



Gigabit Route Processor Installation and Configuration Note

Product Numbers: GRP-B=, GRP=

Document Order Number: DOC-784339=

This hardware installation and configuration note describes the Gigabit Route Processor (GRP), the route processor for use in Cisco 12000 Series Routers.

Document Contents

Following are the sections in this document:

- [Important Information, page 2](#)
- [Product Overview, page 3](#)
- [Preparing for Installation, page 10](#)
- [Replacing a GRP, page 14](#)
- [GRP Boot Process Overview, page 24](#)
- [Starting the System and Observing Initial Conditions, page 24](#)
- [Verifying Interface Status, page 27](#)
- [Configuring the Ethernet Interface, page 28](#)
- [Implementing Additional Configuration and Maintenance Tasks, page 30](#)
- [Obtaining Documentation, page 53](#)
- [Documentation Feedback, page 54](#)
- [Obtaining Technical Assistance, page 54](#)
- [Obtaining Additional Publications and Information, page 55](#)



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

Copyright © 1997-2002. Cisco Systems, Inc. All rights reserved.

Important Information

This section contains information about the following hardware and software requirements:

- [Router Information](#)
- [Cisco IOS Software Requirements](#)
- [Product Overview](#)

Router Information

For hardware installation and maintenance information on Cisco 12000 Series Routers, refer to the installation and configuration guide for your router. This includes information on card slot locations and other general requirements.

Supported Platforms

The GRP operates on all Cisco 12000 series Internet Routers with the following requirements:

- Cisco 12016 and Cisco 12416—GRP plugs into slot 7 in the upper card cage. If the router is equipped with an optional, redundant GRP, it must be installed in the far left slot of the lower card cage (slot 8).
- Cisco 12410—GRP plugs into slot 9. If the router is equipped with an optional, redundant GRP, it must be installed in slot 8.
- Cisco 12406—GRP plugs into any slot; however, slot 5 is recommended. If the router is equipped with an optional, redundant GRP, it can be installed in any of the remaining five slots.
- Cisco 12404—GRP plugs into any of the five slots in the card cage, but slot 0 (zero) is the recommended slot for the first GRP. If the router is equipped with an optional, redundant GRP, it can be installed in any of the remaining slots.
- Cisco 12012—GRP plugs into slot 0 in the upper card cage. In a dual GRP system, the second GRP is located in slot 11. This is the default factory configuration and is recommended to avoid heat-related problems. The far right slot labeled *Alarm card* is reserved for the alarm card.
- Cisco 12008—GRP plugs into any slot in the upper card cage in the Cisco 12008 except the middle two slots (which are reserved for the CSC cards and labeled *CSC 0 and CSC 1*).

GRP Redundancy

When two GRPs are installed in a Cisco 12000 Series Router, one GRP is the active GRP, and the other is the backup, or standby GRP. If the active GRP fails or is removed from the system, the standby GRP detects the failure and initiates a switchover. During a switchover, the standby GRP assumes control of the router, connects with the network interfaces, and activates the local network management interface and system console.

**Note**

If your system includes redundant GRPs, both GRPs should have the same memory size. Redundancy is not supported when using a GRP and a PRP in the same chassis. Cisco strongly recommends that you avoid using mixed route processor cards to configure your router. *Refer to the Route Processor Redundancy Plus for the Cisco 12000 Series Internet Router* publication for more information on redundancy.

- Providing an auxiliary port for other external equipment (such as modems)
- Providing an IEEE 802.3, 10/100-megabits-per-second (Mbps) Ethernet port for Telnet functionality
- Running routing protocols
- Building and distributing routing tables to the line cards
- Providing general system maintenance functions
- Communicating with the line cards either through the switch fabric or through the maintenance bus (MBus)

The MBus connection allows the GRP to download a system bootstrap image, collect or load diagnostic information, and perform general, internal system maintenance operations. The switch fabric connection is the main data path for routing table distribution as well as for packets that are sent between line cards and the GRP.

GRP Components

The GRP contains the following components:

- RISC processor—IDT R5000 Reduced Instruction Set Computing (RISC) processor used for the CPU. The CPU runs at an external bus clock speed of 100 MHz and an internal clock speed of 200 MHz.
- DRAM—Up to 512 megabytes (MB) of parity-protected, extended data output (EDO) dynamic random-access memory (DRAM) on two 60-nanosecond (ns), dual in-line memory modules (DIMMs). 128 MB of DRAM is the minimum shipping configuration for the GRP.



Note GRP route memory configurations of 512 MB are only compatible with Product Number GRP-B=. In addition, Cisco IOS Release 12.0(19)S or 12.0(19)ST or later and ROMMON Release 11.2 (181) or later are also required.

- SRAM—512 kilobytes (KB) of static random-access memory (SRAM) for secondary CPU cache memory functions. (SRAM is *not* user configurable or field upgradeable.)
- NVRAM—512 KB of nonvolatile RAM (NVRAM). (NVRAM is *not* user configurable or field upgradeable.)
- Memory—Most of the additional memory components used by the system, including onboard Flash memory and up to two Personal Computer Memory Card International Association (PCMCIA)-based Flash memory cards and advanced technology attachment (ATA) Flash disks.
- Sensors—Air-temperature sensors for environmental monitoring.

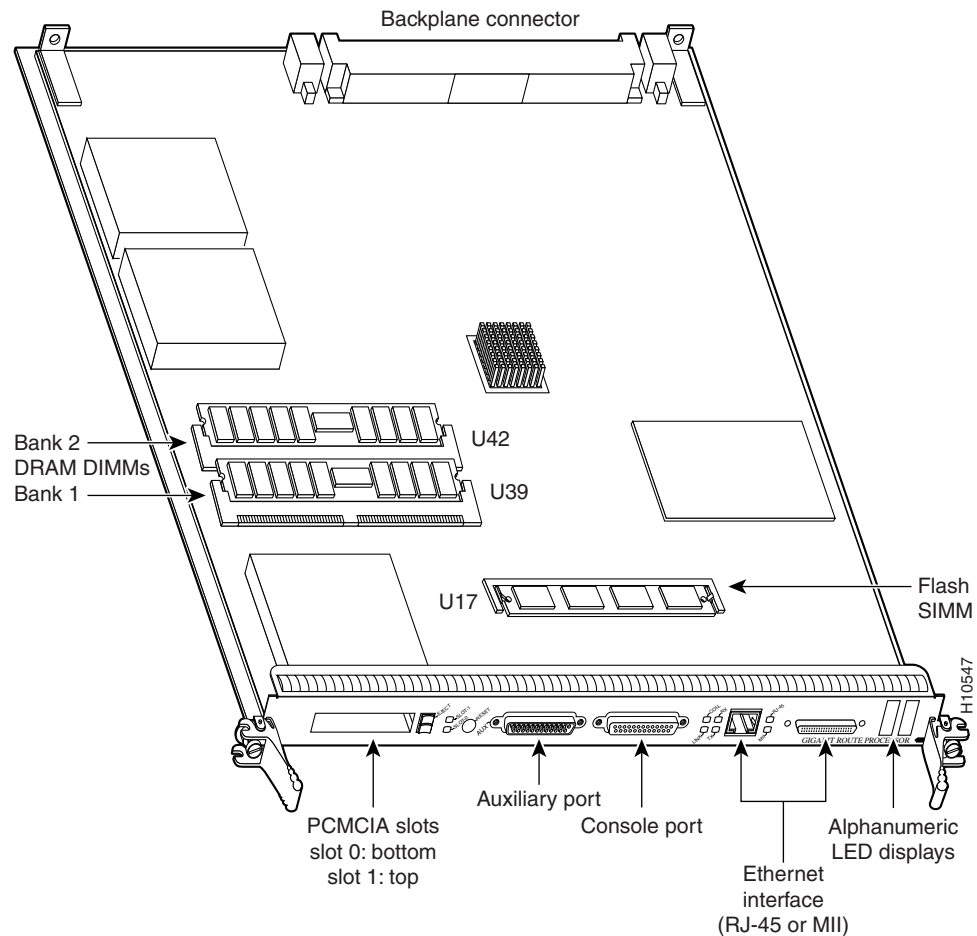
Cisco IOS Software

The Cisco IOS software images that run the Cisco 12000 Series Router system reside in Flash memory, which is located on the GRP in the form of a single in-line memory module (SIMM), and on up to two Flash cards (called Flash memory cards or Flash disks), which insert into the two slots (slot 0 and slot 1) on the front of the GRP. (See [Figure 2](#).)



Note

Figure 2 GRP (Horizontal Orientation)



Note

The onboard Flash memory (called bootflash) contains the Cisco IOS software boot image, and a Flash memory card or Flash disk contains the Cisco IOS software image.

Storing the Cisco IOS images in Flash memory enables you to download and boot from upgraded Cisco IOS software images remotely or from software images that reside in GRP Flash memory.

The Cisco 12000 Series Router system supports downloadable system software for most Cisco IOS software upgrades, which enables you to remotely download, store, and boot from a new Cisco IOS software image. The Cisco IOS software runs from within GRP DRAM.

For specific Cisco IOS software requirements for the GRP, see the [“Cisco IOS Software Requirements” section on page 3](#).

Memory Components

Figure 2 shows the locations of the various types of memory used on the GRP. GRP memory component types are presented in the following sections:

- DRAM
- SRAM
- NVRAM
- Flash Memory

Their functions are presented in Table 1.

Table 1 GRP Memory Components

Type	Size	Quantity	Description	Location
DRAM	64 ¹ to 512 MB ²	1 or 2	64-, 128-, or 256-MB DIMMs (based on the required DRAM configuration) for main Cisco IOS software functions (default configuration is 128 MB ³)	U39 (bank 1) U42 (bank 2)
SRAM ⁴	512 KB (fixed)	—	SRAM for secondary CPU cache memory functions	—
NVRAM ⁵	512 KB (fixed)	1	NVRAM for system configuration files	—
Flash memory	8 MB SIMM ⁶	1	Contains Cisco IOS software images, system configuration files, and other user-defined files on the GRP	U17
—	Flash memory ⁷	1 to 2	Contains Cisco IOS software images, system configuration files, and other user-defined files on up to two Flash memory cards or Flash disks ⁸	Flash disk slot 0 and slot 1
Flash boot ROM	512 KB	1	Flash EPROM for the ROM monitor program boot image	—

1. 64 MB of DRAM serves as a replacement for any DRAM DIMM slot on a minimum configuration of 128 MB (both slots populated) for the GRP.
2. GRP route memory configurations of 512 MB are only compatible with Product Number GRP-B=. Cisco IOS Release 12.0(19)S or 12.0(19)ST or later and ROMMON Release 11.2 (181) or later are also required.
3. Default DRAM configuration is 128 MB. Bank 1 (U39) must be populated first. You can use one or both banks to configure DRAM up to 512 MB.
4. SRAM is not user configurable or field upgradeable.
5. NVRAM is not user configurable or field upgradeable.
6. SIMM socket is wired for Cisco's own design and does not accept industry-standard 80-pin Flash SIMMs.
7. Cisco IOS Release 12.0(17)S or 12.0(17)ST or later is required, along with the corresponding boot images, for the GRP to function with a Flash disk.
8. Linear Flash memory cards and ATA Flash disks can be used in either (or both) Flash card slot(s).

DRAM

DRAM stores routing tables, protocols, and network accounting applications, and runs the Cisco IOS software. The standard (default) GRP configuration is 128 MB of extended data output (EDO) DRAM, with up to 512 MB available through DIMM upgrades.



Note

GRP route memory configurations of 512 MB are only compatible with Product Number GRP-B=. In addition, Cisco IOS Release 12.0(19)S or 12.0(19)ST or later and ROMMON Release 11.2 (181) or later are also required.

**Caution**

To prevent memory problems, DRAM DIMMs must be +3.3VDC, 60-nanosecond (ns) EDO devices. Do not attempt to install other devices in the DIMM sockets. Cisco recommends that you use Cisco-approved memory options. (See [Table 14](#) on page 49.)

The following DRAM upgrade kits for the GRP and line cards are listed by product number:

- 64-MB DRAM upgrade kit (one 64-MB DIMM)—MEM-GRP/LC-64=
- 128-MB DRAM upgrade kit (one 128-MB DIMM)—MEM-GRP/LC-128=
- 256-MB DRAM upgrade kit (two 128-MB DIMMs)—MEM-GRP/LC-256=

The following DRAM upgrade kits for Product Number GRP-B= are available (listed by product number):

- 256-MB DRAM upgrade kit (one 256-MB DIMM)—MEM-GRP-256=
- 512-MB DRAM upgrade kit (two 256-MB DIMMs)—MEM-GRP-512-UPG=

These kits are available only for Product Number GRP-B=. They are not compatible with any other Cisco product. See [Table 14](#) for all requirements related to the 512-MB memory upgrade.

**Note**

MEM-GRP/LC-64= can be used to replace bank 1 or bank 2 in the 128-MB default configuration on the GRP line card. Cisco does not recommend using a 64-MB configuration on this card.

