Installing the Router

This chapter describes how to do the initial installation and setup of Cisco 12006 and Cisco 12406 Routers. It includes the following sections:

Installing a Router

This section explains the procedures for installing Cisco 12006 and Cisco 12406 Routers and contains the following sections:

Before installing Cisco 12006 and Cisco 12406 Routers, see Chapter 2, "Preparing for Installation," for information on environmental considerations and requirements.

Ensure the following before you install the router:

- The exhaust vents on the blower module mounted at the rear of the chassis are not blocked.
- The air filter is mounted on the right side as you face the router; air flow to the blower module is not blocked.
- There is 24 inches (61 cm) of clearance at the rear of the chassis so you can read the blower module LEDs and perform maintenance on the module.
- There is 24 inches (61 cm) of clearance in front of the router chassis to enable working with line cards and power supplies, and attaching Network Interface Cable (NICs) or other components.
- Location is temperature controlled, air conditioned, and dust free.
- Power cables and power supplies have been checked for compatibility with your power service.
- Labels on the equipment have been checked to ensure that the power service at your site is suitable for the router.
- AC power source receptacles are easy to reach.

Warning **Do not mix power module input types in the router. All power modules installed in a router must be either AC-input power supplies or DC-input PEMs.**

Installing the Rack-Mount Brackets (Optional)

The router accessory kit includes a pair of rack-mount brackets that can be used as a temporary aid to bear the weight of the router while it is being positioned in the equipment rack and secured. The use of these mounting brackets is optional; you can install the router in the rack without using these brackets. These brackets can be left in place following router installation.

Tools and Equipment Required

You need the following items to install the optional rack-mount brackets:

- Number 2 Phillips screwdriver
- Tape measure (optional)
- Level (optional)

Installing the Optional Rack-Mount Brackets

To install the rack-mount brackets, see Figure 3-1 and follow these steps:

Step 1 Measure and mark the hole at the same height on both the left and right rack rails.

Step 2 Mount the right mounting bracket:

a. Hold the right rack-mount bracket against the right rack rail and align the bottom screw hole in the bracket with the marked screw hole on the rail.

b. Insert a screw through the bottom hole in the bracket and finger tighten the screw.

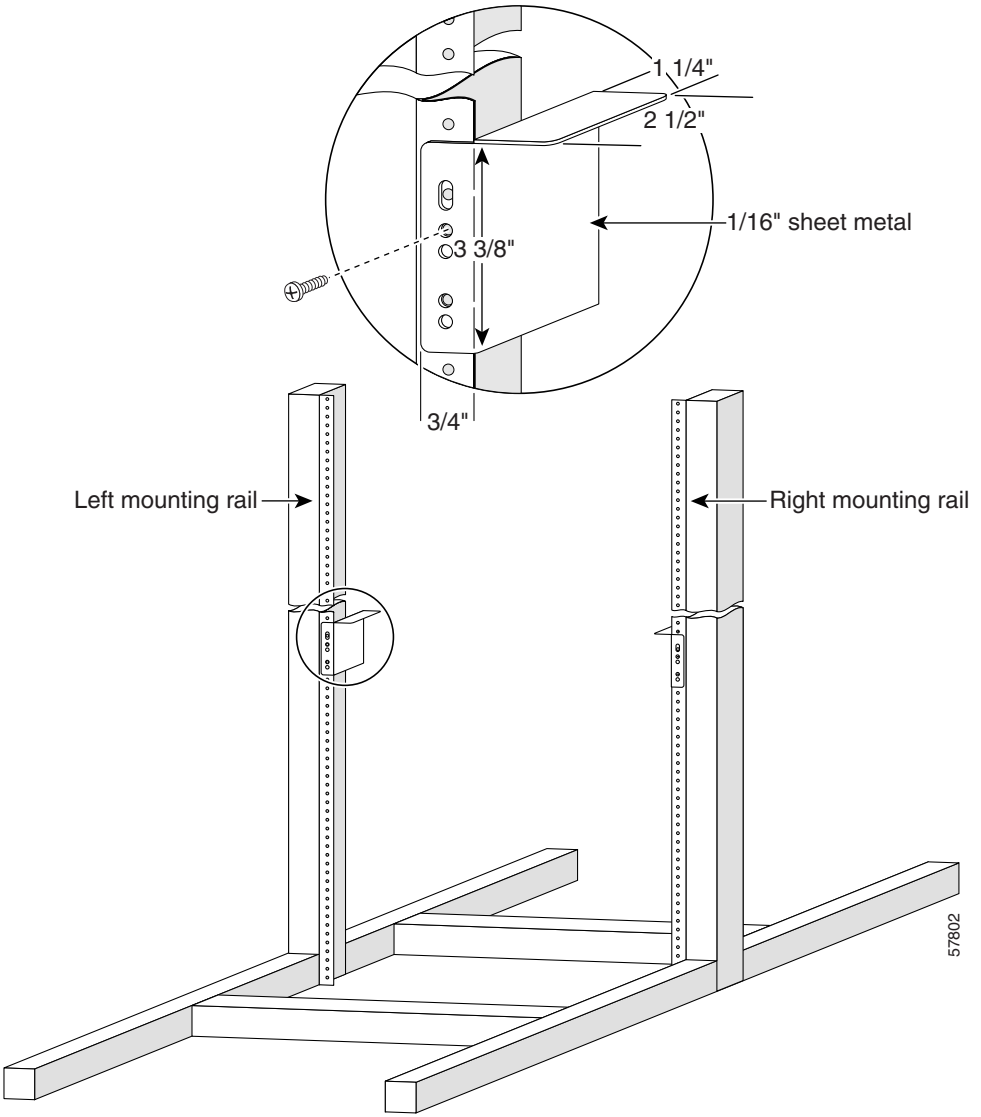
c. Insert and finger tighten a second screw in the top hole in the bracket.

Step 3 Follow Step 2a through Step 2c to mount the left rack-mount bracket.

Step 4 Use a level to verify that the tops of the two brackets are level, or use a measuring tape to verify that both brackets are the same distance from the tops of both rack rails.

Step 5 Use a screwdriver to tighten all the screws.

