discard them.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the CLI procedure for adding the SCP server to the SSH known hosts list, see Adding Hosts to the SSH Known Hosts List, page 4-42.
- For the output of the **show statistics host** command, see Displaying Statistics, page 16-26.

Downgrading the Sensor

Caution You cannot use the **downgrade** command to go from Cisco IPS 6.1 to 6.0. To revert to 6.0, you must reimage the sensor. You can only use the **downgrade** command to downgrade from the latest service pack or signature update.

Use the **downgrade** command to remove the last applied service pack or signature upgrade from the sensor.

To remove the last applied service pack or signature update from the sensor, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Downgrade the sensor.

```
sensor(config)# downgrade
Warning: Executing this command will reboot the system and downgrade to
IPS-K9-sp.6.0-2-E1.pkg. Configuration changes made since the last upgrade will be lost and
the system may be rebooted.
Continue with downgrade?:
```

Step 4 Enter **yes** to continue with the downgrade.

Step 5 If there is no recently applied service pack or signature update, the **downgrade** command is not available.

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

Recovering the Application Partition

This section explains how to recover the application partition, and contains the following topics:

Application Partition

You can recover the application partition image for the appliance if it becomes unusable. Some network configuration information is retained when you use this method, which lets you have network access after the recovery is performed.

Use the **recover application-partition** command to boot to the recovery partition, which automatically recovers the application partition on your appliance.

Note If you have upgraded your recovery partition to the most recent version before you recover the application partition image, you can install the most up-to-date software image.

Because you can execute the **recover application-partition** command through a Telnet or SSH connection, we recommend using this command to recover sensors that are installed at remote locations.

Note When you reconnect to the sensor after recovery, you must log in with the default username and password **cisco**.

For More Information

For the procedure for upgrading the recovery partition to the most recent version, see Upgrading the Recovery Partition, page 22-5.

Using the recover Command

To recover the application partition image, follow these steps:

Step 1 Download the recovery partition image file (IPS-K9-r-1.1-a-6.1-1-E1.pkg) to an FTP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Note To upgrade the recovery partition the sensor must already be running IPS 6.1(1) or later.

Step 4 Recover the application partition image.

```
sensor(config)# recover application-partition
```

```
Warning: Executing this command will stop all applications and re-image the node to
version 6.1(1)E1. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

Step 5 Enter **yes** to continue.

Shutdown begins immediately after you execute the **recover** command. Shutdown can take a while, and you will still have access to the CLI, but access will be terminated without warning.

The application partition is reimaged using the image stored on the recovery partition. You must now initialize the appliance with the **setup** command.The IP address, netmask, access lists, time zone, and offset are saved and applied to the reimaged application partition. If you executed the **recover application-partition** command remotely, you can SSH to the sensor with the default username and password (**cisco/cisco**) and then initialize the sensor again with the **setup** command. You cannot use Telnet until you initialize the sensor because Telnet is disabled by default.

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for using the **setup** command to initialize the sensor, see Basic Sensor Setup, page 3-3.

Installing System Images

This section contains the procedures for installing system images on the appliances and modules. It contains the following topics:

Caution All user configuration settings are lost when you install the system image. Before trying to recover the sensor by installing the system image, try to recover by using the **recover application-partition** command or by selecting the recovery partition during sensor bootup.

Understanding ROMMON

Some Cisco sensors include a preboot CLI called ROMMON, which lets you boot images on sensors where the image on the primary device is missing, corrupt, or otherwise unable to boot the normal application. ROMMON is particularly useful for recovering remote sensors as long as the serial console port is available.

Access to ROMMON is available only through the serial console port, a Cisco-standard asynchronous RS-232C DTE available in an RJ-45F connector on the sensor chassis. The serial port is configured for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For More Information

For the procedure for using a terminal server, see Connecting an Appliance to a Terminal Server, page 22-13.

TFTP Servers

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server.

In enable mode, enter the following configuration, where # is the line number of the port to be configured:

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
```

```
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Installing the IPS 4240 and the IPS 4255 System Images

You can install the IPS 4240 and the IPS 4255 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

Note This procedure is for the IPS 4240, but is also applicable to the IPS 4255. The system image for the IPS 4255 has "4255" in the filename.

To install the IPS 4240 and the IPS 4255 system image, follow these steps:

Step 1 Download the IPS 4240 system image file (IPS-4240-K9-sys-1.1-a-6.1-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4240.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4240.

Step 2 Boot the IPS 4240.

The console display resembles the following:

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB
High Memory: 2048 MB
interface Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  interface-to-interface Bridge
00  03  00   8086   257B  interface-to-interface Bridge
00  1C  00   8086   25AE  interface-to-interface Bridge
00  1D  00   8086   25A9  Serial Bus         11
```

```
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  interface-to-interface Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS-4240-K9
Management0/0

MAC Address: 0000.c0ff.ee01
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set
```