SRAM

SRAM provides secondary CPU cache memory. The standard GRP configuration is 512 KB. Its principal function is to act as a staging area for routing table updates information to and from the line cards. SRAM is not user configurable or field upgradeable.

NVRAM

System configuration files, software configuration register settings, and environmental monitoring logs are contained in the 512-KB NVRAM, which is backed up with built-in lithium batteries that retain the contents for a minimum of 5 years. NVRAM is *not* user configurable or field-upgradeable.

Flash Memory

Both the onboard and Flash card-based Flash memory allow you to remotely load and store multiple Cisco IOS software and microcode images. You can download a new image over the network or from a local server and then add the new image to Flash memory or replace the existing files. You can then boot the routers either manually or automatically from any of the stored images.

Flash memory also functions as a Trivial File Transfer Protocol (TFTP) server to allow other servers to boot remotely from stored images or to copy them into their own Flash memory. The onboard Flash memory (called *bootflash*) contains the Cisco IOS software boot image, and the Flash memory card or Flash disk contains the Cisco IOS software image.

System Status LEDs

The two types of system status LEDs used on the GRP.

- [Status LEDs](#)
- [Display LEDs](#)

Status LEDs

The GRP has the following eight status LEDs:

- 2 PCMCIA activity LEDs (one LED per PCMCIA slot)—Each LED goes on when its PCMCIA slot is accessed. The LEDs receive power from the switched slot voltage.
- 4 RJ-45 Ethernet port LEDs—These LEDs are used in conjunction with the RJ-45 Ethernet connector. When the MII Ethernet port is in use, the LEDs are disabled. The LEDs indicate link activity (LINK), collision detection (COLL), data transmission (TX), and data reception (RX).
- 2 RJ-45 or MII Ethernet port selection LEDs—These two LEDs, when on, identify which of the two Ethernet connections you selected. When the RJ-45 port is selected, its LED is on, and the MII LED is off. When the MII port is selected, its LED is on, and the RJ-45 LED is off.

Display LEDs

The alphanumeric display LEDs are organized as two rows of four characters each. The display content is controlled by the MBus software of the GRP. Both rows of the display are powered by the MBus module.

These alphanumeric display LEDs provide system status messages that are displayed during the boot process and after the boot process is completed.

During the boot process, the display LEDs are controlled directly by the MBus. After the boot process, they are controlled by the Cisco IOS software (via the MBus), and display messages designated by the Cisco IOS software.

The LED displays indicate the following:

- Status of the GRP
- System error messages
- User-defined status/error messages

Soft Reset Switch

A soft reset switch provides a reset to the R5000 software on the GRP. You access the soft reset switch through a small opening in the GRP faceplate. To depress the switch, insert a paperclip or a similar object into the opening.



Caution

To prevent system problems or loss of data, use the soft reset switch *only* on the advice of Cisco service personnel.

Flash Card Slots

The GRP includes two Flash card slots. Either slot can support an ATA Flash disk or a linear Flash memory card.



Note

The GRP only supports +5VDC Flash card devices. It does *not* support +3.3VDC Flash card devices.

All combinations of different Flash card devices are supported by the GRP. You can use ATA Flash disks, linear Flash memory cards, or a combination of the two. Each slot has an ejector button for ejecting a card from the slot.



Note

Linear Flash memory cards may not have the capacity to meet the requirements of your configuration. However, they can be used for emergency file recovery applications.

Asynchronous Serial Ports

Two asynchronous serial ports on the GRP, the console and auxiliary ports, allow you to connect external serial devices to monitor and manage the system. The console port is an Electronic Industries Association/Telecommunications Industry Association (EIA/TIA)-232 receptacle (female) that provides a data circuit-terminating equipment (DCE) interface for connecting a console terminal.



Note

EIA/TIA-232 was formerly RS-232.

The auxiliary port is an EIA/TIA-232 plug (male) that provides a data terminal equipment (DTE) interface; the auxiliary port supports flow control and is often used to connect a modem, a channel service unit (CSU), or other optional equipment for Telnet management.

Ethernet Port

The GRP has one Ethernet port available, using one of the following connection types:

- RJ-45 receptacle—8-pin RJ-45 receptacle for either IEEE 802.3 10BASE-T (10 Mbps) or IEEE 802.3u 100BASE-TX (100 Mbps) connections.
- MII receptacle—40-pin media independent interface (MII) receptacle that provides additional flexibility in Ethernet connections. The pinout of this standard 40-pin receptacle is defined by the IEEE 802.3u standard.



Note

The RJ-45 and MII receptacles on the GRP represent two physical connection options for *one* Ethernet interface; therefore, you can use *either* the RJ-45 connection *or* the MII connection, but not both simultaneously.

The transmission speed of the Ethernet port is auto-sensing and is determined by the network to which the Ethernet interface is connected; it is not user configurable. At the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth that is less than 100 Mbps; a maximum usable bandwidth of approximately 20 Mbps can be expected if you use either the MII or RJ-45 connection.

Preparing for Installation

Installation preparation is presented in the following sections:

- [Safety Guidelines](#)
- [Translated Safety Warnings and Agency Approvals](#)
- [Electromagnetic Compatibility Regulatory Statements](#)
- [Preventing Electrostatic Discharge](#)
- [Working with Electrical Equipment](#)
- [Required Tools and Parts](#)

Safety Guidelines

Before you perform any procedure in this publication, review the safety guidelines in this section to avoid injuring yourself or damaging the equipment.

The following guidelines are for your safety and to protect the equipment. The guidelines do not include all hazards. Be alert.

**Note**

Review the safety warnings listed in the *Regulatory Compliance and Safety Information for Cisco 12000 Series Internet Routers* publication (Document Number 78-4347-xx) for your router before installing, configuring, or maintaining the GRP.

- Keep the work area clear and dust free during and after installation. Do not allow dirt or debris to enter into any components.
- Do not wear loose clothing, jewelry, or other items that could get caught in the router while working with the GRP.
- The GRP operates safely when it is used in accordance with its specifications and product usage instructions.
- Review all safety and ESD-prevention guidelines to help you to avoid injury or damage to the equipment.
- Ensure that your equipment configuration meets the minimum requirements for the upgrade or replacement you will perform and that you have all the parts and tools you need.
- If you plan to replace a GRP, back up your current configuration file to a remote server or to Flash memory before you remove the GRP. This prevents you from having to reenter all your current configuration information manually. To back up the file, copy your configuration file to a Flash disk or access a remote server.

Translated Safety Warnings and Agency Approvals

The complete list of safety warnings and agency approvals for the PRP is available in the *Regulatory Compliance and Safety Information for Cisco 12000 Series Internet Routers* publication (Document Number 78-4347-xx).

Electromagnetic Compatibility Regulatory Statements

FCC Class A Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulation and you may be required to correct any interference to radio or television communication at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

CISPR 22

This apparatus complies with EN55022 Class B radiated and conducted emissions requirements.

Canada

English Statement of Compliance

This class A digital apparatus complies with Canadian ICES-003.

French Statement of Compliance

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Europe (EU)

This apparatus complies with EN55022 Class A and EN55024 standards when used as ITE/TTE equipment, and EN 300 386-2 (EN55022 class B with shielded CAT5 Ethernet cable, non-central office equipment) for Telecommunications Network Equipment (TNE).

Class A Notice for Hungary

Warning This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelem Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfelelően kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelő kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelő speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Class A Notice for Taiwan and Other Traditional Chinese Markets

Warning This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures. Statement 257

警告 這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Class A Notice for Japan

Warning This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions. Statement 191

警告 これは、情報処理装置等電波障害自主規制協議会（VCCI）の規定に基づくクラスA装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を取るようにより要求されることがあります。

Class A Notice for Korea

Warning This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type. Statement 294

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이
오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약
잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Preventing Electrostatic Discharge

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Electromagnetic interference (EMI) shielding is an integral component of the GRP. Cisco recommends using a ESD-preventive strap whenever you are handling a router or one of its components.

Following are guidelines for preventing ESD damage:

- Always use an ESD-preventive wrist or ankle strap and ensure that it makes good skin contact. Connect the equipment end of the connection cord to an ESD connection socket on the router or to bare metal on the router chassis.
- Handle the GRP by the card carrier and by the left-side spring-loaded screw (horizontal view). Avoid touching board components or connector pins.
- Place a removed GRP board-side-up on an antistatic surface or in a static shielding bag. If you plan to return the component to the factory, immediately place it in a static shielding bag.
- Avoid contact between the GRP and clothing or jewelry. The wrist strap protects the board only from ESD voltages on the body; ESD voltages on clothing or jewelry can still cause damage.

Working with Electrical Equipment

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedure requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before moving a chassis.
- Do not work alone when potentially hazardous conditions exist; never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Required Tools and Parts

You need the following tools and parts to remove and replace a GRP. If you need additional equipment, contact a Cisco customer service representative for ordering information.

- 3/16-inch flat-blade screwdriver for the captive installation screws that secure the GRP in its slot.
- ESD-prevention equipment or the disposable ESD-preventive wrist strap included with all spares and upgrade kits.
- Antistatic mat, foam pad, or bag for the removed GRP. Place the removed GRP into an antistatic bag if you plan to return it to the factory, or on an antistatic mat or foam if you are replacing components and will reinstall the GRP.

Replacing a GRP

The following sections describe the procedures for replacing a GRP in your system.

Before beginning the procedures, verify that your system meets the minimum requirements as described in the [“Preparing for Installation” section on page 10](#).

When your system meets minimum requirements, proceed to the [“Removing a GRP” section on page 14](#) for instructions on removing the GRP, and then to the [“Installing a GRP” section on page 17](#) for reinstallation instructions.

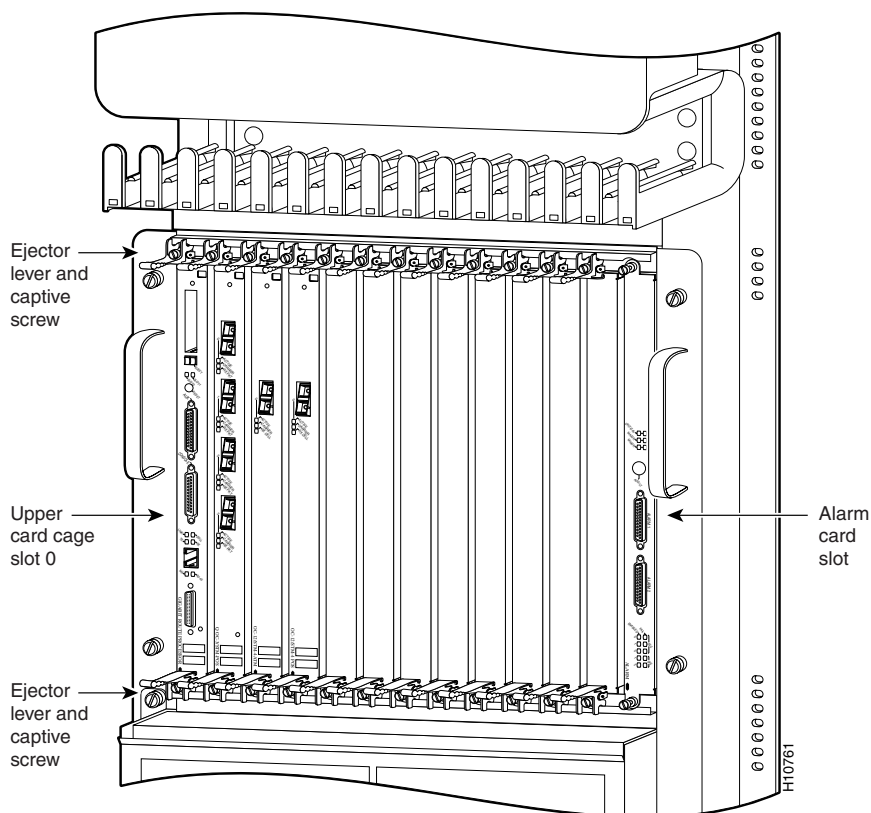
**Caution**

We recommend that you do not remove a GRP while the system is operating. Removing the installed GRP from a system while the system is operating will cause the system to stop forwarding packets and might cause the system to cease network operation.

Removing a GRP

When you remove a GRP from a slot, be sure to use the ejector levers, which help to ensure that the GRP is fully dislodged from the backplane connector. (See [Figure 3](#).)

Figure 3 GRP Ejector Levers, Captive Installation Screws, and Upper Card Cage Slots (Cisco 12012 Shown)



Caution

A GRP that is only partially removed from the backplane can halt the system.