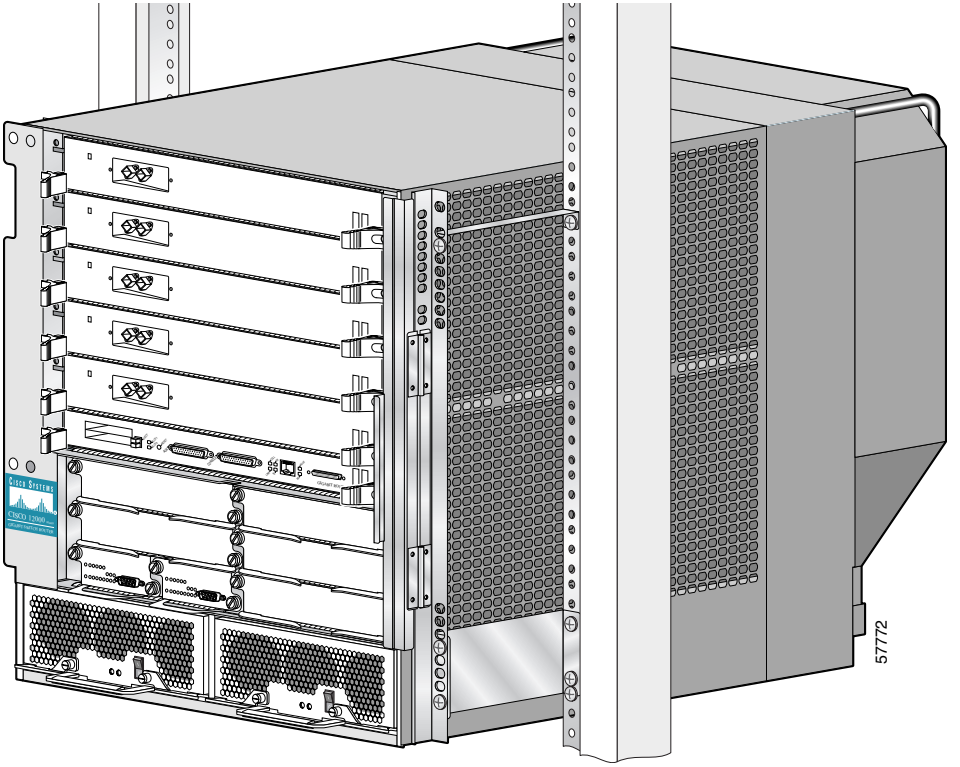
Figure 3-1 Installing the Optional Rack-Mount Brackets



Installing Center-Mount Brackets (Optional)

To install the Cisco 12006 or Cisco 12406 Router in the center-mount position, you must first install the upper and lower center-mount brackets on the equipment rack rails, then secure the chassis to the center-mount brackets. (See Figure 3-2.) If you do not plan to use the optional center-mount brackets, proceed directly to the "Installing the Chassis in a Rack" section on page 3-7.

Figure 3-2 Lower and Upper Center-Mount Brackets



The optional center-mount bracket installation kit ships in an accessories box included in the router shipping container. If any parts are missing, contact a Cisco service representative for assistance.

Tools and Equipment Required

You need the following items to install the optional center-mount rack-mounting brackets:

- Number 2 Phillips screwdriver
- Tape measure (optional)
- Level (optional)

Installing the Optional Center-Mount Brackets

To install the center-mount brackets, see Figure 3-2 and follow these steps:

Step 1 Measure and mark the hole at the same height on both the left and right posts.

Caution When installing the right side lower center-mount bracket, ensure that the bracket does not impede airflow through the air filter, which could cause overheating in the router.

Step 2 Mount the lower right bracket:

a. Hold the lower right bracket against the right rack rail and align the bottom screw hole in the lower bracket with the marked screw hole.

b. Pick a bottom bracket hole that aligns with a hole in the rack rail, then insert a screw in the hole and finger tighten the screw.

c. Insert a second screw in the top hole in the bracket and finger tighten that screw.

Step 3 Repeat Step 2a through Step 2c to mount the lower left center-mount bracket so that it is at the same height as the lower right bracket.

Step 4 Use a level to verify that the tops of the two brackets are level, or use a measuring tape to verify that both brackets are the same distance from the tops of both rack rails.

Step 5 Use a screwdriver to tighten all the screws.

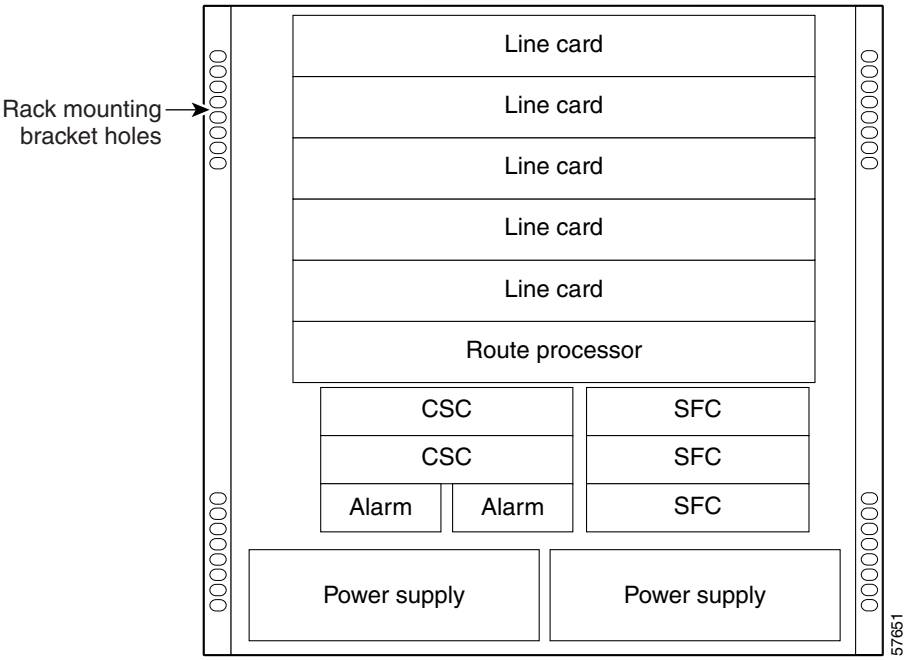
Step 6 Repeat Step 1 through Step 5 for both upper center-mount brackets.