The output on the configured system resembles the following:

```
ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
      CONFIG=
```

The variables have the following definitions:

- Address—Local IP address of the IPS 4240
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by the IPS 4240
- Port—Ethernet interface used for the IPS 4240 management
- VLAN—VLAN ID number (leave as untagged)

- Image—System image file/path name
- Config—Unused by these platforms

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management0/0, which corresponds to the MGMT interface of the IPS 4240.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the IPS 4240.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4240.

Step 7 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX example

```
rommon> IMAGE=/system_images/IPS-4240-K9-sys-1.1-a-6.1-1-E1.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows example

```
rommon> IMAGE=\system_images\IPS-4240-K9-sys-1.1-a-6.1-1-E1.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4240 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4240. Be sure to use the IPS 4240 image.

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Installing the IPS 4260 System Image

You can install the IPS 4260 system image by using the ROMMON on the appliance to TFTP the system image onto the flash device.

To install the IPS 4260 system image, follow these steps:

Step 1 Download the IPS 4260 system image file (IPS-4260-K9-sys-1.1-a-6.1-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4260.

Make sure you can access the TFTP server location from the network connected to your IPS 4260 Ethernet port.

Step 2 Boot the IPS 4260.

Step 3 Press **Ctrl-R** at the following prompt while the system is booting:

```
Evaluating Run Options...
```

Note You have five seconds to press **Ctrl-R**.

The console display resembles the following:

```
Assuming IPS-4260-K9 Platform
```

```
 2 Ethernet Interfaces detected

Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006

Platform IPS-4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047


Use ? for help.
rommon #0>
```

Step 4 If necessary, change the port used for the TFTP download.

```
rommon #1> interface name
```

The port in use is listed just after the platform identification. In the example, port Management0/0 is being used.

Note The default port used for TFTP downloads is Management0/0, which corresponds with the command and control (MGMT) interface of the IPS 4260.

Note Ports Management0/0 (MGMT) and GigabitEthernet0/1 (GE 0/1) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on the IPS 4260.

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to the IPS 4260.

Step 6 Specify the TFTP server IP address.

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address.

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:.

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> file path/filename
```

UNIX example

```
rommon> file /system_images/IPS-4260-K9-sys-1.1-a-6.1-1-E1.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the file location.

Windows example

```
rommon> file <tftpboot_directory>IPS-4260-K9-sys-1.1-a-6.1-1-E1.img
```

Step 10 Download and install the system image.

```
rommon> tftp
```

Note The IPS 4260 reboots once during the reimaging process. Do not remove power from IPS 4260 during the update process or the upgrade can become corrupted.

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Installing the IPS 4270-20 System Image

You can install the IPS 4270-20 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4270-20 system image, follow these steps:

Step 1 Download the IPS 4270-20 system image file (IPS4270-20-K9-sys-1.1-a-6.1-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4270-20.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4270-20.

Step 2 Boot IPS 4270-20.

The console display resembles the following:

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007

ft_id_update: Invalid ID-PROM Controller Type (0x5df)

ft_id_update: Defaulting to Controller Type (0x5c2)
```

Note The controller type errors are a known issue and can be disregarded.

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set
```

The output on the configured system resembles the following:

```
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

The variables have the following definitions:

- Address—Local IP address of IPS 4270-20
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by IPS 4270-20
- Port—Ethernet interface used for IPS 4270-20 management
- VLAN—VLAN ID number (leave as untagged)
- Image—System image file/path name
- Config—Unused by these platforms

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, assign an IP address for the local port on IPS 4270-20.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to IPS 4270-20.

Step 6 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 7 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

UNIX example

