APPENDIX A

Maintaining the MGX RPM-XF

This appendix describes maintenance procedures you might need to perform as your internetworking needs change. Appendix A contains the following sections:

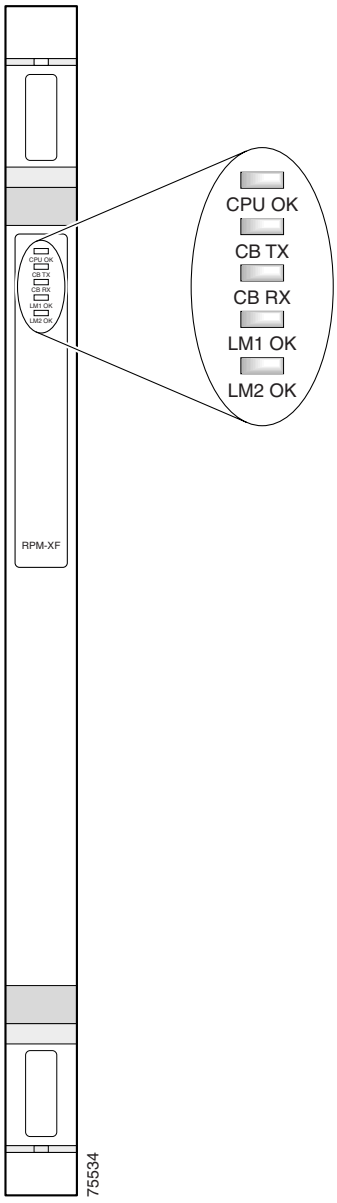
- Reading Front Panel LEDs
- Recovering a Lost Password
- Virtual Configuration Register Settings
- Copying a Cisco IOS Image to Bootflash
- Recovering Boot and System Images

Reading Front Panel LEDs

The LEDs on the front panel of the RPM-XF indicate the current operating condition of the RPM-XF. You can observe the LEDs, note the fault condition the RPM-XF is encountering, and contact your system administrator or TAC, if necessary.

Figure A-1 shows the front panel and LEDs of the RPM-XF. Table A-1 describes how to interpret front-panel LED activity.

Figure A-1 MGX RPM-XF Front Panel LEDs



The LEDs are labeled and indicate overall status and activity on ports by flickering. When there is heavy activity on a port, the LED might be on constantly. If an LED is not on when the port is active and the cable is connected correctly, there might be a problem with the port.

Table A-1 Front Panel LEDs

LED NAME	COLOR	DEFINITION
CPU OK	Off	CPU is not operational
	Green	Card is Active
	Yellow	Card is Standby
	Red	Card has Failed

Table A-1 Front Panel LEDs (continued)

LED NAME	COLOR	DEFINITION
CB TX	Off	Cells are not being transmitted to the cellbus.
	Green	Cells are being transmitted to the cellbus.
CB RX	Off	Cells are not being received from the cellbus.
	Green	Cells are being received from the cellbus.
LM1 OK	Off	Back card in bay 1 is not present.
	Green	Back card in bay 1 is present and active. FPGA and SFP initialization was successful.
	Red	Back card in bay 1 is present, but not active. FPGA and/or SFP initialization failed.
LM2 OK	Off	Back card in bay 2 is not present.
	Green	Back card in bay 2 is present and active. FPGA and SFP initialization was successful.
	Red	Back card in bay 2 is present, but not active. FPGA and/or SFP initialization failed.

Recovering a Lost Password

This section describes how to recover a lost enable or console login password, and how to replace a lost enable secret password on your RPM.

Note It is possible to recover the enable or console login password. The enable secret password is encrypted, however, and must be replaced with a new enable secret password.

Following is an overview of the steps in the password recovery procedure:

- If you can log in to the RPM-XF, enter the **show version** command to determine the existing configuration register value.
- Press the **Break** key to get to the bootstrap program prompt (ROM monitor). You might need to reload the system image by power cycling the RPM-XF.
- Change the configuration register so the following functions are enabled: Break; ignore startup configuration; boot from bootflash memory.

  Note The key to recovering a lost password is to set the configuration register bit 6 (0x0040) so that the startup configuration (usually in NVRAM) is ignored. This will allow you to log in without using a password and to display the startup configuration passwords.