Installing the Chassis in a Rack

This section explains how to install Cisco 12006 and Cisco 12406 Routers in a rack. This procedure assumes you have unpacked the router using the *Cisco 12006 and Cisco 12406 Router Unpacking and Repacking Instructions* (Document number 78-16104-xx) posted on the outside of the shipping container.

You mount the chassis in the equipment rack by setting the chassis in position against the rack rails and then securing it to the rack or optional center-mount brackets with screws through holes in the rack-mounting flanges on either side of the chassis. To accommodate racks with different hole patterns in their rails, the chassis rack-mounting flanges have two groups of eight oblong screw holes on either side. (See Figure 3-3.) The mounting holes in the chassis flanges are spaced so that one mounting hole in each hole group aligns with a hole in the rack rail or optional center-mount bracket. By using the corresponding mounting hole (in the same hole group) on the opposite side of the chassis, you can level the chassis in the rack.

Figure 3-3 Chassis Mounting Bracket Holes



To install the chassis in a rack, see Figure 3-3 and follow these steps:

Step 1 Move the router as close to the installation location as possible without interfering with the installation process.

Step 2 With one person lifting from the front and one from the rear of the chassis, grasp the front and rear of the chassis, lift the chassis off the pallet, and position the chassis in the rack.

Note A third person might be needed to assist in lifting and positioning the chassis in the rack.

Step 3 Install the screws to secure the chassis to the rack:

a. Look at the bottom mounting holes on the chassis rack-mount flanges. Align one of the holes with a mounting hole in the rack.

b. Install one of the mounting screws provided.

c. On the other side of the chassis, adjust the position of the chassis so that the same mounting hole in the bottom group of mounting holes is aligned with a hole in the rack.

d. Install one of the mounting screws provided.

Step 4 Repeat Step 3a through Step 3d for additional mounting holes.

Caution Do not allow the chassis to hang free until you have installed a screw in all four hole groups (at least two screws on each side of the chassis).

Step 5 Use a screwdriver to tighten all the screws.

Installing the Chassis on a Tabletop or Flat Surface

Follow the steps below to install a Cisco 12006 Router or Cisco 12406 Router on a tabletop or stable flat surface. You can use the same mounting hardware that secured your router to the shipping pallet to secure the chassis to a flat surface.

Step 1 Move the router as close to the installation location as possible.

Caution Do not lift the chassis by the blower module handle. This handle is designed to support only the weight of the blower module.

Step 2 With one person positioned at the front of the chassis and one at the rear, lift the chassis off the pallet and position the chassis on the flat surface.

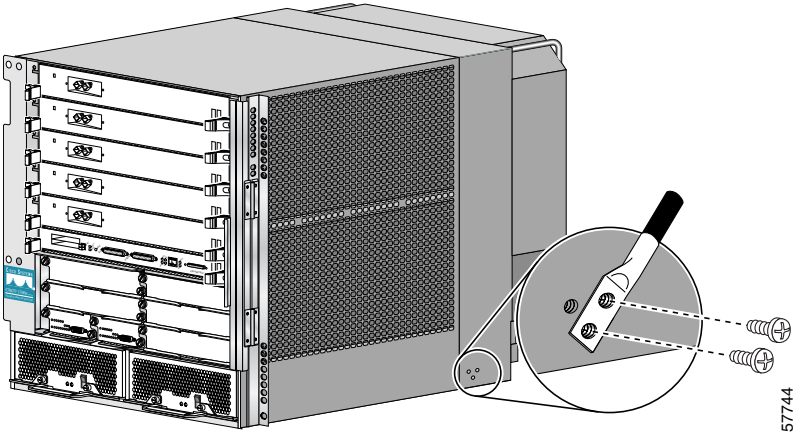
Step 3 Secure the chassis to the flat surface to ensure that it does not fall off.

Supplemental Bonding and Grounding Connections

If the router is installed in a network equipment building system (NEBS) environment, follow the guidelines in this section. For installations other than in a NEBS environment, you may chose to rely on the safety earth ground connection supplied via the International Electrotechnical Commission (IEC) 320 inlets for AC-powered units and the main terminal block ground connection for DC-powered units.

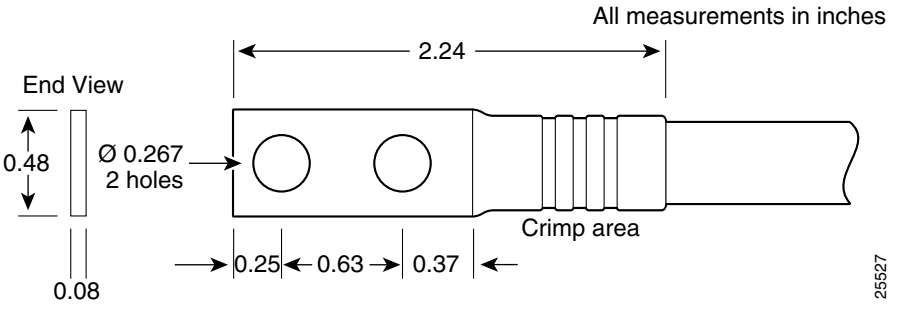
Even though the router chassis requires a safety earth ground connection as part of the power cabling to the PDU, we strongly recommend that you connect the central office ground system or interior equipment grounding system to the supplemental bonding and grounding receptacle on the router chassis, which satisfies the Telcordia NEBS requirement for supplemental bonding and grounding connections. This receptacle consists of three threaded inserts located on the side of the chassis near the back panel. (See Figure 3-4.)