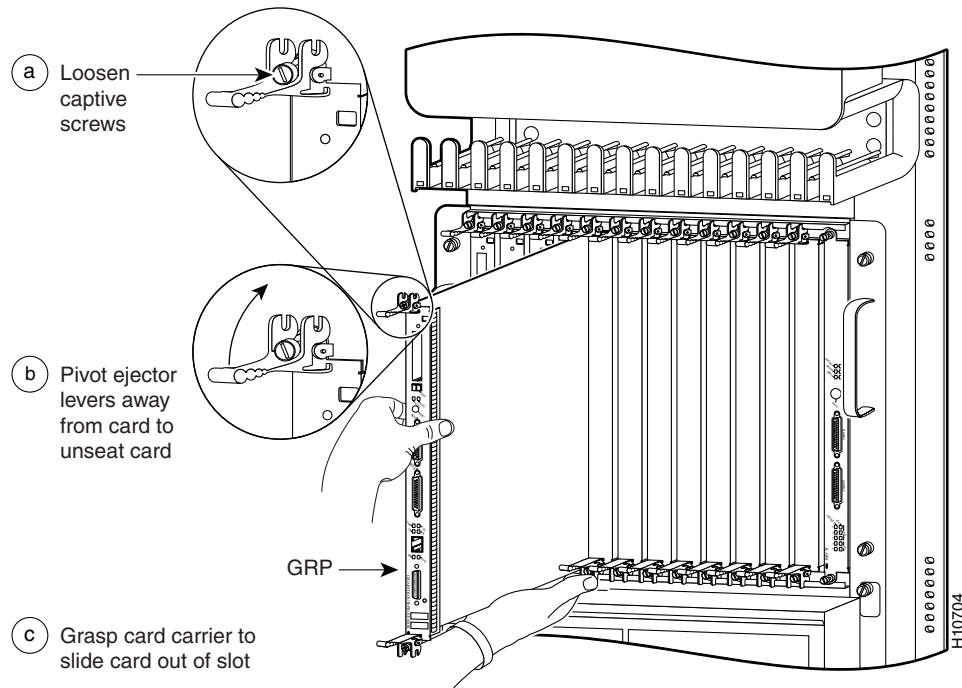


Caution

Before you replace the GRP, back up the running configuration to a Trivial File Transfer Protocol (TFTP) file server or an installed Flash memory card or Flash disk so that you can retrieve it later. If the configuration is not saved, the entire configuration will be lost inside the NVRAM on the removed GRP, and you will have to reenter the entire configuration manually. For instructions on how to save the configuration file, see the “[Copying Files to Flash Memory](#)” section on page 41. This procedure is not necessary if you are temporarily removing a GRP; lithium batteries will retain the configuration in memory until you replace the GRP in the system.

Figure 4 shows the ejector levers.

Figure 4 Ejector Levers and Captive Installation Screw (Cisco 12012 shown)



To remove a GRP, follow these steps:

-
- Step 1** Turn off system power.
 - Step 2** If you are replacing the GRP in a system with one GRP, copy the currently running configuration file to a TFTP server or Flash memory so that you can retrieve it later. (See the [“Copying Files to Flash Memory”](#) section on page 41.)
 - Step 3** Attach an ESD-preventive wrist strap to yourself and to one of the two ESD connection sockets located on the front edges of the upper card cage (Cisco 12012, Cisco 12016, or Cisco 12416); to the ESD connection socket located on the lower left edge of the upper card cage (Cisco 12008); or to bare metal on the frame.

If you are replacing a GRP, disconnect any devices that are attached to the console or auxiliary ports. If you are removing a GRP for maintenance and will reinstall the same one, you can leave the devices attached, provided that doing so will not strain the cables.
 - Step 4** Using a 3/16-inch flat-blade screwdriver, loosen the two captive screws on the ends of the GRP. (See [Figure 4a.](#))
 - Step 5** Place your thumbs on the ends of each of the ejector levers and simultaneously pull them both away from the GRP faceplate (in the direction shown in [Figure 4b](#)) to release the GRP from the upper card cage slot and to dislodge the GRP edge connector from the backplane.
 - Step 6** Grasp the GRP faceplate with one hand and pull the GRP straight out of the slot, keeping your other hand under the GRP to guide it. (See [Figure 4.](#)) Keep the GRP edge connector parallel to the backplane.


Caution

Avoid touching the GRP printed circuit board, components, or any edge connector pins.

- Step 7** Place the removed GRP on an antistatic mat or foam. If you plan to return the GRP to the factory, immediately place it in an antistatic bag to prevent ESD damage.

Installing a GRP

When you install a GRP, be sure to use the ejector levers, which help to ensure that the GRP is fully inserted in the backplane connector. (See [Figure 3](#).) When you simultaneously push the ejector levers inward (toward the center of the GRP), the ejector levers push the GRP into the slot and ensure that the GRP backplane connector is fully seated in the backplane.



Caution

A GRP that is only partially connected to the backplane can halt the system.

Use the following procedure to install a GRP:

- Step 1** Use an ESD-preventive wrist or ankle strap and follow its instructions for use.
- Step 2** Grasp the GRP faceplate with one hand and place your other hand under the carrier to support and guide it into an upper card cage slot. (See [Figure 4](#).)



Caution

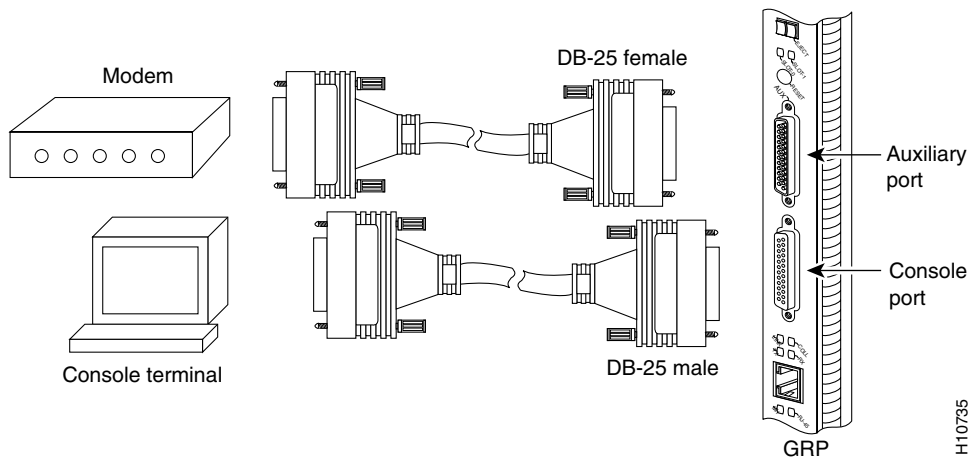
Avoid touching the GRP printed circuit board, components, or any edge connector pins.

- Step 3** Place the bus-connector edge of the GRP in the appropriate slot and align the notches along the edge of the carrier with the grooves at the top and bottom of the slot.
- Step 4** While keeping the GRP edge connector parallel to the backplane, carefully slide the carrier into the slot until the GRP faceplate makes contact with the ejector levers, then *stop*.
- Step 5** Using the thumb and forefinger of each hand to pinch each ejector lever, simultaneously push both ejectors toward the center of the GRP faceplate until they are perpendicular to the GRP faceplate. (See [Figure 4a](#).)
- Step 6** Using a 3/16-inch flat-blade screwdriver, tighten the captive screws on the ends of the GRP. The captive screws prevent the GRP from becoming partially dislodged from the backplane and ensure proper EMI shielding. (These captive screws must be tightened to meet EMI specifications.)
- Step 7** If you disconnected the console terminal to remove the GRP, or if you are installing a new GRP, connect the console terminal to the console port. (See the [“Connecting to the Console Port”](#) section on [page 18](#).)
- Step 8** Ensure that the console terminal is turned on.
- Step 9** Turn on system power.
- Step 10** Attach the network end of your RJ-45 or MII cable to your transceiver, switch, hub, repeater, DTE, or other external equipment. Be sure to use the appropriate strain relief on cable connections.

Connecting to the Console Port

The system console port on the GRP is a DCE DB-25 receptacle for connecting a data terminal, which you must configure. The console port is labeled *Console*, as shown in Figure 5. Before connecting the console port, check your terminal's documentation to determine the baud rate of the terminal you plan to use. The baud rate of the terminal must match the default baud rate (9600 baud). Set up the terminal as follows: 9600 baud, 8 data bits, no parity, and 2 stop bits (9600, 8N2). The console port requires a straight-through EIA/TIA-232 cable. Use the console cable provided to connect the terminal to the console port on the GRP.

Figure 5 Console and Auxiliary Port Connections



Note

The console and auxiliary ports are both asynchronous serial ports; any devices connected to these ports must be capable of asynchronous transmission. (Asynchronous is the most common type of serial device; for example, most modems are asynchronous devices.)

The console port on the GRP is an EIA/TIA-232, DCE DB-25 receptacle. Both Data Set Ready (DSR) and Data Carrier Detect (DCD) signals are active when the system is running. The console port does not support modem control or hardware flow control. Table 2 lists the pinout for this port.

Table 2 Console Port Pinout

Console Port Pin	Signal	Direction	Description
1	GND	—	Signal Ground
2	TxD	←	Transmit Data (from DTE)
3	RxD	→	Receive Data (to DTE)
6	DSR	→	Data Set Ready (always on)
7	GND	—	Signal Ground
8	DCD	→	Data Carrier Detect (always on)

Connecting to the Auxiliary Port

The auxiliary port on the GRP is an EIA/TIA-232 DTE, DB-25 plug for connecting a modem or other DCE device (such as a CSU/DSU or another router) to the router. The port is labeled *Auxiliary*. An example of a modem connection is shown in [Figure 5](#). The asynchronous auxiliary port supports hardware flow control and modem control. [Table 3](#) lists the pinout for this port.

Table 3 Auxiliary Port Pinout

Auxiliary Port Pin	Signal	Direction	Description
2	TxD	—>	Transmit Data (to DCE)
3	RxD	<—	Receive Data (from DCE)
4	RTS	—>	Request To Send (used for hardware flow control)
5	CTS	<—	Clear To Send (used for hardware flow control)
6	DSR	<—	Data Set Ready
7	GND	—	Signal Ground
8	CD	<—	Carrier Detect (used for modem control)
20	DTR	—>	Data Terminal Ready (used for modem control only)

Connecting to the Ethernet Port

Information you need to make connections to the Ethernet port on your GRP is presented in the following sections:

- [Ethernet Interface Receptacles, Cables, and Pinouts](#)
- [Ethernet Interface Cable Connection Procedure](#)

Ethernet Interface Receptacles, Cables, and Pinouts

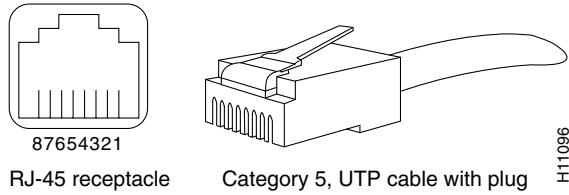
The two Ethernet interface receptacles on the GRP are a single media independent interface (MII), 40-pin, D-shell type receptacle, and a single RJ-45 receptacle. The RJ-45 receptacle provides a media dependent interface (MDI) Ethernet port. You can use either one or the other, but not both at the same time.

Each connection supports IEEE 802.3 and IEEE 802.3u interfaces compliant with the 10BASE-T and 100BASE-TX standards. The transmission speed of the Ethernet port is auto-sensing and is determined by the network to which the Ethernet interface is connected; transmission speed is not user configurable.

RJ-45 Connections

[Figure 6](#) shows the GRP RJ-45 receptacle and cable connectors. The RJ-45 connection does not require an external transceiver. The RJ-45 connection requires Category 5 unshielded twisted-pair (UTP) cables, which are not available from Cisco Systems, but are available from commercial cable vendors. [Table 4](#) lists the pinout for the RJ-45 receptacle.

Figure 6 RJ-45 Receptacle and Plug (Horizontal Orientation)



Warning

The ports labeled Ethernet, 10BASE-T, Token Ring, Console, and AUX are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the basic rate interface (BRI) circuits are treated like telephone-network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.

Table 4 RJ-45 Receptacle Pinout

Pin	Description
1	TxD+
2	TxD-
3	RxD+
4	Termination Network
5	Termination Network
6	RxD-
7	Termination Network
8	Termination Network

Depending on your RJ-45 cabling requirements, use the cable pinouts shown in [Figure 7](#) or [Figure 8](#).

Figure 7 Straight-Through Cable Pinout (Connecting MDI Ethernet Port to MDI-X Wiring)

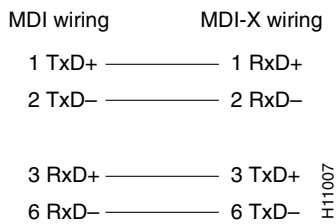
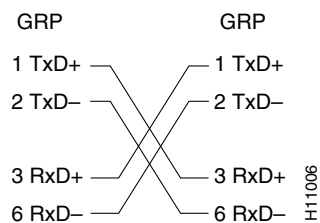


Figure 8 Crossover Cable Pinout (for Connecting Two GRPs)



MII Connections

The MII connection requires an external physical sublayer (PHY) and an external transceiver. Depending on the type of media you use between the MII connection on the GRP and your switch or hub, the network side of your 100BASE-T transceiver should be appropriately equipped—with SC-type or ST-type connectors (for optical fiber), BNC connectors, and so forth. Figure 9 shows the pin orientation of the female MII receptacle on GRP.