```
rommon> IMAGE=/system_images/IPS4270-20-K9-sys-1.1-a-6.1-1-E1.img
```

Note The path is relative to the UNIX TFTP server default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows example

```
rommon> IMAGE=\system_images\IPS4270-20-K9-sys-1.1-a-6.1-1-E1.img
```

Step 10 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 11 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from IPS 4270-20 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on IPS 4270-20. Be sure to use the IPS 4270-20 image.

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Installing the AIM IPS System Image

To install the AIM IPS system image, follow these steps:

Step 1 Download the AIM IPS system image file (IPS-AIM-K9-sys-1.1-6.1-1-E1.img), and place it on a TFTP server relative to the tftp root directory.

Note Make sure the network is configured so that the AIM IPS can access the TFTP server.

If no TFTP server is available, you can configure the router to operate as a TFTP server.

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-AIM-K9-sys-1.1-6.0-3-E1.img
router(config)# exit
router#
```

Step 2 Disable the heartbeat reset.

```
router# service-module IDS-Sensor 0/slot_number heartbeat-reset disable
```

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

Step 3 Session to the AIM IPS.

```
router# service-module IDS-Sensor 0/slot_number session
```

Note Use the **show configuration | include interface IDS-Sensor** command to determine the AIM IPS slot number.

Step 4 Suspend the session by pressing **Shift-Ctrl-6 X**.

You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 5 Reset the AIM IPS.

```
router# service-module IDS-Sensor 0/slot_number reset
```

You are prompted to confirm the **reset** command.

Step 6 Press **Enter** to confirm.

Step 7 Press **Enter** to resume the suspended session.

After displaying its version, the bootloader displays this prompt for 15 seconds:

```
Please enter '***' to change boot configuration:
```

Step 8 Enter ******* during the 15-second delay.

The bootloader prompt appears.

Step 9 Press **Enter** to session back to the AIM IPS.

Step 10 Configure the bootloader.

```
ServicesEngine bootloader> config

IP Address [10.89.148.188]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

For each prompt, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.

Note The gateway IP address must match the IP address of the IDS-Sensor *slot/port* interface.

Note If you set up the module interfaces using the **unnumbered** command, the gateway IP address should be the IP address of the other router interface being used as part of the unnumbered command.

Caution The pathname for the AIM IPS image is full but relative to the tftp server root directory (typically /tftpboot).

Step 11 Start the bootloader.

```
ServicesEngine bootloader> upgrade
```

Step 12 Follow the bootloader instructions to install the software (choose option 1 and follow the wizard instructions).

Note In the following example, the AIM IPS IP address is 10.1.9.201. The imaging process accesses the AIM IPS image from the router TFTP server at IP address 10.1.9.1.

Example

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
11 ***
ServicesEngine boot-loader Version : 1.1.0
ServicesEngine boot-loader > config

IP Address [10.1.9.201]>
Subnet mask [255.255.255.0]>
TFTP server [10.1.9.1]>
Gateway [10.1.9.1]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for AIM-IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.1.9.1]>
full pathname of recovery image []:IPS-AIM-K9-sys-1.1-6.0-3-E1.img
Ready to begin
Are you sure [Y/N]
Returning TRUE
Press <CTRL-C> to abort.
octeth1:        Up     1Gbs Full duplex, (port  1)
octeth0:        Down  10Mbs Half duplex, (port  0)
```

```
Using octeth1 device
TFTP from server 10.1.9.1; our IP address is 10.1.9.201
Filename 'IPS-AIM-K9-sys-1.1-6.0-3-E1.img'.
Load address: 0x21000000
Loading: ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ######
         32 MB received
         ###################################################################
         ######################
done
```

Step 13 Suspend the session by pressing **Shift-Ctrl-6 X**.

You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 14 From the router CLI, clear the session.

```
router# service-module interface ids-sensor 0/slot_number session clear
```

Step 15 Enable the heartbeat reset.

```
router# service-module IDS-sensor 0/slot_number heartbeat-reset enable
```

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for setting up an unnumbered IP address, see Using an Unnumbered IP Address Interface, page 17-5.