Figure 3-4 Supplemental Bonding and Grounding Port for NEBS Compliance



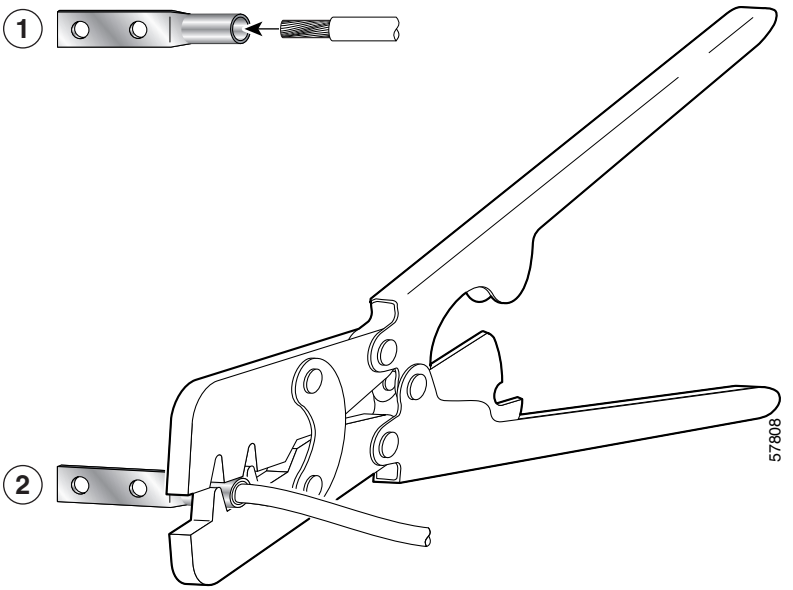
Use a dual-hole lug to connect to the chassis with two 6.3-mm (M6) screws on the 0.63-inch (16-mm) centers as shown in Figure 3-4 and Figure 3-5. The lug can be ordered from Cisco (Part Number 32-0607-01).

Figure 3-5 Cable Lug



The dual-hole lug is crimped onto a grounding wire of a wire size and length determined by your router location and facility environment. The crimping tool shown in Figure 3-6 is a standard crimping tool obtainable from many sources.

Figure 3-6 Crimping the Lug



1	Place ground wire in the lug	**2**	Crimp the lug

Note The three threaded inserts that make up the grounding receptacle are set in a triangle so that you can choose any two of the three holes to attach the lug and grounding cable.

Connecting RP and Line Card Cables

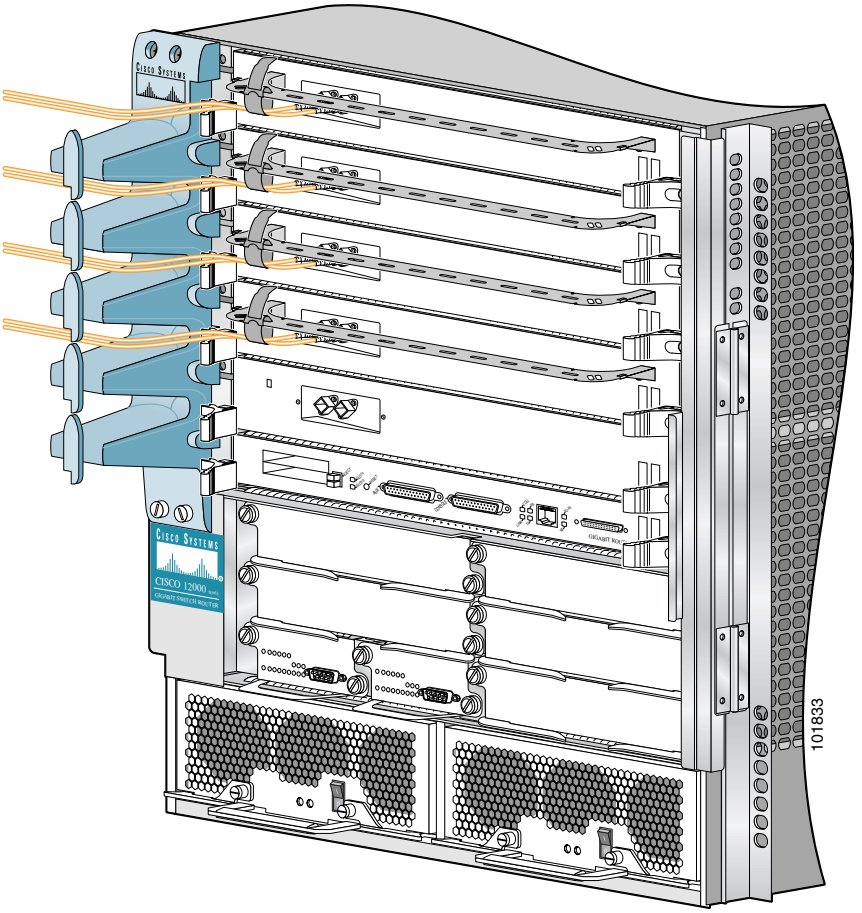
To connect RP and line card cables, see Figure 3-7 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Proceeding from left to right, identify the cables that attach to the first RP or line card.

Step 3 Carefully route the interface cable through the chassis cable-management bracket and across the card to the card interface port; do this for one cable at a time.

Figure 3-7 Chassis Cable-Management Bracket



Step 4 Proceeding from left to right, identify the cable that connects to each card port and connect the cable to the RP or line card port.

Step 5 Proceeding from left to right, carefully wrap the cables into the line card cable-management bracket using the velcro straps.

Caution Carefully adjust the cable in the cable-management brackets to prevent any kinks or sharp bends in the interface cable. Kinks and sharp bends can destroy or degrade the ability of the optical fiber to propagate the signal-encoded beam of light accurately from one end of the cable to the other. Also, allow adequate strain relief in the interface cable.

Step 6 Route the cable through the fingers on the vertical chassis cable-management bracket and turn the latch on the front of the bracket to secure the cables in the bracket.

Connecting Alarm Card Cables

Cisco 12006 and Cisco 12406 Routers have two alarm cards located in the two slots immediately above the left power supply bay and directly below the clock and scheduler card slots. Each alarm card is equipped with a standard DB-9 connector, labeled ALARM. This connector can be used to connect the router to an external site alarm maintenance system so that any critical, major, and minor alarms generated in the router also energize alarm relays on the alarm card and activate the external site alarm. Appendix A, "Technical Specifications," lists the pin-to-signal correspondence between the connector pins and the alarm card relay contacts.