The MII receptacle uses two screw-type locks, called *jackscrews* (see Figure 9), to secure the cable or transceiver to the MII port. MII cables and transceivers have knurled thumbscrews (screws that you can tighten with your fingers) that you fasten to the jackscrews on the GRP's MII connector. Use the jackscrews to provide strain relief for your MII cable. (The RJ-45 modular plug has strain relief functionality incorporated into the design of its standard plastic connector.)

Figure 9 MII Receptacle (Horizontal Orientation)

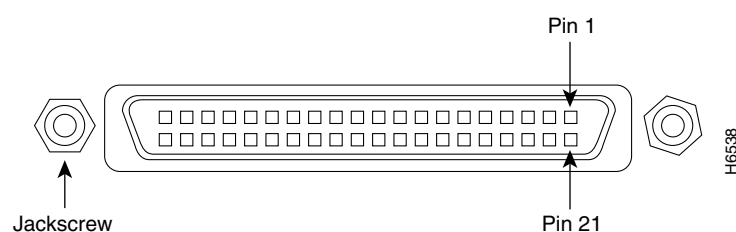


Table 5 lists the MII connector pinout and signals. MII cables and transceivers are not available from Cisco Systems, but are available commercially.

Table 5 MII Receptacle Pinout

Pin ¹	Signal	Input	Output	Input/Output	Description
14 to 17	TxD	—	Yes	—	Transmit Data
12	Tx_CLK	Yes	—	—	Transmit Clock ²
11	Tx_ER	—	Yes	—	Transmit Error
13	Tx_EN	—	Yes	—	Transmit Enable
3	MDC	—	Yes	—	MII Data Clock
4 to 7	RxD	Yes	—	—	Receive Data
9	Rx_CLK	Yes	—	—	Receive Clock
10	Rx_ER	Yes	—	—	Receive Error
8	Rx_DV	Yes	—	—	Receive Data Valid
18	COL	Yes	—	—	Collision
19	CRS	Yes	—	—	Carrier Sense
2	MDIO	—	—	Yes	MII Data Input/Output
22 to 39	GND	—	—	—	Common ground
1, 20, 21, 40	V	—	—	—	+5.0 VDC

1. Any pins not indicated are not used.

2. The signals Tx_CLK and Rx_CLK are generated by the external transceiver.

Table 6 lists the cabling specifications for 100-Mbps transmission over unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cables.



Note

At the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth that is less than 100 Mbps; a maximum usable bandwidth of approximately 20 Mbps can be expected if you use either the MII or RJ-45 connection. Transmission speed is determined by the network to which the Ethernet interface is connected and is not user configurable.

Table 6 Specifications and Connection Limits for 100-Mbps Transmission

Parameter	RJ-45	MII
Cable specification	Category 5 ¹ UTP ² , 22 to 24 AWG ³	Category 3, 4, or 5, 150-ohm UTP or STP, or multimode optical fiber
Cable length (max)	—	1.64 ft (0.5 m) (MII-to-MII cable ⁴)
Segment length (max)	328 feet (100 m) for 100BASE-TX	3.28 ft (1 m) ⁵ or 1312 ft (400 m) for 100BASE-FX
Network length (max)	656 feet (200 m) ⁵ (with 1 repeater)	—

1. EIA/TIA-568 or EIA-TIA-568 TSB-36-compliant.
2. Cisco Systems does not supply Category 5 UTP RJ-45 or 150-ohm STP MII cables or MII transceivers; these items are available commercially.
3. AWG = American Wire Gauge. This gauge is specified by the EIA/TIA-568 standard.
4. This is the cable between the MII port on the GRP and the appropriate transceiver.
5. This length is specifically between any two stations on a repeated segment.

Table 7 lists IEEE 802.3u physical characteristics for 100BASE-TX.

Table 7 IEEE 802.3u Physical Characteristics

Parameter	100BASE-TX
Data rate (Mbps)	100
Signaling method	Baseband
Maximum segment length	100 m between DTE ¹ and repeaters
Media	Category 5 UTP (for RJ-45) or MII
Topology	Star/Hub

1. DTE = data terminal equipment.

Ethernet Interface Cable Connection Procedure

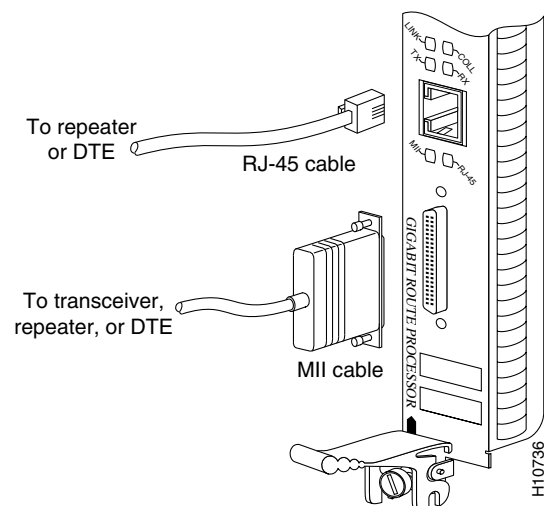
The RJ-45 and MII receptacles on the GRP represent two physical connection options for *one* Ethernet interface; therefore, you can use *either* the RJ-45 connection or the MII connection, but not both simultaneously. RJ-45 and MII cables are not available from Cisco Systems; they are available from outside commercial cable vendors.

Use the following procedure to connect cables to the GRP’s Ethernet interface:

- MII connections—Attach an MII cable directly to the MII receptacle on the GRP or attach a 100BASE-T transceiver with the media appropriate to your application to the MII port on the GRP. (See [Figure 10](#).) Be sure to use the appropriate strain relief on cable connections.
- RJ-45 connections—Attach the Category 5 UTP cable directly to the RJ-45 receptacle on the GRP. (See [Figure 10](#).)

The Ethernet interface on the GRP is an end station device, not a repeater; therefore, you must connect the Ethernet interface to a repeater or hub.

Figure 10 Connecting MII or RJ-45 Cables to GRP (Vertical Orientation)



Caution

To prevent problems on your system and network, do not simultaneously connect RJ-45 and MII cables to a single GRP Ethernet interface. On a single GRP, only one Ethernet connection can be used at a time. Only connect cables that comply with EIA/TIA-568 standards. (Refer to [Table 6](#) and [Table 7](#) for cable recommendations and specifications.)



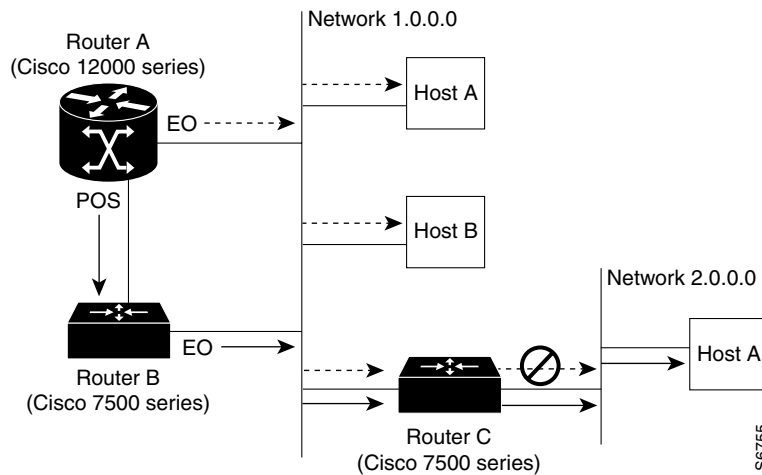
Caution

An Ethernet port is used primarily as a Telnet port into the Cisco 12000 Series Router, or for booting or accessing Cisco IOS software images over a network to which an Ethernet port is directly connected. Cisco Express Forwarding (CEF) functions are switched off by default for security reasons. Cisco strongly cautions you to consider the security implications of switching on CEF routing functions on these ports.

[Figure 11](#) shows an example of the functionality of the Ethernet port. In this example, you cannot access Network 2.0.0.0 via the Ethernet port (E0) on the GRP in Router A; you can only access the hosts and Router C, which are in Network 1.0.0.0. (See dotted arrows in [Figure 11](#).)

To access Network 2.0.0.0 from Router A, you must use an interface port on one of your line cards (in this example, a Packet-over-SONET (POS) line card in Router A) to go through Router B, through Router C, and into Network 2.0.0.0. (See solid arrows in [Figure 11](#).)

Figure 11 Using the Ethernet Port on the GRP



GRP Boot Process Overview

The following sequence describes a typical GRP boot process:

1. System power is turned on.
2. MBus module receives +5 VDC and starts executing MBus software.
3. GRP determines the system configuration by sending a message over the MBus requesting all installed devices to identify themselves. The return response provides slot number, and card and component type. The GRP, line cards, and CSCs are then powered up.
4. GRP power-on-reset logic delay, which allows power and both local and CSC clocks to stabilize.
5. After the power-on reset is released, the GRP begins to execute the ROM monitor software.
6. If the ROM monitor is configured to autoboot, it loads and boots the Cisco IOS software.

or

If the ROM monitor is not configured to autoboot, you must enter the appropriate **b** command at the ROM monitor prompt (`rommon>`) to boot the Cisco IOS software.

7. When the Cisco IOS software boots, it polls all other cards in the system and powers them up, loading their Cisco IOS software as needed.
8. GRP waits for all other cards to finish their boot processes.

Starting the System and Observing Initial Conditions

This section describes the initial system startup processes and procedures.

Use the following procedure to start your system:

-
- Step 1** Turn on each installed power supply by turning its system power switch to the on (I) position.

For AC-input power supplies, the green AC OK LED should go on. For DC-input power supplies, the green input OK LED should go on. For both types of power supplies, the output fail LED should be off.

- Step 2** Listen for the system blower modules or fan trays in the router; you should immediately hear them operating. In a noisy environment, place your hand in front of the exhaust vents to verify that the blower modules are operating.
- Step 3** During the GRP boot process, observe the GRP alphanumeric display LEDs, which are located at one end of the GRP, near the ejector lever. (See [Figure 12](#).)

The 4-digit displays show system messages and displays a sequence similar to that shown in [Table 8](#).

Figure 12 GRP Alphanumeric Display LEDs (Front Panel View)

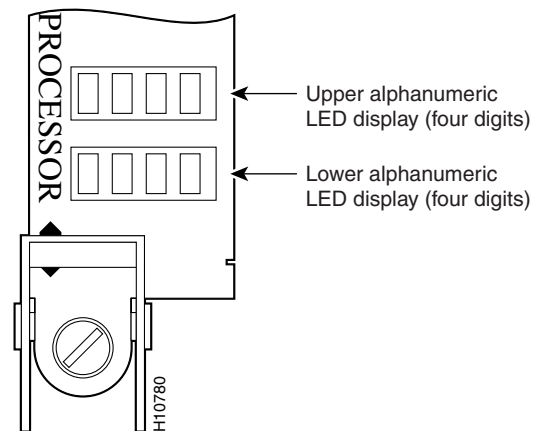


Table 8 GRP Alphanumeric Display LED Sequences

LED Display	Description
MRAM <i>nnnn</i>	GRP microcode loads into MBus random-access memory (RAM); where <i>nnnn</i> is the microcode version. For example, Microcode Version 1.17 displays as <i>0117</i> . ¹
MSTR RP	This GRP is enabled and recognized by the system.

1. The version of microcode running on your GRP might be different.

Step 4 During the line card boot process, which occurs immediately after the GRP boots, observe the alphanumeric display LEDs on each line card.

The system attempts to boot identical line cards in parallel. Furthermore, the system boots line cards as soon as they are powered on and become available for a system boot. (The physical location of the alphanumeric display LEDs on the line cards is the same as on the GRP, which is shown in [Figure 12](#).)

Refer to the appropriate line card installation and configuration note for complete details on line card display LED sequences.

You must meet the following criteria to successfully boot the GRP:

- Flash memory card or Flash disk is installed in Flash card slot 0
- Flash memory card or Flash disk contains a valid Cisco IOS software image
- Software configuration register is set to 0x2102.

The system automatically boots this Cisco IOS software image. The system then enters the setup facility, where you are prompted to perform a basic configuration of the system.

Otherwise, the system enters the ROM monitor and the appropriate prompt (`rommon>`).

Step 5 If the ROM monitor prompt (`rommon>`) appears, you must boot the Cisco IOS software image you want to use by entering the appropriate **b** command at the ROM monitor prompt:

- **b**—Boots the default system software from onboard Flash memory (if it is present in onboard Flash memory)
- **b filename [host]**—Boots the file *filename* from the server *host* using TFTP
- **b flash**—Boots the first file in the Flash memory card in Flash card slot 0



Caution

To prevent system problems, use the **b flash** command option carefully; otherwise, you might instruct the system to boot a non-Cisco IOS software image from Flash memory. This command is not used with Flash disks.