- Power cycle the RPM-XF by turning power off and then back on.
- Log in to the RPM-XF and enter the privileged EXEC mode.
- Enter the **show startup-config** command to display the passwords.
  - Recover or replace the displayed passwords.
  - Change the configuration register back to its original setting.

Note To recover a lost password if Break is disabled on the RPM-XF, you must have physical access to the RPM-XF.

Password Recovery Procedure

Complete the following steps to recover or replace a lost enable, enable secret, or console login password.

Step 1 Attach an ASCII terminal to the console port on your MGX-XF-UI or MGX-XF-UI/B back card.

Step 2 Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1stop bit. If you have changed the configuration parameters of the console port, then configure the terminal to use those parameters instead.

Step 3 If you can log in to the RPM-XF as a non privileged user, enter the **show version** command to display the existing configuration register value. Note the value for use later. If you cannot log in to the RPM-XF, go to the next step.

Step 4 Press the **Break** key or send a Break from the console terminal.

If Break is enabled, the RPM-XF enters the ROM monitor, indicated by the ROM monitor prompt (`rommon 1>`). Proceed to Step 6. If Break is disabled, power cycle the RPM-XF. (Remove the RPM-XF from the Cisco MGX 8850 chassis and then reinsert it.) Then proceed to Step 5.

Step 5 Within 60 seconds of restoring the power to the RPM-XF, press the **Break** key or send a Break.

This action causes the RPM-XF to enter the ROM monitor and display the ROM monitor prompt (`rommon 1>`).

Step 6 To set the configuration register on an RPM-XF, use the configuration register utility by entering the **confreg** command at the ROM monitor prompt as follows:

```
rommon 1> confreg
```

Answer **yes** to the enable question “ignore system config info?” Note the current configuration register settings.

Step 7 Initialize the RPM-XF by entering the **reset** command as follows:

```
rommon 2> reset
```

The RPM-XF will initialize, the configuration register will be set to 2142, and the RPM-XF will boot the system image from Flash memory and enter the system configuration dialog (setup) as follows:

```
--- System Configuration Dialog --
```

Step 8 Enter **no** in response to the system configuration dialog prompts until the following message is displayed:

```
Press RETURN to get started!
```

Step 9 Press **Return**. The user EXEC prompt is displayed as follows:

```
Router>
```

Step 10 Enter the **enable** command to enter the privileged EXEC mode.

Then enter the **show startup-config** command to display the passwords in the configuration file as follows:

```
Router# show startup-config
```

Step 11 Scan the configuration file display looking for the passwords (the enable passwords are usually near the beginning of the file, and the console login or user EXEC password is near the end). The passwords displayed will look something like this:

```
enable secret 5 $1$ORPP$s9syZt4uKn3SnpuLDrhuei
enable password 23skiddoo
.
.
line con 0
 password onramp
```

The enable secret password is encrypted and cannot be recovered; it must be replaced. The enable and console passwords may be encrypted or clear text. Proceed to the next step to replace an enable secret, console login, or enable password. If there is no enable secret password, note the enable and console login passwords if they are not encrypted and proceed to Step 16.

Caution *Do not* start the next step unless you determine you must change or replace the enable, enable secret, or console login passwords. Failure to follow the steps as shown may cause you to erase your RPM-XF configuration.

Step 12 Enter the **configure memory** command to load the startup configuration file into running memory. This action allows you to modify or replace passwords in the configuration.

```
Router# configure memory
```

Step 13 Enter the privileged EXEC command **configure terminal** to enter configuration mode.

```
Router# configure terminal
```

Step 14 To change all three passwords, enter the following commands:

```
Router(config)# enable secret newpassword1
Router(config)# enable password newpassword2
Router(config)# line con 0
Router(config-line)# password newpassword3
```

Change only the passwords necessary for your configuration. You can remove individual passwords by using the **no** form of the above commands. For example, entering the **no enable secret** command will remove the enable secret password.

Step 15 You must configure all interfaces to not administratively shutdown as follows:

```
Router(config)# interface fastethernet 2/0
Router(config-int)# no shutdown
```

Enter the equivalent commands for all interfaces that were originally configured. If you omit this step, all interfaces will be administratively shutdown and unavailable when the RPM-XF is restarted.