Because alarm contact cables are entirely dependent on installation site circumstances, alarm connector cables are not available from Cisco Systems.

Note Only safety extra-low voltage (SELV) circuits can be connected to the alarm connector. Maximum rating for the alarm circuit is 2A, 50VA.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, you must use a shielded cable when connecting to the external alarm ports on the alarm card. The shielded cable is terminated by shielded connectors on both ends, with the cable shield material tied to both connectors.

Connecting to the Console and Auxiliary Ports

This section provides the information for connecting console terminals and other auxiliary devices to the console and auxiliary ports on the router. 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. GRP ports are discussed below. PRP ports are discussed in the "PRP Console and Auxiliary Ports" section on page 3-18.

GRP Console and Auxiliary Ports

This section provides connection equipment and pin designation information for the console and auxiliary ports on the Gigabit Route Processor (GRP).

Note To maintain Class B, EMI compliance, shielded cables must be used on the console and auxiliary ports of the GRP= and GRP-B=.

The GRP has two EIA/TIA-232 ports:

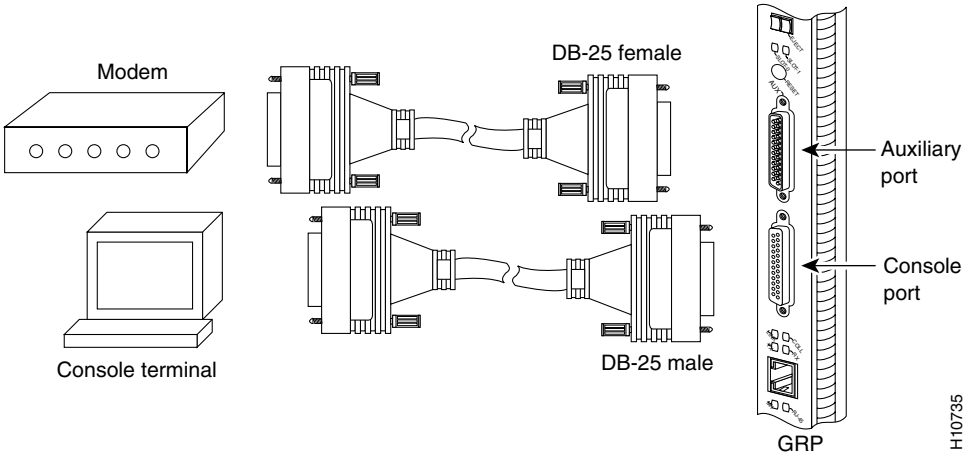
- DCE DB-25 receptacle for connecting a console terminal
- DTE DB-25 plug for connecting other DTE devices

The DCE-mode console port is a DCE DB-25 receptacle used for connecting a console terminal, which you will need to configure the router.

The DTE-mode auxiliary port is a DTE DB-25 plug for connecting a modem or other DCE device (such as a channel service unit/data service unit [CSU/DSU] or another router) to the router.

Note The console and auxiliary ports are 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.

Figure 3-8 GRP Console DCE and Auxiliary DTE Port Connections



Check your terminal documentation to determine the baud rate of the terminal you plan to use. If your documentation does not specify settings, use the following terminal settings: 9600 baud, 8 data bits, no parity, and 2 stop bits. You will need an EIA/TIA-232 DCE console cable to connect the terminal to the console port.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect all console, auxiliary, and Ethernet interfaces only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

GRP Console Port Signals

The console port on the GRP requires a straight-through EIA/TIA-232 cable. Table 3-1 lists the signal-to-pin correspondence for the GRP console port.

Table 3-1 GRP Console Port Pin Signals

Pin	Signal	Input/Output	Description
1	GND	–	Ground
2	TxD	Output	Transmit Data
3	RxD	Input	Receive Data
6	DSR	Input	Data Set Ready (always on)
7	GND	–	Ground
8	DCD	Input	Data Carrier Detect (always on)
20	DTR	Output	Data Terminal Ready

GRP Auxiliary Port Signals

The GRP auxiliary port is a DB-25 plug DTE port for connecting a modem or other DCE device (such as a CSU/DSU or other router) to the router. The auxiliary port is located next to the console port on the GRP card. The auxiliary port supports hardware flow control and modem control. An example of a modem connection is shown in Figure 3-8. Table 3-2 lists the signal-to-pin correspondence for the auxiliary port.

Note To maintain Class B EMI compliance, shielded cables must be used on the console and auxiliary ports of the GRP= and GRP-B=.

Table 3-2 GRP Auxiliary Port Signals

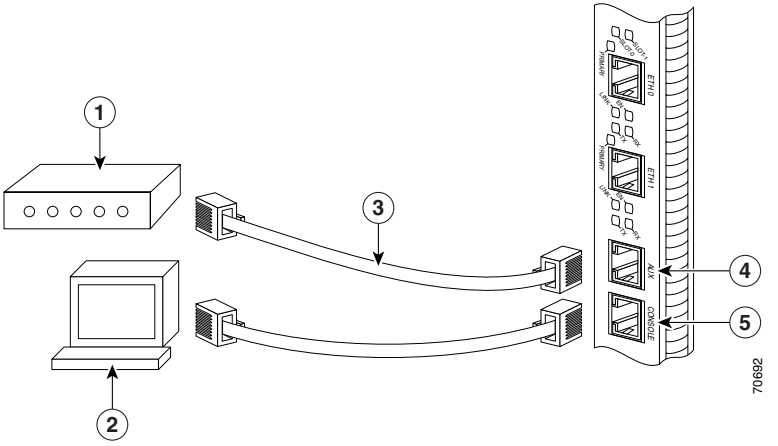
Pin	Signal	Input/Output	Description
1	Signal Ground	–	Signal Ground
2	TxD	Input	Transmit Data
3	RxD	Output	Receive Data
4	RTS	Input	Request To Send (used for hardware flow control)
5	CTS	Output	Clear To Send (used for hardware flow control)
6	DSR	Output	Data Set Ready
7	Signal Ground	–	Signal Ground
8	CD	Output	Carrier Detect (used for modem control)
20	DTR	Input	Data Terminal Ready (used for modem control only)
22	RING	Output	Ring

PRP Console and Auxiliary Ports

The system console port on the PRP is a DCE RJ-45 receptacle for connecting a data terminal, which you must configure. The console port is labeled *Console*, as shown in Figure 3-9. Before connecting the console port, check the documentation for your terminal to determine the baud rate.