- **b slot0: filename**—Boots the file *filename* from the Flash memory card in Flash card slot 0
- **b slot1: filename**—Boots the file *filename* from the Flash memory card in Flash card slot 1
- **b flash disk0: filename**—Boots the file *filename* from the Flash disk in Flash card slot 0
- **b flash disk1: filename**—Boots the file *filename* from the Flash disk in Flash card slot 1



Caution

The **b flash disk0:** and **b flash disk1:** commands are only used from the ROM monitor (`rommon>`) prompt when the system fails to load normally. Do not use these commands from the router (`router>`) prompt.

While the system boots, the console screen displays a script and system banner similar to the following:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-MZ), Released Version 11.2(9)GS
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Sat 10-May-97 06:02a
```

Step 6 Observe the system startup banner. When you start up an unconfigured system for the first time, the system automatically enters the setup facility, which determines which interfaces are installed and prompts you for configuration information for each one.

On the console screen, after the system displays the system banner and hardware configuration, the following System Configuration Dialog prompt appears:

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

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

- Step 7** You have the option of proceeding with the setup facility or exiting from setup and using configuration commands to configure global (system-wide) and interface-specific parameters.

You do not have to configure the interfaces immediately; however, you cannot enable the interfaces or connect them to any networks until you have configured them.

The interface-specific LEDs on line cards might not go on until after you configure the line card interfaces. In order to verify correct operation of each interface, complete the first-time setup procedures and configuration, then refer to the LED descriptions in the configuration notes for each line card to check the status of the interfaces.

Verifying Interface Status

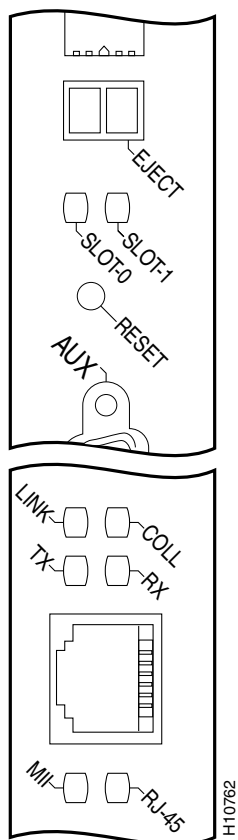
This section provides functional descriptions of the status LEDs on the GRP (see [Figure 13](#)) and the processes you should observe.

The status LEDs on the GRP indicate system and GRP status, which Flash memory card or Flash disk slot is active, which Ethernet connection is in use, and what is occurring on the Ethernet interface. (A successful boot is indicated by the alphanumeric display LEDs as shown in [Table 8](#); however, this does not necessarily mean that the system has reached normal operation.)

The GRP has the following eight LED indicators:

- 2 Flash card activity LEDs (labeled *Slot 0* and *Slot 1*)—1 LED per slot— Goes on when the slot is accessed. The LEDs receive power from the switched slot voltage.
- 4 RJ-45 Ethernet port LEDs (labeled *LINK*, *COLL*, *TX*, and *RX*)—Used in conjunction with the RJ-45 Ethernet connector. When the MII Ethernet port is in use, the LEDs are disabled. The LEDs indicate link activity (*LINK*), collision detection (*COLL*), data transmission (*TX*), and data reception (*RX*).
- 2 RJ-45 or MII Ethernet port selection LEDs (labeled *MII* and *RJ-45*)—When on, identify which one of the two Ethernet connections you selected. When the RJ-45 port is selected, its LED is on and the MII LED is off. When the MII port is selected, its LED is on, and the RJ-45 LED is off.

Figure 13 GRP LEDs (Partial Front Panel View)



Configuring the Ethernet Interface

The IEEE 802.3 Ethernet interface, located on the GRP, allows connections to external Ethernet networks and is capable of data transmission rates of 10 Mbps and 100 Mbps. At the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth that is less than 100 Mbps; expect a maximum usable bandwidth of approximately 20 Mbps for either the MII or RJ-45 connection. Transmission speed, which is not user configurable, is determined by the network to which the Ethernet interface is connected.

The Ethernet interface does not provide external routing functions; it is primarily designed as a Telnet port into the GRP, and for booting and/or accessing Cisco IOS software images over a network to which the Ethernet interface is directly connected.



Caution

An Ethernet port is used primarily as a Telnet port into the Cisco 12000 Series Router, or for booting or accessing Cisco IOS software images over a network to which an Ethernet port is directly connected. Cisco Express Forwarding (CEF) functions are switched off by default for security reasons. Cisco strongly cautions you to consider the security implications of switching on CEF routing functions on these ports.

The following sections provide two methods for configuring the Ethernet interface.

- [Using Configuration Mode to Configure the Ethernet Interface, page 29](#)
- [Using the setup Command Facility to Configure the Ethernet Interface, page 29](#)

Using Configuration Mode to Configure the Ethernet Interface

Use the following procedure to perform a basic configuration of the Ethernet interface in configuration mode:

-
- Step 1** At the privileged-level prompt, enter configuration mode and specify that the console terminal is the source of the configuration subcommands as follows:
- ```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```
- Step 2** At the configuration mode prompt, specify the Ethernet interface by entering the subcommand **interface**, followed by the *type* (**ethernet**) and *port* (**0**) as follows:
- ```
Router(config)# interface ethernet 0
Router(config-if)#
```
- Step 3** Determine the physical Ethernet connection you want to use (RJ-45 or MII), then use the **media-type** *type* command as appropriate for your physical Ethernet connection:
- ```
Router(config-if)# media-type type
```
- where *type* is RJ45 or MII. The system default is RJ45.
- Step 4** If IP routing is enabled on the system, you can assign an IP address and subnet mask to the interface with the **ip address** configuration subcommand, as in the following example:
- ```
Router(config-int)# ip address 1.1.1.10 255.255.255.0
```
- Step 5** Add any additional configuration subcommands required to enable or disable routing protocols (such as the **no ip mroute-cache** command) and to set other interface characteristics.
- Step 6** Change the shutdown state to up and enable the Ethernet interface as follows:
- ```
Router(config-int)# no shutdown
```
- Step 7** After you include all the configuration subcommands necessary to complete the configuration, press **Ctrl-Z** to exit configuration mode.
- Step 8** Write the new configuration to nonvolatile memory as follows:
- ```
Router# copy running-config startup-config
[OK]
Router#
```
-

Using the setup Command Facility to Configure the Ethernet Interface

In the following example of an Ethernet configuration using the **setup** command facility, the Ethernet interface is configured using IP and CLNS. (In this example, you want to use IP, CLNS, and the default RJ-45 Ethernet connection.)

Enter the setup facility using the **setup** command and respond to prompts as appropriate for your needs, using your own address and mask for the setup prompts.

```
(Additional displayed text omitted from this example.)

Configuring interface Ethernet0:
Is this interface in use?: yes
Configure IP on this interface?: yes
  IP address for this interface: 3.3.1.1
  Number of bits in subnet field: 8
  Class A network is 3.0.0.0, 8 subnet bits; mask is 255.255.0.0
Configure CLNS on this interface?: yes
```

Implementing Additional Configuration and Maintenance Tasks

This section contains information on the following additional configuration, troubleshooting, and maintenance tasks:

- [Configuring the Software Configuration Register](#)
- [Flash Disks and Flash Memory Cards in the GRP](#)
- [Recovering Lost Password](#)
- [Upgrading GRP Memory](#)

Configuring the Software Configuration Register

The system uses a 16-bit software configuration register, which allows you to set specific system parameters. Settings for the software configuration register are written into non-volatile random access memory (NVRAM).

Following are some reasons for changing the software configuration register settings:

- To select a boot source and default boot filename
- To enable or disable the Break function
- To control broadcast addresses
- To set the console terminal baud rate
- To load operating software from Flash memory
- To enable booting from a Trivial File Transfer Protocol (TFTP) server
- To recover a lost password
- To allow you to manually boot the system using the **b** command at the bootstrap program prompt
- To force an automatic boot from the system bootstrap software (boot image) or from a default system image in onboard Flash memory, and to read any **boot system** commands that are stored in the configuration file in NVRAM

[Table 9](#) provides descriptions of each of the software configuration memory bits, and [Table 10](#) defines the boot field, specified as a binary number that consists of bits 0 through 3 of the software configuration register.



Caution

To avoid confusion and possibly halting the Cisco 12000 Series Router, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in [Table 9](#). For example, the factory default value of 0x2102 is a combination of settings.

Table 9 Software Configuration Register Bit Descriptions

Bit ¹	Hexadecimal	Description
00 to 03	0x0000 to 0x000F	Boot field (see Table 10)
06	0x0040	System software ignores NVRAM contents
07	0x0080	OEM ² bit enabled
08	0x0100	Break disabled
09	0x0200	Use secondary bootstrap
10	0x0400	IP ³ broadcast with all zeros
11 to 12	0x0800 to 0x1000	Console line speed (default is 9600 baud)
13	0x2000	Boot default Flash software if network boot fails
14	0x4000	IP broadcasts without network numbers
15	0x8000	Enable diagnostic messages and ignore NVRAM contents

1. The factory default value for the configuration register is 0x2102. This value is a combination of the following: binary bit 8 = 0x0100 and binary bits 00 through 03 = 0x0002 (see [Table 10](#)).
2. OEM = original equipment manufacturer
3. IP = Internet Protocol

Table 10 Boot Field Descriptions (Configuration Register Bits 00 to 03)

Boot Field	Description
00	Stays at the system bootstrap prompt.
01	Boots the first system image in onboard Flash memory.
02 to 0F	Specifies a default filename for booting over the network. Enables boot system commands that override the default filename.

Boot Field Settings and the boot Command

Bits 0 through 3 of the software configuration register form the boot field, specified as a binary number.



Note

The factory default configuration register setting for systems and GRP spares is 0x2102.

Boot field—When the boot field is set to either 0 or 1 (0-0-0-0 or 0-0-0-1), the system ignores any boot instructions in the system configuration file and the following occurs:

- When the boot field is set to 0, you must boot the operating system manually by using the **boot** command to the system bootstrap program, or *rom monitor*.

or

- When the boot field is set to 1, the system boots the first image in the onboard bootflash single in-line memory module (SIMM).

You can enter the **boot** command only, or include additional boot instructions with the command such as the name of a file stored in Flash memory or a file that you specify for booting from a network server. If you use the **boot** command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory).

Otherwise, you can instruct the system to boot from a specific Flash image (using the **boot system flash filename** command), or boot from a network server by sending broadcast TFTP requests (using the **boot system filename** command), or send a direct TFTP request to a specific server (using the **boot system filename ip-address** command).

You can also use the **boot** command to boot images stored in the Personal Computer Memory Card International Association (PCMCIA) Flash memory cards or Flash disks located in PCMCIA slot 0 or slot 1 on the GRP. If you set the boot field to any bit pattern other than 0 or 1, the system uses the resulting number to form a filename for booting over the network.

To form this filename, the system starts with *cisco* and links the octal equivalent of the boot field value and the processor type in the format *cisco<bootfieldvalue>-<processorname>*; for example, *cisco2-GRP*. The system uses this filename to invoke the system image by booting over the network. However, if the configuration file contains any boot instructions, the system uses those boot instructions instead of the filename it computed from the configuration register settings.



Note

If a bootable Cisco IOS software image exists in a Flash memory card or Flash disk installed in PCMCIA slot 0 or slot 1, the configuration register setting is overridden, and the bootable Cisco IOS software image will be booted instead of the default TFTP-bootable Cisco IOS software image (cisco2-GRP through cisco17-GRP).

You must set the boot field for the boot functions you require.

Changing Configuration Register Settings

Use the following procedure to change the configuration register while running the system software:

Step 1 Enter the **enable** command and your password to enter privileged level as follows:

```
Router> enable
Password:
Router#
```

Step 2 Enter the **configure terminal** command at the privileged-level system prompt (#), also called the enabled prompt. You are prompted, as shown in the following example:

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

Step 3 Set the contents of the configuration register by entering the **config-register value** configuration command, where *value* is a hexadecimal number preceded by 0x (see [Table 9](#)), as in the following example:

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

Step 4 Exit configuration mode by entering **Ctrl-Z**.

The new value settings are saved to memory; however, the new settings do not take effect until the system software is reloaded by rebooting the system.

Step 5 Display the configuration register value currently in effect, which will be used at the next reload by entering the **show version EXEC** command.

The value is displayed on the last line of the screen display, as in the following example:

```
Configuration register is 0x141 (will be 0x2102 at next reload)
```

Step 6 Save your settings.

Configuration register changes take effect only after the system reloads, such as when you issue a **reload** command from the console.

Step 7 Reboot the system. The new configuration register value takes effect with the next system boot.

Configuration Register Bit Meanings

The lowest four bits of the software configuration register (bits 3, 2, 1, and 0) form the *boot field*. (See [Table 10](#).) 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 (>).