Step 16 Use the **config-register** command to set the configuration register to the original value noted in Step 3 or Step 7, or to the factory default value 0x2102 as follows:

```
Router(config)# config-register 0x2102
```

Step 17 Press **Ctrl-Z** or enter **end** to exit configuration mode and return to the EXEC command interpreter.

Caution *Do not* start the next step unless you have changed or replaced a password. If you skipped Step 12 through Step 15, skip to Step 19. Failure to observe this caution will cause you to erase your RPM-XF configuration file.

Step 18 Enter the **copy running-config startup-config** command to save the new configuration to nonvolatile memory.

Step 19 Enter the **reload** command to reboot the RPM-XF.

Step 20 Log in to the RPM-XF with the new or recovered passwords.

This routine completes the steps for recovering or replacing a lost enable, enable secret, or console login password.

Virtual Configuration Register Settings

The RPM-XF has a 16-bit virtual configuration register, which is written into NVRAM. You might want to change the virtual configuration register settings for the following reasons:

- Set and display the configuration register value.
- Force the system into the ROM monitor or boot ROM.
- Select a boot source and default boot filename.
- Enable or disable the Break function.
- Control broadcast addresses.
- Set the console terminal baud rate.
- Recover a lost password (ignore the configuration file in NVRAM).
- Enable Trivial File Transfer Protocol (TFTP) server boot.

Table A-2 lists the meaning of each of the virtual configuration memory bits and defines the boot field names.

Caution To avoid confusion and possibly halting the RPM-XF, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table A-2. For example, the factory default value of 0x2102 is a combination of settings.

Table A-2 Virtual Configuration Register Bit Meaning

Bit No.[1]	Hexadecimal	Meaning
00–03	0x0000–0x000F	Boot field
05	0x0020	Console line speed
06	0x0040	Causes system software to ignore the contents of NVRAM (startup-config)
07	0x0080	OEM bit is enabled

Table A-2 Virtual Configuration Register Bit Meaning (continued)

Bit No.[1]	Hexadecimal	Meaning
08	0x0100	Break is disabled
10	0x0400	IP broadcast with all zeros
11–12	0x0800–0x1000	Console line speed
13	0x2000	Load the boot ROM software if a Flash boot fails five times
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore the contents of NVRAM

1. The factory default value for the configuration register is 0x2102. This value is a combination of the following: bit 13 = 0x2000, bit 8 = 0x0100, and bits 00 through 03 = 0x0002.

Changing Configuration Register Settings

Complete the following steps to change the configuration register while running Cisco IOS software.

Step 1 Enter the **enable** command and your password to enter privileged mode.

```
Router> enable
password: enablepassword
MGX 8850-RPM#
```

Step 2 Enter the **configure terminal** command at the privileged-level system prompt (#).

```
Router# configure terminal
```

Step 3 To set the contents of the configuration register, enter the configuration command **config-register 0x**<*value*>, where *value* is a hexadecimal number (see Table A-2 and Table A-3).

```
Router(config)# config-register 0xvalue
```

(The virtual configuration register is stored in NVRAM.)

Table A-3 Explanation of Boot Field (Configuration Register Bits 00 to 03)

Boot Field	Boot Process
0x0	Stops the boot process in the ROM monitor.
0x1	Stops the boot process in the boot ROM monitor.
0x2	Full boot process, which loads the Cisco IOS image in Flash memory.
0x3–0xF	Specifies a default filename for booting over the network from a TFTP server. Enables boot system commands that override the default filename for booting over the network from a TFTP server.

Step 4 Press **Ctrl-Z** to exit configuration mode.

The new settings will be saved to memory; however, the new settings are not effective until the system software is reloaded by rebooting the RPM-XF.

Step 5 To display the configuration register value currently in effect and the value that will be used at the next reload, enter the **show version** EXEC command. The value displays on the last line of the screen display.

```
Configuration register is 0x142 (will be 0x102 at next reload)
```

Step 6 Reboot the RPM-XF.

The new value takes effect. Configuration register changes take effect only when the RPM-XF restarts, which occurs when you turn the system on or when you enter the **reload** command.