If your documentation does not specify settings, use the following terminal settings: 9600 baud, 8 data bits, no parity, and 2 stop bits. The console port requires a rollover RJ-45 cable.

Figure 3-9 PRP Console and Auxiliary Port Connections



1	Modem	**4**	Auxiliary port
2	Console terminal	**5**	Console port
3	RJ-45 Ethernet cables	**–**	—

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.

Caution 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.

Note RP cables are not available from Cisco, but are available from any commercial cable vendor.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect all console, auxiliary, Ethernet, and BITS (PRP2) interfaces only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

PRP Console Port Signals

The console port on the PRP is a DCE RJ-45 receptacle. Table 3-3 lists the signal-to-pin correspondence for the PRP console port.

Table 3-3 PRP Console Port Signals

Console Port Pin	Signal	Input/Output	Description
1[1]	—	—	—
2	DTR	Output	Data Terminal Ready
3	TxD	Output	Transmit Data
4	GND	—	Signal Ground
5	GND	—	Signal Ground
6	RxD	Input	Receive Data
7	DSR	Input	Data Set Ready
8[1]	—	—	—

1. These pins are not connected.

PRP Auxiliary Port Signals

The auxiliary port on the PRP is a DTE, RJ-45 plug for connecting a modem or other DCE device (such as a CSU/DSU or another router) to the router. The port is labeled *AUX*, as shown in Figure 3-9. The asynchronous auxiliary port supports hardware flow control and modem control. Table 3-4 lists the signal-to-pin correspondence for the PRP auxiliary port.

Table 3-4 PRP Auxiliary Port Signals

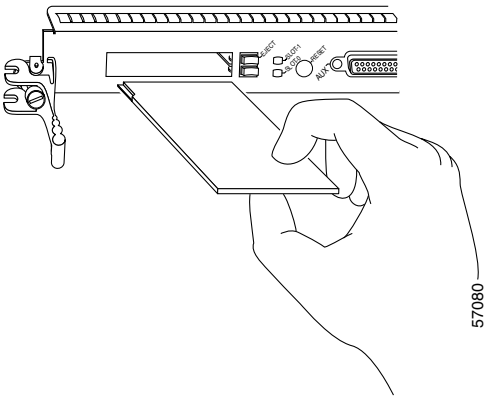
Auxiliary Port Pin	Signal	Input/Output	Description
1	RTS	Output	Request To Send
2	DTR	Output	Data Terminal Ready
3	TxD	Output	Transmit Data
4	GND	—	Signal Ground
5	GND	—	Signal Ground
6	RxD	Input	Receive Data
7	DSR	Input	Data Set Ready
8	CTS	Input	Clear To Send

Installing a Flash Memory Card

By default, a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 before the router is shipped. (See Figure 3-10.) PCMCIA slot 0 (SLOT-0) is the bottom slot and slot 1 (SLOT-1) is the top slot. Both Flash memory card slots on each RP can be used at the same time.

The software configuration register is set to 0x0102, which causes the router to boot automatically from the Cisco IOS software image stored on the Flash memory card.

Figure 3-10 Flash Memory Card Slot Opening

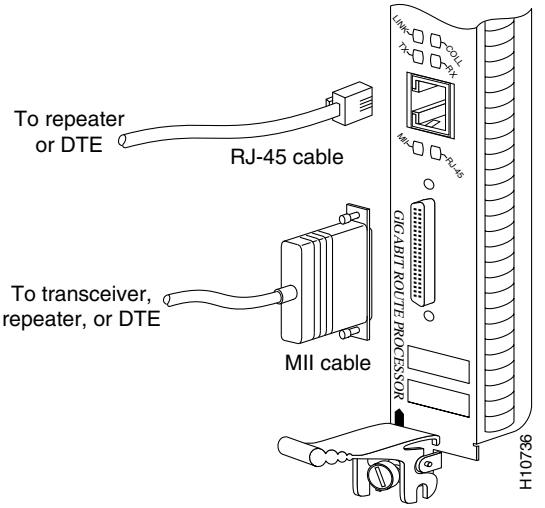


Ensure that a console terminal is connected to the RP console port and turned on, or that you have a remote login to the router from another device through a Telnet session.

Connecting the GRP to an Ethernet Network

This section provides information for connecting the GRP to an Ethernet network. Figure 3-11 shows the RJ-45 and MII Ethernet ports on the GRP.

Figure 3-11 RJ-45 and MII Ethernet Connections



The GRP has one Ethernet port, which uses either of these port connectors:

- RJ-45 receptacle—An 8-pin media-dependent interface (MDI) RJ-45 receptacle for either an IEEE 802.3 10BASE-T (10 Mbps) or an IEEE 802.3u 100BASE-TX (100 Mbps) connection.
- MII receptacle—A 40-pin media independent interface (MII) receptacle that provides additional flexibility in Ethernet connections. This connector can also be used for either an IEEE 802.3 10BASE-T (10 Mbps) or an IEEE 802.3u 100BASE-TX (100 Mbps) connection.

Note The RJ-45 and MII receptacles on the GRP represent two physical connection options for one Ethernet interface; you can use either the MDI RJ-45 connection or the MII connection, but not both simultaneously. The transmission speed of the Ethernet port is set through an auto-sensing scheme on the GRP.
The speed is determined by the network to which the Ethernet interface is connected, and is not user-configurable. Moreover, even at the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth of less than 100 Mbps. Expect a maximum usable bandwidth of approximately 20 Mbps when using either the MII or RJ-45 connection.

The Ethernet port can use either unshielded twisted-pair or screened twisted-pair cable. In sites where extremely high immunity to noise is required, screened twisted-pair cable is recommended. Figure 3-12 shows the layout of the Ethernet MII receptacle on the GRP.