Installing the AIP SSM System Image

This section describes how to install the AIP SSM system image, and contains the following topics:

Reimaging the AIP SSM

You can reimage the AIP SSM in one of the following ways:

- From ASA using the **hw-module module 1 recover configure/boot** command.
- Recovering the application image from the sensor CLI using the **recover application-partition** command.
- Upgrading the recovery image from the sensor CLI using the **upgrade** command.

For More Information

- For the procedure for using the **hw-module module 1 recover configure/boot** command, see Reimaging the AIP SSM Using the recover configure/boot Command, page 22-25.
- For the procedure for recovering the application partition, see Recovering the Application Partition, page 22-11.
- For the procedure for upgrading the recovery image, see Upgrading the Recovery Partition, page 22-5.

Reimaging the AIP SSM Using the recover configure/boot Command

To install the AIP SSM system image, follow these steps:

Step 1 Log in to the ASA.

Step 2 Enter enable mode.

```
asa# enable
```

Step 3 Configure the recovery settings for the AIP SSM.

```
asa (enable)# hw-module module 1 recover configure
```

Note If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

Step 4 Specify the TFTP URL for the system image.

```
Image URL [tftp://0.0.0.0/]:
```

Example

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-6.1-1-E1.img
```

Step 5 Specify the command and control interface of the AIP SSM.

Note The port IP address is the management IP address of the AIP SSM.

```
Port IP Address [0.0.0.0]:
```

Example

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

Step 6 Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

Step 7 Specify the default gateway of the AIP SSM.

```
Gateway IP Address [0.0.0.0]:
```

Example:

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

Step 8 Execute the recovery.

```
asa# hw-module module 1 recover boot
```

Step 9 Periodically check the recovery until it is complete.

Note The status reads `Recovery` during recovery and reads `Up` when reimaging is complete.

```
asa# show module 1

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance         ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P1D000004F4

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#
```

Note To debug any errors that may happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

Step 10 Session to the AIP SSM and initialize the AIP SSM with the **setup** command.

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for initializing AIP SSM, see Advanced Setup for the AIP SSM, page 3-15.

Installing the IDSM2 System Image

This section describes how to the install the IDSM2 system image, and contains the following topics:

Understanding the IDSM2 System Image

If the IDSM2 application partition becomes unusable, you can reimage it from the maintenance partition. After you reimage the application partition of the IDSM2, you must initialize the IDSM2 using the **setup** command. When there is a new maintenance partition image file, you can reimage the maintenance partition from the application partition.

For More Information

For the procedure to use the **setup** command, see Advanced Setup for the IDSM2, page 3-20.

Installing the IDSM2 System Image for Catalyst Software

To install the system image, follow these steps:

Step 1 Download the IDSM2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Boot the IDSM2 to the maintenance partition.

```
console> (enable) reset module_number cf:1
```

Step 4 Log in to the maintenance partition CLI.

```
login: guest
Password: cisco
```

Note You must configure the maintenance partition on the IDSM2.

Step 5 Install the system image.

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1.bin.gz
```

Step 6 Specify the FTP server password.

After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing
it [y|n]:
```

Step 7 Enter **y** to continue.

When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 8 Exit the maintenance partition CLI and return to the switch CLI.

Step 9 Reboot the IDSM2 to the application partition.

```
console> (enable) reset module_number hdd:1
```

Step 10 When the IDSM2 has rebooted, check the software version.

Step 11 Log in to the application partition CLI and initialize the IDSM2.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for configuration the maintenance partition on IDMS-2, see Configuring the IDSM2 Maintenance Partition for Catalyst Software, page 22-29 and Configuring the IDSM2 Maintenance Partition for Cisco IOS Software, page 22-33.
- For the procedure for initializing the IDSM2, see Advanced Setup for the IDSM2, page 3-20.

Installing the IDSM2 System Image for Cisco IOS Software

To install the system image, follow these steps:

Step 1 Download the IDSM2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Boot the IDSM2 to the maintenance partition.

```
router# hw-module module module_number reset cf:1
```

Step 4 Session to the maintenance partition CLI.

```
router# session slot slot_number processor 1
```

Step 5 Log in to the maintenance partition CLI.