Virtual Configuration Register Bit Meanings

The lowest four bits of the virtual configuration register (bits 3, 2, 1, and 0) form the boot field (see Table A-3). The boot field specifies a number in binary form. If you set the boot field value to 0, you must boot the operating system manually by entering the **b** command at the bootstrap prompt. For example

```
> b [tftp] bootflash filename
```

The **b** command options are as follows:

- **b**—Boots the default system software from ROM
- **b bootflash**—Boots the first file in bootflash memory
- **b** *filename [host]*—Boots from the network using a TFTP server
- **b bootflash** *[filename]*—Boots the file *filename* from bootflash memory

For more information about the command **b [tftp] bootflash** *filename*, refer to the Cisco IOS configuration publications.

If you set the boot field value to a value of 0x2 through 0xF, and a valid system **boot** command is stored in the configuration file, the RPM-XF boots the system software as directed by that value. If you set the boot field to any other bit pattern, the RPM-XF uses the resulting number to form a default boot filename for booting from the network using a TFTP server. (See Table A-4.)

Table A-4 Default Boot Filenames

Filename	Bit 3	Bit 2	Bit 1	Bit 0
bootstrap mode	0	0	0	0
ROM software	0	0	0	1
cisco2-RPM-XF	0	0	1	0
cisco3-RPM-XF	0	0	1	1
cisco4-RPM-XF	0	1	0	0
cisco5-RPM-XF	0	1	0	1
cisco6-RPM-XF	0	1	1	0
cisco7-RPM-XF	0	1	1	1
cisco10-RPM-XF	1	0	0	0
cisco11-RPM-XF	1	0	0	1
cisco12-RPM-XF	1	0	1	0
cisco13-RPM-XF	1	0	1	1
cisco14-RPM-XF	1	1	0	0
cisco15-RPM-XF	1	1	0	1

Table A-4 Default Boot Filenames (continued)

Filename	Bit 3	Bit 2	Bit 1	Bit 0
cisco16-RPM-XF	1	1	1	0
cisco17-RPM-XF	1	1	1	1

In the following example, the virtual configuration register is set to boot the RPM-XF from bootflash memory and to ignore Break at the next reboot of the RPM-XF.

```
Router> enable
Password: enablepassword
Router#config terminal
Enter configuration commands, one per line. End with CTRL/Z
Router(config)#config-register 0x2102
Router(config)#no boot system
Router(config)#boot system bootflash:rpmxf-p12-mz.122-7b.bin
Router(config)#end
```

The RPM-XF creates a default boot filename as part of the automatic configuration processes. The boot filename consists of *cisco* plus the octal equivalent of the boot field number, a hyphen, and the processor type.

Note A **boot system** configuration command in the RPM-XF configuration in NVRAM overrides the default boot filename.

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret the Break key as a command to force the system into the bootstrap monitor, thereby halting normal operation. A break can be sent in the first 60 seconds while the system reboots, regardless of the configuration settings.

Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the broadcast address. (See Table A-5.)

Table A-5 Configuration Register Settings for Broadcast Address Destination

Bit 14	Bit 10	Address (<net > <host>)
Off	Off	<ones> <ones>
Off	On	<zeros> <zeros>
On	On	<net> <zeros>
On	Off	<net> <ones>

Bits 5, 11, and 12 in the configuration register determine the baud rate of the console terminal. Table A-6 shows the bit settings for the available baud rates. (The factory-set default baud rate is 9600 baud.)

Table A-6 System Console Terminal Baud Rate Settings

Baud	Bit 12	Bit 11	Bit 05
1200	1	0	0
2400	1	1	0

Table A-6 System Console Terminal Baud Rate Settings (continued)

Baud	Bit 12	Bit 11	Bit 05
4800	0	1	0
9600	0	0	0
19200	0	0	1
38400	0	1	1
57600	1	0	1
115200	1	1	1

Bit 13 determines the server response to a bootload failure. Setting bit 13 causes the server to load operating software from ROM after five unsuccessful attempts to load a boot file from the network. Clearing bit 13 causes the server to continue attempting to load a boot file from the network indefinitely. By factory default, bit 13 is set to 1.