Figure 3-12 Ethernet MII Receptacle

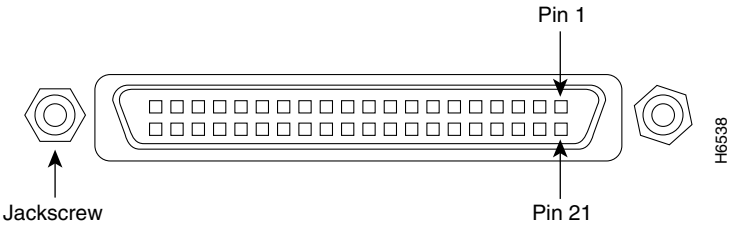


Table 3-5 lists the signal-to-pin correspondence for the Ethernet MII connector.

Table 3-5 Ethernet MII Pin Configuration

Pin[1]	In	Out	Input/Output	Description	Code
14 to17	–	Yes	–	Transmit Data	TxD
12	Yes	–	–	Transmit Clock	Tx_CLK[2]
11	–	Yes	–	Transmit Error	Tx_ER
13	–	Yes	–	Transmit Enable	Tx_EN
3	–	Yes	–	MII Data Clock	MDC
4 to 7	Yes	–	–	Receive Data	RxD

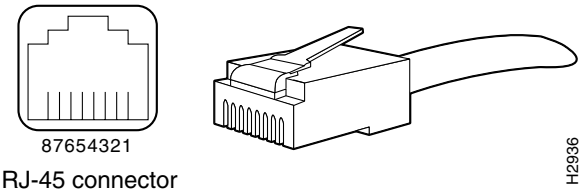
Table 3-5 Ethernet MII Pin Configuration (continued)

Pin[1]	In	Out	Input/Output	Description	Code
9	Yes	–	–	Receive Clock	Rx_CLK
10	Yes	–	–	Receive Error	Rx_ER
8	Yes	–	–	Receive Data Valid	Rx_DV
18	Yes	–	–	Collision	COL
19	Yes	–	–	Carrier Sense	CRS
2	–	–	Yes	MII Data Input/Output	MDIO
22 to 39	–	–	–	Common	Ground
1, 20, 21, 40	–	–	–	+5.0 V	V

1. Unlisted pins are not used.
2. Tx_CLK and Rx_CLK are provided by the external transceiver.

Figure 3-13 shows the pin configuration on the Ethernet RJ-45 receptacle on the GRP. Table 3-6 lists the signal-to-pin correspondence for the Ethernet RJ-45 receptacle on the GRP.

Figure 3-13 Ethernet RJ-45 Receptacle



RJ-45 connector

Table 3-6 Ethernet RJ-45 Receptacle Pin Configuration

Pin	Signal
1	TX+
2	TX–
3	RX+

Table 3-6 Ethernet RJ-45 Receptacle Pin Configuration (continued)

Pin	Signal
4	Termination Network
5	Termination Network
6	RX–
7	Termination Network
8	Termination Network

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.**

Connecting the PRP to an Ethernet Network

This section provides information for connecting the PRP on your router to an Ethernet network.

The PRP includes two 10/100 Mbps Ethernet ports, each using an 8-pin RJ-45 receptacle for either IEEE 802.3 10BASE-T (10 Mbps) or IEEE 802.3u 100BASE-TX (100 Mbps) connections. The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

The Ethernet interfaces on the PRP are end-station devices, not repeaters; therefore, you *must* connect an Ethernet interface to a repeater or hub. To connect cables to the PRP Ethernet interfaces (ports labeled ETH0 and ETH1), attach the Category 5 UTP cable directly to a RJ-45 receptacle on the PRP.

RJ-45 cables are not available from Cisco Systems, but are available from outside commercial cable vendors.

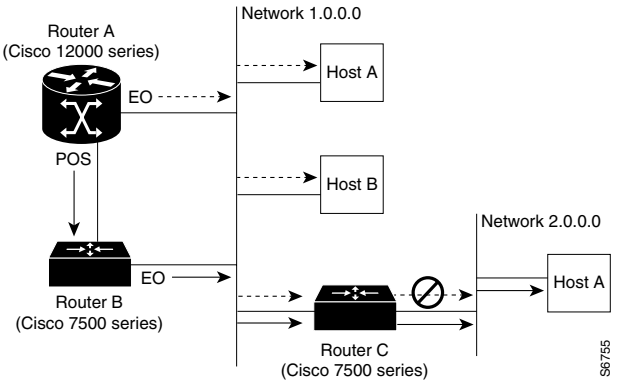
Note Use cables that comply with EIA/TIA-568 standards. (See Table 3-8 on page 3-29 and Table 3-9 on page 3-29 for cable recommendations and specifications.)

Caution The Ethernet ports are used primarily as Telnet ports into the router, and 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 3-14 shows an example of the functionality of an Ethernet port. In this example, you cannot access Network 2.0.0.0 via the Ethernet port (ETH0) on the PRP 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 3-14.)

To access Network 2.0.0.0 from Router A, use an interface port on one of the 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 3-14.)

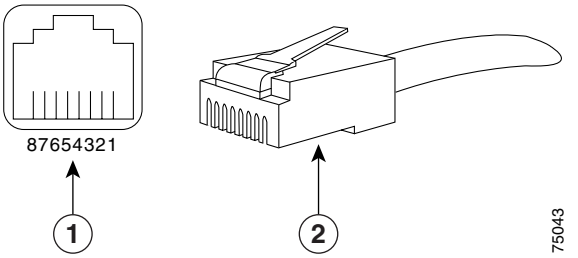
Figure 3-14 Using the Ethernet Port on the PRP



PRP Ethernet Connections

Figure 3-15 shows a PRP RJ-45 receptacle and cable connector. 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 3-7 lists the signal-to-pin correspondence for the RJ-45 receptacle.