```
login: guest
Password: cisco
```

Step 6 Configure the maintenance partition interface IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

Note Choose an address that is appropriate for the VLAN on which the IDSM2 management interface is located based on the switch configuration.

Step 7 Configure the maintenance partition default gateway address.

```
guest@localhost.localdomain# ip gateway gateway_address
```

Step 8 Install the system image.

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_ip_address/directory_path/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.
1.bin.gz-install
```

Step 9 Specify the FTP server password.

After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

Step 10 Enter **y** to continue.

When the application partition file has been installed, you are returned to the maintenance partition CLI.

Step 11 Exit the maintenance partition CLI and return to the switch CLI.

Step 12 Reboot the IDSM2 to the application partition.

```
router# hw-module module module_number reset hdd:1
```

Step 13 Verify that the IDSM2 is online and that the software version is correct and that the status is `ok`.

```
router# show module module_number
```

Step 14 Session to the IDSM2 application partition CLI.

```
router# session slot slot_number processor 1
```

Step 15 Initialize the IDSM2 using the **setup** command.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for configuration the maintenance partition on IDMS-2, see Configuring the IDSM2 Maintenance Partition for Catalyst Software, page 22-29 and Configuring the IDSM2 Maintenance Partition for Cisco IOS Software, page 22-33.
- For the procedure for initializing the IDSM2, see Advanced Setup for the IDSM2, page 3-20.

Configuring the IDSM2 Maintenance Partition for Catalyst Software

To configure the IDSM2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Enter privileged mode.

```
console# enable
console(enable)#
```

Step 3 Reload the IDSM2.

```
console> (enable) reset module_number cf:1
```

Step 4 Session to the IDSM2.

```
console# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM2 maintenance partition.You must session to it from the switch CLI.

Step 5 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM2 application partition for some reason, the IDSM2 requires an RMA.

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 6 View the IDSM2 maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 7 Clear the IDSM2 maintenance partition host configuration (ip address, gateway, hostname).

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 8 Configure the maintenance partition host configuration:

a. Specify the IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway.

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname.

```
guest@localhost.localdomain# ip host hostname
```

Step 9 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :
```

```
guest@idsm2.localdomain#
```

Step 10 Verify the image installed on the application partition.

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       6.1(1)
guest@idsm2.localdomain#
```

Step 11 Verify the maintenance partition version (including the BIOS version).

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 12 Upgrade the application partition.

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.
1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'WS-SVC-IDSM2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1.
bin.gz (unknown size)
/tmp/upgrade.gz            [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1
.bin.gz is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 13 Enter **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 14 Display the upgrade log.

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1
.bin.gz
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 15 Clear the upgrade log.

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 16 Display the upgrade log.

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 17 Ping another computer:.

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 18 Reset the IDSM2.

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. The IDSM2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, the IDSM2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!
console> (enable)#
```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.

Configuring the IDSM2 Maintenance Partition for Cisco IOS Software

To configure the IDSM2 maintenance partition, follow these steps:

Step 1 Log in to the switch CLI.

Step 2 Session to the IDSM2.

```
router# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

Note You cannot Telnet or SSH to the IDSM2 maintenance partition.You must session to it from the switch CLI.

Step 3 Log in as user **guest** and password **cisco**.

Note You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM2 application partition for some reason, you will have to RMA the IDSM2.

```
login: guest
password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 4 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 5 Clear the maintenance partition host configuration (ip address, gateway, hostname).

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

Step 6 Configure the maintenance partition host configuration:

a. Specify the IP address.

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. Specify the default gateway.

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. Specify the hostname.

```
guest@localhost.localdomain# ip host hostname
```

Step 7 View the maintenance partition host configuration.

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

Step 8 Verify the image installed on the application partition.

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       6.1(1)
guest@idsm2.localdomain#
```

Step 9 Verify the maintenance partition version (including the BIOS version).

```
guest@idsm2.localdomain# show version
```

```
Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

Step 10 Upgrade the application partition.

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.img
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.img
(unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.img
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

Step 11 Enter **y** to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

Step 12 Display the upgrade log.

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.1-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.img
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
```

```
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

Step 13 Clear the upgrade log.

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

Step 14 Display the upgrade log.

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

Step 15 Ping another computer.

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

Step 16 Reset the IDSM2.