Enabling Booting from the PXM Hard Disk

To disable break and enable booting from the PXM hard disk, use the following commands:

```
Router> enable
Password:enablepassword
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#no boot system
Router(config)#boot system x:rpmxf-p12-mz.122-7b.bin
Router(config)#end
```

Enabling Booting from Bootflash

To disable break and enable booting from bootflash, use the following commands:

```
Router> enable
Password:enablepassword
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#no boot system
Router(config)#boot system bootflash:rpmxf-p12-mz.122-7b.bin
Router(config)#end
```

Copying a Cisco IOS Image to Bootflash

You may need to copy a new Cisco IOS image to bootflash whenever a new image or maintenance release becomes available. Enter the **copy tftp bootflash** command for the copy procedure.

Perform the following steps to copy a new image to Bootflash memory from a TFTP server.

Step 1 Enter the **show bootflash** command to ensure that there is enough space available before copying a file to bootflash memory. Compare the size of the file you want to copy to the amount of available bootflash memory displayed.

Step 2 Make a backup copy of the current image.

Enter **enable** mode and then enter the **copy bootflash tftp** command. Ensure that the filename of the current image is different from the new image so that you do not overwrite it.

Step 3 Enter the **copy tftp bootflash** command to copy the new image into bootflash.

```
Router> enable
Password: enablepassword
Router# copy tftp bootflash
```

Step 4 The RPM-XF prompts you for the IP address or name of the remote TFTP server.

```
Address or name of remote host [ ]?
```

Step 5 Enter the IP address or name of the remote host.

The RPM-XF then prompts you for the name of the source file.

```
Source filename []?
```

Step 6 Enter the name of the source file. The following prompt displays.

```
Destination filename [filename]?
```

Step 7 Press **Return** to accept the default filename or enter a different filename. A message similar to the following example displays.

```
Accessing tftp://hostname/rpmxf-p12-mz.122-7b.bin...
Loading rpmxf-p12-mz.122-7b.bin from 172.16.72.1 (via FastEthernet2/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 2647996/5295104 bytes]
```

Step 8 Update your configuration to use the new software image. For example,

```
Router> enable
Password: enablepassword
Router# config terminal
Router(config)# no boot system
Router(config)# boot system bootflash:rpmxf-p12-mz.122-7b.bin
```

Press **Ctrl-Z** to exit configuration mode

Step 9 Write the new configuration to memory.

```
Router# copy running-config startup-config
```

The system displays an OK message when the configuration has been saved.

Step 10 Enter the **reload** command to reboot the RPM-XF.

Note For more information on the **copy tftp bootflash** command and other related commands, refer to the Cisco IOS command reference publications.

Recovering Boot and System Images

If your RPM-XF experiences difficulties and no longer contains a valid Cisco IOS software image in bootflash memory, the ROM Monitor contains tools to help you recover from this situation. You can recover the Cisco IOS image using one of the following ROM monitor commands:

- **xmodem**—Use this to download a new image directly over the console port on the management back card via the xmodem protocol.
- **tftpdnld**—Use this to download a new image directly from a TFTP server via one of the fast ethernet ports on the management back card.

Using the xmodem Command

Enter the **xmodem** command to establish a connection between a console and the router console port for disaster recovery, if both the boot and system images are erased from bootflash memory. The **xmodem** command syntax is the following.

xmodem [*-r* | -x | *-c* | *-y*] [*filename*]

Where:

- -r—Immediately launch the image after the download.
- -x—Use 1024 byte packets during the download.
- -c—Use CRC-16 instead of checksum during the download.
- -y—Use Y-modem (instead of X-modem) for the download.

Step 1 At the ROM Monitor prompt, issue the **xmodem -r** command to download a new Cisco IOS image into the RPM-XF and launch it. For example:

```
rommon 1> xmodem -r filename
Do not start the sending program yet...
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]: y
Ready to receive file  ...
```

Step 2 Using your terminal program, start the X-modem upload.

Step 3 After the image download is complete, the ROM monitor will launch the image.

Step 4 After the Cisco IOS image loads, squeeze the bootflash as follows:

```
Router> enable
Password: enablepassword
Router# squeeze bootflash:
```

Step 5 Copy a Cisco IOS image into bootflash.

See "Copying a Cisco IOS Image to Bootflash" section on page A-10 for additional information.