If you set the boot field value to *0x2* through *0xF* and there is a valid **boot system** command stored in the configuration file, the Cisco 12000 Series Router boots the system software as directed by that value. If there is no **boot system** command, the Cisco 12000 Series Router forms a default boot filename for booting from a network server. (See [Table 11](#) for the format of these default filenames.)

In the following example, the software configuration register is set to boot the system from onboard Flash memory and to ignore Break at the next reboot of the system:

```
Router# conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# config-register 0x2102
Router(config)# boot system flash [filename]
Ctrl-z
Router#
```

The server creates a default boot filename as part of the automatic configuration process. To form the boot filename, the server starts with the name *cisco* and adds the octal equivalent of the boot field number, a hyphen, and the processor-type name (*GRP*).

[Table 11](#) lists the default boot filenames. A **boot system** configuration command in the configuration file in NVRAM overrides the default filename created for booting over the network.



Note

If a bootable Cisco IOS software image exists in a Flash memory card or Flash disk installed in PCMCIA slot 0 or slot 1, the configuration register setting is overridden, and the bootable Cisco IOS software image will be booted instead of the default TFTP-bootable Cisco IOS software image (cisco2-GRP through cisco17-GRP).

Table 11 Default Boot Filenames

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
Default software	0	0	0	1
cisco2-GRP	0	0	1	0
cisco3-GRP	0	0	1	1

Table 11 Default Boot Filenames (continued)

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
cisco4-GRP	0	1	0	0
cisco5-GRP	0	1	0	1
cisco6-GRP	0	1	1	0
cisco7-GRP	0	1	1	1
cisco10-GRP	1	0	0	0
cisco11-GRP	1	0	0	1
cisco12-GRP	1	0	1	0
cisco13-GRP	1	0	1	1
cisco14-GRP	1	1	0	0
cisco15-GRP	1	1	0	1
cisco16-GRP	1	1	1	0
cisco17-GRP	1	1	1	1

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the system to ignore the console Break key. Clearing bit 8 causes the system to interpret the Break key as a command, which forces the system into the bootstrap (or ROM) monitor, thereby halting normal operation. Regardless of the setting of the break enable bit, a break causes a return to the ROM monitor during the first few seconds (approximately 5 seconds) of booting.

Bit 9 is unused.

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.

Table 12 shows the combined effect of bits 10 and 14.

Table 12 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 11 and 12 in the configuration register determine the data transmission rate of the console terminal. Table 13 shows the bit settings for the four available rates. (The factory-set default data transmission rate is 9600.)

Table 13 System Console Terminal Transmission Rate Settings

Baud	Bit 12	Bit 11
9600	0	0
4800	0	1

Table 13 System Console Terminal Transmission Rate Settings (continued)

Baud	Bit 12	Bit 11
2400	1	1
1200	1	0

Bit 13 determines the server response to a bootload failure. Setting bit 13 causes the server to load operating software from Flash memory 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 cleared to 0.

Flash Disks and Flash Memory Cards in the GRP

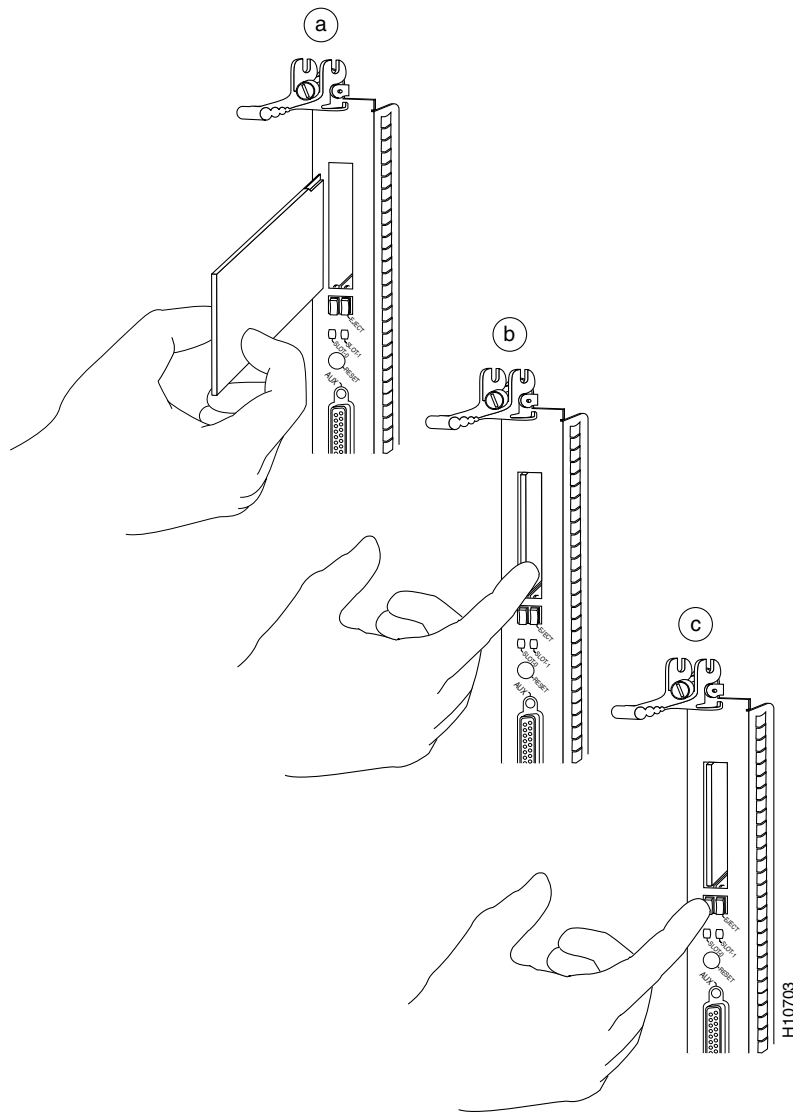
Procedures for using Flash memory cards or Flash disks in the GRP and information on the Flash memory functions are presented in the following sections:

- [Installing and Removing Flash Memory Card or Flash Disk in GRP](#)
- [Notes About ATA Flash Disks](#)
- [ATA Flash Disk Boot Image Support Requirements](#)
- [Formatting a Flash Memory Card or Flash Disk](#)
- [Specifying Cisco IOS Image Used to Boot the System](#)
- [Software Commands Associated with Flash Memory](#)
- [Enabling Booting from Flash Memory](#)
- [Copying Files to Flash Memory](#)
- [Copying a Cisco IOS Software Image into Flash Memory Card or Flash Disk](#)
- [Copying Cisco IOS Software Images Between Flash Memory Cards or Flash Disks](#)
- [Copying System Configuration Files Between GRP Memory and a Flash Memory Card or Flash Disk](#)
- [Recovering from Locked Blocks in Flash Memory Cards or Flash Disks](#)

Installing and Removing Flash Memory Card or Flash Disk in GRP

The GRP has two Flash Card slots (slot 0 and slot 1), into which you can install a linear Flash memory card or an ATA Flash disk. The slots are positioned with slot 0 on the left and slot 1 on the right. (See [Figure 14](#).)

Figure 14 Installing and Removing Flash Memory Card or Flash Disk



Both slots can be used at the same time. Use the following procedure to install a Flash memory card or Flash disk:

- Step 1** Facing the GRP front panel, hold the Flash memory card or Flash disk with the connector end of the card toward the slot and the label facing right. (See [Figure 14a.](#))



Note The Flash memory card or Flash disk is keyed and cannot be seated the wrong way. The ejector button will not pop out if the card is not properly inserted.

- Step 2** Insert the card into the appropriate slot until the card completely seats in the connector at the back of the slot, and the ejector button pops out toward you. (See [Figure 14b.](#))

**Caution**

The Flash memory card or Flash disk does not insert all the way inside the GRP; a portion of the card remains outside of the slot. *Do not attempt to force the card past this point.*

Use the following procedure to remove a Flash memory card or Flash disk:

-
- Step 1** To eject the card, press the ejector button until the card is free of the connector at the back of the slot. (See [Figure 14c.](#))
- Step 2** Remove the card from the slot and place it in an antistatic bag to protect it.
-

Notes About ATA Flash Disks

Note the following issues when using an ATA Flash disk with Cisco IOS Releases prior to 12.0(22)S:

- Cisco IOS Release 12.0(17)S or 12.0(17)ST or later is required, along with the corresponding boot images for the GRP to function with a Flash disk. Flash disk system boot support is provided only in the IOS bootloader.
- In ROM Monitor version 181 or earlier, the Flash disk file system is not recognized.
- If you upgrade to ROM Monitor version 182 or later, you must also format the Flash disk with Cisco IOS Release 12.0(22)S or later.

ATA Flash Disk Boot Image Support Requirements

A boot image that supports the ATA file system must reside in bootflash. To enable booting from a Flash disk, set the configuration register bits to 0x2102 and add a **boot system** command to the configuration as follows:

```
Router(config)# config-reg 0x2102
Router(config)#^Z
Router#write mem

Router# configure terminal
Enter configuration commands, one per line. End with CTRL-Z.
Router(config)# boot system disk0:gsr-p-mz.120-19.S
```

**Note**

See the Cisco IOS online publication *Loading and Maintaining System Images and Microcode* for details on this procedure.

Formatting a Flash Memory Card or Flash Disk

The Flash memory card or Flash disk that shipped with your router contains the Cisco IOS software image you need to boot your router. In some cases, you might need to insert a new Flash memory card or Flash disk and copy images or backup configuration files onto it. Before you can use a *new* Flash memory card or Flash disk, you must format it.

**Note**

In the following procedure, you are assumed to have already booted your router. Use only linear Flash memory cards, or ATA Flash disks.



Caution

The following formatting procedure erases all information on the Flash memory card or Flash disk. To prevent the loss of important data that might be stored on a Flash memory card or Flash disk, proceed carefully. If you want to save the data on a Flash memory card or Flash disk, copy the data to a server before you format the card.

To format a new Flash memory card or Flash disk, follow these steps:



Note

The flash card command examples presented in this publication assume the use of a standard linear Flash memory card. If you are using an ATA Flash disk, replace any commands with either the **slot0:** or **slot1:** command argument with a **disk0:** or **disk1:** command argument.

Step 1

After booting your router, insert the Flash memory card or Flash disk into slot 0. (Use the procedure in the [“Installing and Removing Flash Memory Card or Flash Disk in GRP”](#) section on page 35.) If slot 0 is not available, use slot 1.

Step 2

Enter the **format slot0:** (or **format slot1:**) command as follows:

```
Router# format slot0:
All sectors will be erased, proceed? [confirm]
Enter volume id (up to 30 characters): NewCard
Formatting sector 1
Format device slot0 completed
Router#
```



Note

For this example, a 20-MB Flash memory card was used. At the line “Formatting sector,” the system counts backward from 160 to 1.

The new Flash memory card or Flash disk is now formatted and ready to use.

For complete command descriptions and configuration information, refer to the *Configuration Fundamentals Command Reference*, the *Configuration Fundamentals Configuration Guide*, and the *Cisco 12000 Series Internet Router Flash Disk Information* publications. (For information on obtaining these publications, see the [“Obtaining Documentation”](#) section on page 53.)

Specifying Cisco IOS Image Used to Boot the System

Use the following series of commands to specify that a Cisco IOS software image is bootable. (In this example, the file is named *new.image*.) Note that because the configuration register must be set to 0x2102, the **config-register** command is part of the sequence.

```
Router# config terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:new.image
Router(config)# config-register 0x102
Ctrl-z
Router# copy running-config startup-config
Router# reload
```

When the system reloads, it will boot the Cisco IOS software image from the Flash memory card or Flash disk in slot 0.



Note

In the preceding example, the configuration register value 0x102 instructs the system to boot a default Cisco IOS software image from Flash memory. If a network boot fails, the value 0x2102 instructs the system to ignore a break, and the value 0x0002 instructs the system to look in Flash memory for this default Cisco IOS software image.

Software Commands Associated with Flash Memory

Following are software commands related to the onboard Flash memory on the GRP and the Flash memory cards and Flash disks.



Note

If using an ATA Flash disk, replace any commands that include a **slot0:** or **slot1:** command argument with a **disk0:** or **disk1:** command argument.

Determine which memory media you are accessing using the **pwd** command as follows:

```
Router# pwd
slot0
```

Move between Flash memory media using the **cd device-name** command, where *device-name* can be **slot1:**, **slot0:**, or **bootflash:**. Examples follow:

```
Router# cd slot1:
Router# pwd
slot1
```

```
Router# cd slot0:
Router# pwd
slot0
```

You can list the directory of Flash memory media using the **dir [device-name]** command, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**. An example of the **dir** command follows:

```
Router# dir
-#- -length- ----date/time----- name
1 4601977 May 10 1997 09:42:19 myfile1
6 679 May 10 1997 05:43:56 todays-config
7 1 May 10 1997 09:54:53 fun1
```

You can delete a file from any Flash memory media using the **delete filename** command, where *filename* is any file within Flash memory. An example of deleting the file *fun1* from the Flash memory card or Flash disk in slot 0 follows:

```
Router# delete fun1
Router# dir
-#- -length- ----date/time----- name
1  4601977  May 10 1997 09:42:19 myfile1
6   679    May 10 1997 05:43:56 todays-config
```

Files that are deleted are marked as deleted, but still occupy space in Flash memory. The command **squeeze device-name** (where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**) removes them permanently and pushes all other undeleted files together to eliminate spaces between them.