Note You cannot specify a partition when issuing the **reset** command from the maintenance partition. The IDSM2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, the IDSM2 boots to the application partition.

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...
```

```
The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
router#
```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.

Upgrading the IDSM2 Maintenance Partition for Catalyst Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Session to the IDSM2 from the switch.

```
console>(enable) session slot_number
```

Step 3 Log in to the IDSM2 CLI.

Step 4 Enter configuration mode.

```
idsm2# configure terminal
```

Step 5 Upgrade the maintenance partition.

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

You are asked whether you want continue.

Step 6 Enter the FTP server password.

Step 7 Enter **y** to continue.

The maintenance partition file is upgraded.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Upgrading the IDSM2 Maintenance Partition for Cisco IOS Software

To upgrade the maintenance partition, follow these steps:

Step 1 Download the IDSM2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM2.

Step 2 Log in to the switch CLI.

Step 3 Session in to the application partition CLI.

```
router# session slot slot_number processor 1
```

Step 4 Log in to the IDSM2.

Step 5 Enter configuration mode.

```
idsm2# configure terminal
```

Step 6 Upgrade the maintenance partition.

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

Step 7 Specify the FTP server password.

```
Password: ********
```

You are prompted to continue.

```
Continue with upgrade?:
```

Step 8 Enter **yes** to continue.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 22-2.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.

Installing the NME IPS System Image

Note Use the **show configuration | include interface ids-sensor** command to determine the NME IPS slot number.

To install the NME IPS system image, follow these steps:

Step 1 Download the NME IPS system image file (IPS-NME-K9-sys-1.1-6.1-1-E2.img), and place it on a TFTP server relative to the tftp root directory.

Note Make sure the network is configured so that the NME IPS can access the TFTP server.

If no TFTP server is available, you can configure the router to operate as a TFTP server.

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-NME-K9-sys-1.1-6.1-1-E2.img
router(config)# exit
router#
```

Step 2 Disable the heartbeat reset.

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

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

Step 3 Session to the NME IPS.

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

Step 4 Suspend the session by pressing **Shift-Ctrl-6 X**.

You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 5 Reset the NME IPS.

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

You are prompted to confirm the **reset** command.

Step 6 Press **Enter** to confirm.

Step 7 Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds:

```
Please enter '***' to change boot configuration:
```

Step 8 Enter ******* during the 15-second delay.

The bootloader prompt appears.

Step 9 Press **Enter** to session back to the NME IPS.

Step 10 Configure the bootloader.

```
ServicesEngine bootloader> config

IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

For each prompt, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.

Caution The pathname for the NME IPS image is full but relative to the tftp server root directory (typically /tftpboot).

Step 11 Start the bootloader.

```
ServicesEngine bootloader> upgrade
```

Step 12 Follow the bootloader instructions to install the software (choose option 1 and follow the wizard instructions).

Example

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
12 ***
ServicesEngine boot-loader Version : 1.2.0
ServicesEngine boot-loader > config
```

```
IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for NM-IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.89.150.74]>
full pathname of recovery image []:test/sensor/6.1-1-E2/IPS-NME-K9-sys-1.1-a-6.1-1-E2.img
Ready to begin
Are you sure [Y/N]
Press <CTRL-C> to abort.
octeth0:        Up     1Gbs Full duplex, (port  0)
octeth1:        Up     1Gbs Full duplex, (port  1)
Using octeth0 device
TFTP from server 10.89.150.74; our IP address is 10.89.148.195; sending through gateway
10.89.148.254
Filename 'test/sensor/6.1-1-E2/IPS-NME-K9-sys-1.1-a-6.1-1-E2.img'.
Load address: 0x21000000
Loading: octeth0: Down   1Gbs Half duplex, (port  0)
octeth0: Down   1Gbs Full duplex, (port  0)
octeth0: Up     1Gbs Full duplex, (port  0)
T T T T T T T T ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ######
         32 MB received
         ###################################################################
         ###################################################################
         ##################
done
```

Step 13 Suspend the session by pressing **Shift-Ctrl-6 X**.

You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 14 From the router CLI, clear the session.

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

Step 15 Enable the heartbeat reset:

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

For More Information

- For more information about TFTP servers, see TFTP Servers, page 22-13.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 21-1.