Using the tftpdnld Command

Enter the **tftpdnld** command on the fast ethernet ports on the MGX-XF-UI or MGX-XF-UI/B management back card to download a new Cisco IOS image for disaster recovery, if both the boot and system images are erased from bootflash memory. The **tftpdnld** command syntax is the following:

tftpdnld [*-r*]

Where

- -r—Immediately launch the image after the download.

The following variables are REQUIRED and must be set for the **tftpdnld** command:

- IP_ADDRESS—The IP address to use for the TFTP download.
- IP_SUBNET_MASK—The subnet mask to use for the TFTP download.
- DEFAULT_GATEWAY—The default gateway to use for the TFTP download.
- TFTP_SERVER—The IP address of the TFTP server from which to download.
- TFTP_FILE—The name of the file to download.
- TFTP_MACADDR—The MAC address to assign to the fast ethernet port for the TFTP download.

The following variables are OPTIONAL and do not have to be set for the **tftpdnld** command:

- TFTP_VERBOSE—Verbosity setting; 0 = quiet, 1 = progress(default), 2 = verbose
- TFTP_RETRY_COUNT—Retry count for ARP and TFTP (default = 7)
- TFTP_TIMEOUT—Overall time-out of TFTP operation in seconds (default = 7200)
- TFTP_CHECKSUM—Perform checksum test on downloaded image 0 = no, 1 = yes (default = 1)
- FE_PORT—0 = Ethernet 0 (default), 1 = Ethernet 1
- FE_SPEED_MOD —0 = 10Mbps half-duplex, 1 = 10Mbps full-duplex, 2 = 100Mbps half-duplex, 3 = 100Mbps full-duplex, 4 = Auto Speed, Auto Duplex (default)

Step 1 At the ROM Monitor prompt enter the **tftpdnld -r** command to download a new Cisco IOS image into the RPM-XF and launch it. For example,

```
rommon 1> IP_ADDRESS=10.1.0.1
rommon 2> IP_SUBNET_MASK=255.255.255.0
rommon 3> DEFAULT_GATEWAY=10.0.0.1
rommon 4> TFTP_SERVER=10.2.0.3
rommon 5> TFTP_FILE=rpmxf-p12-mz.122-7b.bin
rommon 6> TFTP_MACADDR=0050.3eff.f301
rommon 7> tftpdnld -r
```

Step 2 After the image download is complete, the ROM monitor will launch the image.

Step 3 After the Cisco IOS image loads, squeeze the bootflash, as follows:

```
Router> enable
Password: enablepassword
Router# squeeze bootflash:
```

Step 4 Copy a Cisco IOS image into bootflash. See "Copying a Cisco IOS Image to Bootflash" section on page A-10 for additional information.

Flash MIB Support

Network management system (NMS) can manage software images stored in bootflash using SNMP when the device supports the CISCO-FLASH-MIB. The RPM-XF supports the CISCO-FLASH-MIB in Cisco IOS Release 12.4(9)T and later. For MGX 8800/8900 multiservice switches, the NMS can query objects defined in the CISCO-FLASH-MIB through the PXM management interface or the RPM-XF management interface.

Table 0-7 summarizes the tables defined in the CISCO-FLASH MIB and identifies the objects and commands that the RPM-XF management back card supports:

Table 0-7 Supported Objects in CISCO-FLASH-MIB

CISCO-FLASH-MIB Tables	Supported Objects
ciscoFlashDeviceTable	All objects except: ciscoFlashDeviceCard
ciscoFlashChipTable	All
ciscoFlashPartitionTable	All
ciscoFlashFileTable	All
ciscoFlashPartitioningTable	Not Applicable
ciscoFlashMiscOpTable	All except: ciscoFlashMiscOpCommand—erase(1)
ciscoFlashCopyTable	All

The following traps are supported on the RPM-XF management back card:

- ciscoFlashCopyCompletionTrap
- ciscoFlashMiscOpCompletionTrap

The RPM-XF management back card does not support partitioning, insertion, or removal of Flash devices, so the following traps in the CISCO-FLASH-MIB are unused:

- ciscoFlashPartitioningCompletionTrap
- ciscoFlashDeviceChangeTrap
- ciscoFlashDeviceInsertedNotif
- ciscoFlashDeviceRemovedNotif
- ciscoFlashDeviceInsertedNotifRev1
- ciscoFlashDeviceRemovedNotifRev1