Note

The **squeeze** command is used with Flash memory cards only. This command is not needed when using Flash disks.

An example of the **squeeze** command follows:

```
Router# squeeze slot0:
All deleted files will be removed, proceed? [confirm]
Squeeze operation may take a while, proceed? [confirm]
ebESZ
```

To prevent loss of data from sudden power loss, the “squeezed” data is temporarily saved to another location of Flash memory, which is specially used by the system.

The meanings of the characters in the preceding command display output as follows:

- e—This special location has been erased (which must occur before any write operation).
- b—The data that is about to be written to this special location has been temporarily copied.
- E—The sector that was temporarily occupied by the data was erased.
- S—The data was written to its permanent location in Flash memory.
- Z—This log was erased after the successful **squeeze** command operation.

The **squeeze** command operation keeps a log of which of these functions was performed, so that in case of sudden power failure, it can return to the correct place and continue with the process.

The configuration register setting 0x0101 tells the system to boot the default image (the first image) from onboard Flash memory, but *not* reset the Break disable or check for a default filename to be booted over the network. The configuration register setting 0x0102 tells the system to boot from Flash memory if netboot fails, then disable Break and check for a default netboot filename.

For more information on the **copy tftp:filename [bootflash: | slot0: | slot1:]filename** command and other related commands, refer to the set of configuration and reference publications.

Enabling Booting from Flash Memory

To enable booting from Flash memory, set configuration register bits 3, 2, 1, and 0 to a value between 2 and 15 in conjunction with the **boot system flash device-name:filename** configuration command, where *device-name* is **bootflash:**, **slot0:**, or **slot1:** (Flash memory cards), and **bootflash:**, **disk0:**, or **disk 1:** (ATA Flash disk cards) and *filename* is the name of the file from which you want to boot the system.

To enter configuration mode while in the system software image and specify a Flash filename from which to boot, enter the **configure terminal** command at the enable prompt as follows:

```
Router#configure terminal
```


Copying a Cisco IOS Software Image into Flash Memory Card or Flash Disk

You can copy a Cisco IOS software image into Flash memory; however, you must first format the Flash memory card or Flash disk and make the image in the Flash memory card or Flash disk bootable. (If you have not already done this, see the [“Formatting a Flash Memory Card or Flash Disk”](#) section on page 37 and the [“Specifying Cisco IOS Image Used to Boot the System”](#) section on page 39.)



Note

If using an ATA Flash disk, replace any commands that include a **slot0:** or **slot1:** command argument with a **disk0:** or **disk1:** command argument.

Before you copy a Cisco IOS software image, you must do the following:

- Install a formatted Flash memory card or Flash disk in your GRP.
- Have a bootable Cisco IOS software image in the onboard Flash memory so you can start the router.
- Ensure that the bootable Cisco IOS software image you want to copy to the Flash memory card or Flash disk exists on a TFTP server to which you have access (meaning that you know its name and can connect to it), and at least one interface is available to access this server. To ensure access to a TFTP server, you need to configure one interface.
- Know the filename of the image you want to copy into the Flash memory card or Flash disk.

Use the following procedure to copy a bootable image into the Flash memory card or Flash disk:

Step 1 Boot the router and allow it to initialize.

Step 2 Enable the router and copy the image *new.image* to the Flash memory card or Flash disk in slot 0 using the following series of commands:

```
Router> enable
Password:
Router# copy tftp:new.image slot0:new.image
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

In the preceding example, the exclamation points (!!!) appear as the file is downloaded, and the C characters signify calculation of the cyclic redundancy check (CRC) value, which is a verification that the file has been correctly downloaded to the Flash memory card or Flash disk. You must now reboot the system.

Copying Cisco IOS Software Images Between Flash Memory Cards or Flash Disks

As future releases of Cisco IOS software become available, you will receive these images either as a file booted from a network server, a file on floppy disk, or a file on a Flash memory card or Flash disk.

The following scenario describes how to use a newly released Cisco IOS software image on a Flash memory card or Flash disk in a system that has an older image on a Flash memory card or Flash disk in slot 0 and a default boot Cisco IOS software image in the onboard Flash memory.

For this scenario, the filenames are as follows:

- The New image on the new Flash memory card or Flash disk is *image.new*.
- The old image in the Flash memory card or Flash disk in slot 0 is *image.old*.
- The bootable image in onboard Flash memory is *image.boot*. (Use the Cisco IOS software image used by default to boot the system if no other images are available.)

You will copy the new Cisco IOS software image from the new Flash memory card or Flash disk onto the Flash memory card or Flash disk that contains the old Cisco IOS software image.



Note

For this scenario, the new Cisco IOS software image fits on the Flash memory card or Flash disk in slot 0 next to the old image. If there is not enough available space, use the **delete** command to delete files from the Flash memory card or Flash disk to make sufficient room for the new Cisco IOS software image; however, *do not* delete the *image.old* file. Then use the **squeeze** command to remove these deleted files from the Flash memory card or Flash disk. (For information on the **squeeze** command, see the [“Software Commands Associated with Flash Memory”](#) section on page 39.)

If, after you delete files and use the **squeeze** command, the two files cannot coexist on the Flash memory card or Flash disk in slot 0, remove this card (place it in an antistatic bag and store it in a safe place), and insert the new Flash memory card or Flash disk (with the file *image.new*) in slot 0. Proceed to [Step 5](#) in the following procedure and use the command **boot system flash slot0:image.new** to designate the file *image.new* as the default boot Cisco IOS software image.



Note

If using an ATA Flash disk, replace any commands that include a **slot0:** or **slot1:** command argument with a **disk0:** or **disk1:** command argument.

Use the following procedure to copy bootable Cisco IOS software images between Flash memory cards or Flash disks:

Step 1 Boot the router. (For this example, the file *image.boot* is used.)

Step 2 Enable the router as follows:

```
Router> enable
Password:
Router#
```

Step 3 Insert the new Flash memory card or Flash disk in slot 1.

Step 4 Use the following command to copy the file *image.new* in slot 1 to the Flash memory card or Flash disk in slot 0, *only if* there is enough memory space for the two images to coexist:

```
Router# copy slot1:image.new slot0:image.new
```

You can also enter the previous command as **copy slot1:image.new slot0:**.

- Step 5** Use the following series of commands to designate the file *image.new* (in the Flash memory card or Flash disk in slot 0) as the default boot image:

```
Router# config t
Router(config)# no boot system
Router(config)# boot system flash slot0:image.new
Crtl-z
Router# copy running-config startup-config
Router# reload
```

When the system reloads, it will boot the file *image.new* from the Flash memory card or Flash disk in slot 0.

Copying System Configuration Files Between GRP Memory and a Flash Memory Card or Flash Disk

Copying a configuration file to a Flash memory card or Flash disk in PCMCIA slot 0 or slot 1 might be required if you do not have access to a TFTP server on which you can temporarily store your configuration file. You can then copy the configuration file back to NVRAM at any time. You can copy your startup configuration file (from NVRAM) or your running configuration file (from DRAM).

Use the procedures in the following sections to first copy the configuration file from either NVRAM or DRAM to a Flash memory card or Flash disk, and then to copy the configuration file from a Flash memory card or Flash disk back to NVRAM.



Note You cannot copy files directly into DRAM.

Copying Configuration File from GRP NVRAM to Flash Memory Card or Flash Disk

You can use the command **copy startup-config [slot0: | slot1:]filename** for the copy procedure, where **startup-config** is the file's source (NVRAM), and **[slot0: | slot1:]filename** is the file's destination in either of the Flash memory cards or Flash disks. Note that the environmental variable **CONFIG_FILE** must be pointing (set) to NVRAM, which is the system default.



Note If using an ATA Flash disk, replace any commands that include a **slot0:** or **slot1:** command argument with a **disk0:** or **disk1:** command argument.

Use the following procedure to copy a configuration file from GRP NVRAM to a Flash memory card or Flash disk:

- Step 1** Use the **show boot** command to display the current setting for the environmental variable **CONFIG_FILE** as follows:

```
Router# show boot
(display text omitted)

CONFIG_FILE variable =
Current CONFIG_FILE variable =

(display text omitted)
```

The preceding example shows that the environmental variable **CONFIG_FILE** is set for NVRAM, by default.

Step 1 Use the `copy running-config slot0:filename` command as follows:

```
Router# copy running-config slot0:myfile2
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Router#
```

In the preceding example, the exclamation points (!!!) appear as the file is copied.

Step 2 Use the `dir` command to verify the file was copied correctly as follows:

```
Router# dir slot0:
-#- -length- ----date/time----- name
1 5200084 May 10 1997 19:24:12 gsr-p-mz.112-8
3 1215 May 10 1997 20:30:52 myfile1
4 6176844 May 10 1997 23:04:10 gsr-p-mz.112-8.1
5 1186 May 10 1997 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
```

Copying Configuration File from Flash Memory Card or Flash Disk to GRP NVRAM

Following is an example of copying your startup configuration file from a Flash memory card or Flash disk in PCMCIA slot 0 or slot 1 back to NVRAM.

- Flash memory cards—Use the command `copy [slot0 | slot1]:filename startup-config`, where `[slot0 | slot1]:filename` is the source of the file (Flash memory card), and `startup-config` is the destination (NVRAM).
- Flash disks—Use the command `copy [disk0 | disk1]:filename startup-config`, where `[disk0 | disk1]:filename` is the source of the file (Flash disk), and `startup-config` is the destination (NVRAM).

Step 1 Use the `copy slot0:filename startup-config` command as follows:

```
Router# copy slot0:myfile startup-config
[ok]
Router#
```

Step 2 Use the `copy startup-config running-config` command to ensure that the startup configuration file, now stored in NVRAM, is the default running configuration file used by the system as follows:

```
Router# copy startup-config running-config
Router#
%SYS-5-CONFIG_I: Configured from memory by console
Router#
```

Recovering from Locked Blocks in Flash Memory Cards or Flash Disks

A locked block in Flash memory cards or Flash disks occurs when power is lost, or a Flash memory card or Flash disk is unplugged during a write or erase operation. When a block of Flash memory is locked, it cannot be written to or erased, and the operation will consistently fail at a particular block location. The only way to recover from locked blocks is to reformat the Flash memory card or Flash disk with the **format** command. (See the “[Formatting a Flash Memory Card or Flash Disk](#)” section on page 37.)



Caution

Formatting a Flash memory card or Flash disk erases its data.

Recovering Lost Password

This section provides information on how to recover a lost password.

The following overview describes this process:

1. Use the **show version** command to note the existing software configuration register value.
2. Break to the bootstrap program prompt.
3. Change the configuration register to ignore NVRAM.



Note

A key to recovering a lost password is to set the configuration register so that the contents of NVRAM are ignored (0x0040), allowing you to see your password.

4. Enter privileged level in the system EXEC.
5. Use the **show startup-config** command to display the enable password.
6. Change the configuration register value back to its original setting.

Use the following procedure to recover a lost password.



Note

If the enable password is encrypted, the following password recovery procedure will not work and you will have to reconfigure the system; you will not be able to reboot it. To reconfigure the system, use the displayed configuration, which is shown using the **show startup-config EXEC** command. (See [Step 11](#).)

- Step 1** Attach an ASCII terminal to the GRP console port.
- Step 2** Configure the terminal to operate at 9600 bps, 8 data bits, no parity, 2 stop bits (or to whatever settings the console port is set).
- Step 3** Enter the **show version** command to display the existing configuration register value. Note this value for later use.
- Step 4** If Break is disabled, power cycle the router. (To power cycle, turn off power, wait 5 seconds, then turn it on again.) If Break is enabled on the router, press the Break key or send a break by holding down the **Control** key and pressing the right square bracket key (^); then proceed to [Step 5](#).
- Step 5** Within 5 seconds of turning on the router, press the Break key. This action causes the terminal to display the bootstrap program prompt as follows:

```
rommon 1>
```

Step 6 Set the configuration register to ignore the configuration file information as follows:

```
rommon 1> confreg
Configuration Summary
enabled are:
console baud: 9600
boot: image specified by the boot system command
or default to: cisco2-GRP

do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
enable "load rom after netbootfails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect?" y/n [n]:
enable "ignore system config info?" [n]: y
change console baud rate? y/n [n]:
change boot characteristics? y/n [n]

Configuration Summary
enabled are:
console baud: 9600
boot: image specified by the boot system command
or default to: cisco2-GRP
Do you wish to change the configuration? y/n [n]
```

You must reset or power cycle for the new config to take effect

Step 7 Initialize the router by entering the **i** command as follows:

```
rommon 1> i
```

The router power cycles, the configuration register is set to ignore the configuration file, and the router boots the boot system image and prompts you with the system configuration dialog as follows:

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

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

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

Step 9 Press **Return**.

After some interface information displays, the prompt appears as follows:

```
Router>
```

Step 10 Enter the **enable** command to enter enabled mode.

The prompt changes to the following:

```
Router#
```

Step 11 Enter the **show start-up config EXEC** command to display the enable password in the configuration file.

Step 12 Enter the **configure terminal** command at the EXEC prompt.

You are prompted as follows:

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

Change the configuration register value back to its original value (noted from [Step 3](#).)

Change it to a value of 0x2102 (factory default) using the **config-register** 0x *value* command.

- Step 13** Enter **Ctrl-Z** to exit configuration mode.
- Step 14** Reboot the router and enable it using the recovered password.

Upgrading GRP Memory

This section provides the procedure for increasing the amount of extended data output (EDO) DRAM on a GRP by replacing up to two dual in-line memory modules (DIMMs). The system DRAM resides on up to two DIMMs on the GRP. The DRAM DIMM sockets are U39 (bank 1) and U42 (bank 2). (See [Figure 15](#) and [Table 14](#).)

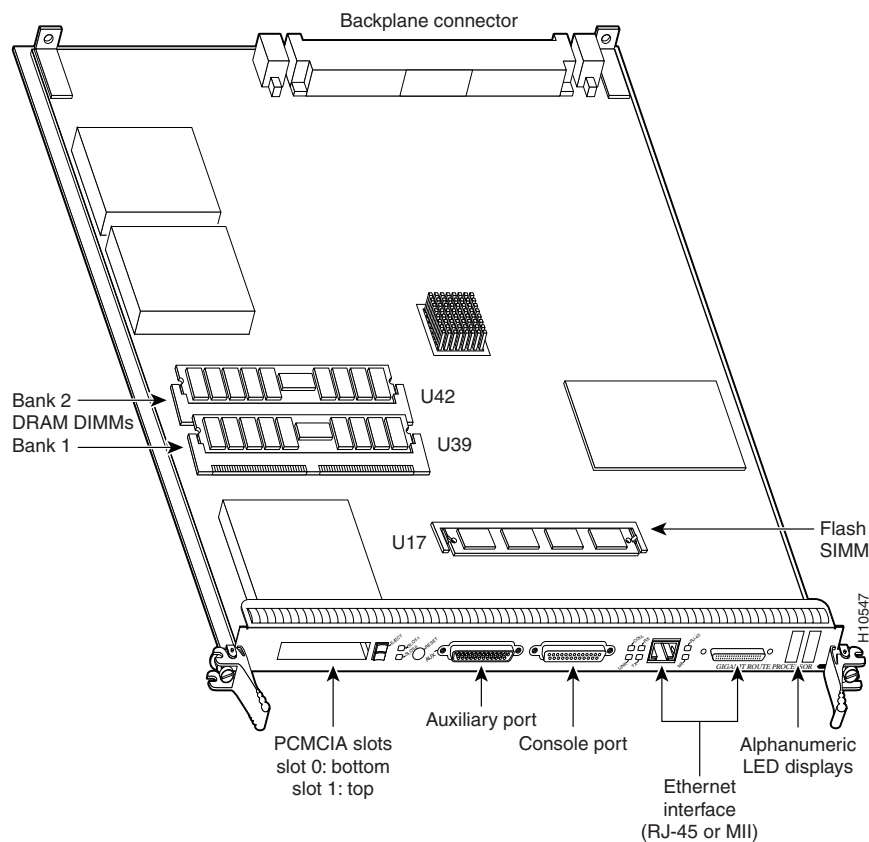
The default DRAM configuration is 128 MB (one 128-MB DIMM in U39).



Note

The total number of memory devices per DIMM differs for each manufacturer. The DIMMs in [Figure 16](#) and [Figure 17](#) show a generic representation of the actual DRAM DIMMs for your GRP. To be assured that you are using the correct DIMMs, refer to the specific part numbers for your DRAM upgrade kit (see the “[DRAM](#)” section on [page 6](#)) and to the Cisco part numbers on the DIMMs. (See [Table 14](#).)

Figure 15 Locations of GRP Memory Components





Note

Each GRP DIMM socket has one plastic lever on one end, which you use to remove the DIMM from its socket. (See [Figure 16](#).)

Before proceeding, ensure that you have the proper tools and ESD-prevention equipment available. To upgrade DRAM, you will install DIMMs in one or two banks (U39 and U42). [Table 14](#) lists the various available configurations of DRAM DIMMs, the number of DIMMs for each configuration, and the DRAM banks they occupy. Note which banks you should use, given the combinations of available DIMM sizes and the maximum DRAM you require.



Note

Depending on your router's configuration and the protocols and features your system is running, you might require more than 128 MB of DRAM. Upgrade your system DRAM based on your current configuration, this potential requirement, and the information in [Table 14](#).

Table 14 GRP Memory Options

Total Route Memory Ordered ¹	Cisco Product Number	DIMM Modules	DRAM DIMM Sockets
64 MB	MEM-GRP/LC-64= ²	1 64-MB DIMM	U39 or U42
128 MB	MEM-GRP/LC-128= ²	1 128-MB DIMM	U39
256 MB	MEM-GRP/LC-256= ³	2 128-MB DIMMs	U39 and U42
256 MB	MEM-GRP-256= ⁴	1 256-MB DIMM	U39
512 MB	MEM-GRP-512= ⁵	2 256-MB DIMMs	U39 and U42

1. Do not mix memory sizes. If installing 2 DIMMs, both DIMMs must be the same size.
2. For GRPs equipped with 64 MB, this option adds a second 64-MB DIMM for a total of 128 MB.
3. This product is no longer available. Replace it with Cisco Product Number MEM-GRP-256.
4. Only compatible with Product Number GRP-B=.
5. GRP route memory configurations of 512-MB are only compatible with Product Number GRP-B=. In addition, Cisco IOS Release 12.0(19)S or 12.0(19)ST or later and ROMMON Release 11.2 (181) or later are also required.



Note

If your system includes redundant GRPs, both GRPs should have the same memory size. Redundancy is not supported when using a GRP and a PRP in the same chassis. Cisco strongly recommends that you avoid configuring your router using mixed route processor cards. Refer to the *Route Processor Redundancy Plus for the Cisco 12000 Series Internet Router* publication for more information on redundancy.



Caution

To prevent system and memory problems when installing DRAM, make sure that the card's DRAM DIMMs are +3.3VDC, 60-ns, EDO devices. Do not attempt to install other DRAM devices in the GRPs DIMM sockets.

Removing DIMMs

This section provides the procedure for removing DIMMs. As you remove DIMMs, place them on an antistatic mat or store them in an antistatic bag. You can use the DIMMs that you remove in other compatible equipment.



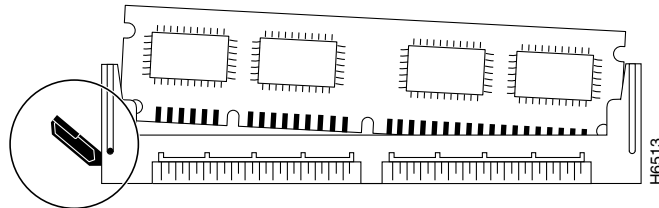
Caution

To prevent ESD damage, handle DIMMs by the card edges only.

Use the following procedure to remove the existing DIMM(s):

-
- Step 1** Turn off the system power.
 - Step 2** Attach an ESD-preventive wrist strap to yourself following the instructions that came with the strap.
 - Step 3** Remove the GRP. (Follow the steps in the [“Removing a GRP”](#) section on page 14.)
 - Step 4** Place the GRP on an antistatic mat or pad.
 - Step 5** Position the GRP so that the faceplate is toward you, and the backplane connector is away from you. (See [Figure 15](#).)
 - Step 6** Locate the DRAM DIMMs on the GRP. The DIMMs occupy U39 (bank 1) and U42 (bank 2). (See [Figure 15](#).)
 - Step 7** For the DIMM you want to remove, pull down the lever on the DIMM socket to release the DIMM from the socket. (See [Figure 16](#).)

Figure 16 Using DIMM Socket Release Lever to Remove DIMMs



- Step 8** When one end of the DIMM is released from the socket, grasp each end of the DIMM with your thumb and forefinger and pull the DIMM completely out of the socket. Handle the edges of the DIMM only (see [Figure 17](#)); avoid touching the memory module or pins and the metal traces, or *fingers*, along the socket edge.
 - Step 9** Place the DIMM in an antistatic bag to protect it from ESD damage.
 - Step 10** Repeat Step 6 through Step 9 for the remaining DIMM, if required for your upgrade.
-

Installing New DIMMs

This section provides the procedure for installing new DIMMs.



Caution

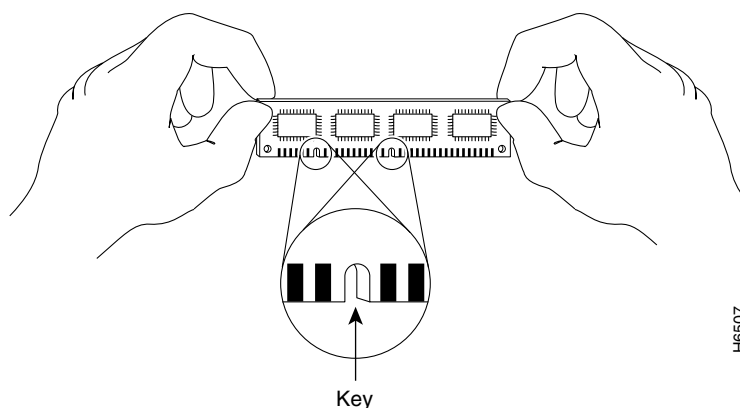
To prevent system and memory problems when installing DRAM, make sure that the card's DRAM DIMMs are +3.3VDC, 60-ns, EDO devices. Do not attempt to install other DRAM devices in the GRPs DIMM sockets.



Caution

DIMMs are sensitive components that can be shorted by mishandling; they are susceptible to ESD damage. Handle DIMMs by the edges only (see [Figure 17](#)); avoid touching the DIMMs, pins, or traces (the metal fingers along the connector edge of the DIMM).

Figure 17 Handling a DIMM



Use the following procedure to install the new DIMMs:

- Step 1** Attach an ESD-preventive wrist strap to yourself following the instructions that came with the strap.
- Step 2** Place the GRP on an antistatic mat or pad.
- Step 3** Position the GRP so that the faceplate is toward you and the backplane connector is away from you. (See [Figure 15](#).)
- Step 4** Remove a new DIMM from the antistatic bag.
- Step 5** Hold the DIMM component-side-up, with the connector edge (the metal fingers) closest to you. Hold the ends of the DIMM between your thumb and forefinger. (See [Figure 17](#).)
- Step 6** Tilt the DIMM to approximately the same angle as the socket and insert the entire connector edge into the socket.

Note the two notches (keys) on the connector edge of the DIMM. (See [Figure 17](#).) These keys are intended to ensure correct orientation of the DIMM in the socket.
- Step 7** Gently push the DIMM into the socket until the lever is flush against the side of the DIMM socket (see [Figure 16](#)), and the backplane connector of the DIMM is fully inserted. If necessary, rock the DIMM gently back and forth to seat it properly.

- Step 8** When the DIMM is installed, check that the release lever is flush against the side of the DIMM socket. If it is not, the DIMM might not be seated properly. If the DIMM appears misaligned, carefully remove it and reseat it in the socket. Push the DIMM firmly back into the socket until the release lever is flush against the side of the DIMM socket.

**Caution**

When inserting DIMMs, use firm but not excessive pressure. If you damage a socket, you will have to return the GRP to the factory for repair.

- Step 9** Repeat Step 4 through Step 8 for the remaining DIMM, as required.

Checking the DIMM Installation

After you install the new DIMMs and replace the GRP, turn on system power and allow the system to reboot.

**Note**

The time required for the system to initialize might vary with different router configurations and DRAM configurations. Routers with 256 MB or more of DRAM might take longer to boot than those with less DRAM.

If the system fails to boot properly, or if the console terminal displays a checksum or memory error, check the following:

- Ensure that all DIMMs are installed correctly. If necessary, shut down the system and remove the GRP to check the DIMMs. Look straight down on the DIMMs to inspect them at eye level. They all should be aligned at the same angle and the same height when properly installed. If a DIMM appears to stick out or rest in the socket at a different angle from the others, remove the DIMM and reinsert it. Then replace the GRP and reboot the system for another installation check.
- DIMMs must be extended data output (EDO), +3.3VDC, 60-ns DRAM devices. The speed is printed along one edge of the DIMM.

If after several attempts the system fails to restart properly, contact a service representative for assistance. Before you call, make note of any error messages, unusual LED states, or any other indications that might help solve the problem.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the installation and configuration guide for your Cisco 12000 Series Router.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.