Figure 3-15 RJ-45 Receptacle and Plug (Horizontal Orientation)



1	RJ-45 receptacle	**2**	Category 5 UTP cable with plug

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 BRI circuits are treated like telephone network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.**

Table 3-7 PRP RJ-45 Ethernet Receptacle Pinout

Ethernet Port Pin	Signal	Description
1	TxD+	Transmit data +
2	TxD–	Transmit data –
3	RxD+	Receive data +
4	Termination Network	No connection
5	Termination Network	No connection

Table 3-7 PRP RJ-45 Ethernet Receptacle Pinout (continued)

Ethernet Port Pin	Signal	Description
6	RxD–	Receive data –
7	Termination Network	No connection
8	Termination Network	No connection

Depending on your RJ-45 cabling requirements, use the connector pinouts shown in Figure 3-16 or Figure 3-17.

Figure 3-16 Straight-Through Cable Pinout (Connecting MDI Ethernet Port to MDI-X Wiring)

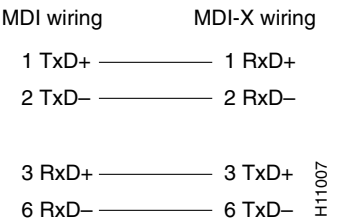


Figure 3-17 Crossover Cable Pinout (for Connecting Two PRPs)

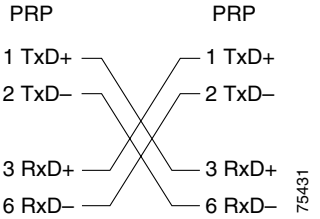


Table 3-8 lists the cabling specifications for 100-Mbps transmission over unshielded twisted-pair (UTP) cables.

Note The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

Table 3-8 Specifications and Connection Limits for 100-Mbps Transmission

Parameter	RJ-45
Cable specification	Category 5[1] UTP, 22 to 24 AWG[2]
Cable length (max)	—
Segment length (max)	328 feet (100 m) for 100BASE-TX
Network length (max)	656 feet (200 m)[3] (with 1 repeater)

1. EIA/TIA-568- or EIA-TIA-568 TSB-36-compliant. Not supplied by Cisco.
2. AWG = American Wire Gauge. This gauge is specified by the EIA/TIA-568 standard.
3. This length is specifically between any two stations on a repeated segment.

Table 3-9 lists IEEE 802.3u physical characteristics for 100BASE-TX.

Table 3-9 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)
Topology	Star/Hub

1. DTE = data terminal equipment.

Connecting to an AC Power Source

This section presents the procedure for connecting your router to an AC power source. A power factor corrector (PFC) allows the AC-input power supply to accept AC power source voltage from an AC power source operating between 100 and 240 VAC, 20-Amp service in North America; and a range of from 185 to 264 VAC, 16-Amp service in an international environment.

Caution The AC-input power supply weighs 14 pounds (6.4 kilograms). Use two hands when handling a power supply.

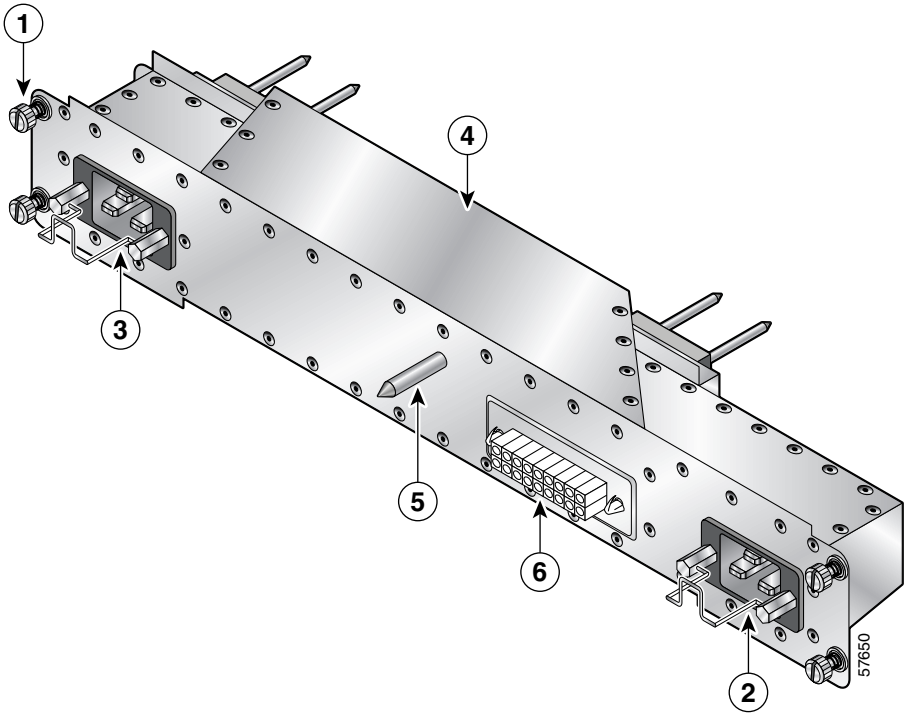
Warning **The AC-input power supply power standby switch should be in the OFF position.**

When operating your router on a power source, the power supply bays must have one of the following power combinations installed before operating the router:

Table 3-10 Required Power Combinations

Router Power	Combination
AC power	1 AC-input power supply 1 power supply blank
	2 AC-input power supplies
DC power	1 DC-input PEM 1 PEM blank
	2 DC-input PEMs

Figure 3-18 AC Power Distribution Unit



1	Captive screws (four)	**4**	AC power distribution unit
2	AC power cord receptacle A	**5**	Guide pin
3	AC power cord receptacle B	**6**	Blower module connector

To connect AC power to the AC PDU on the router, see Figure 3-18 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Locate the two AC power cords and remove them from their shipping packaging. Verify that the AC power cords shipped with the power supplies are the correct type for your site.

Note If you have received the wrong type of AC power cord, contact your service representative for a replacement.

Step 3 Plug the socket end of each AC power cord into a receptacle on the PDU. (See Figure 3-18.)

Step 4 Insert the plug end of each AC power cord into the AC power source outlet.

For full redundancy, connect each AC-input power supply to an independent power circuit with its own circuit breaker. We also recommend that you use an uninterruptable power source (UPS) to protect against power failures at your site.

Step 5 Verify that the AC power source circuit breaker servicing each of the AC-input power supplies is switched on.

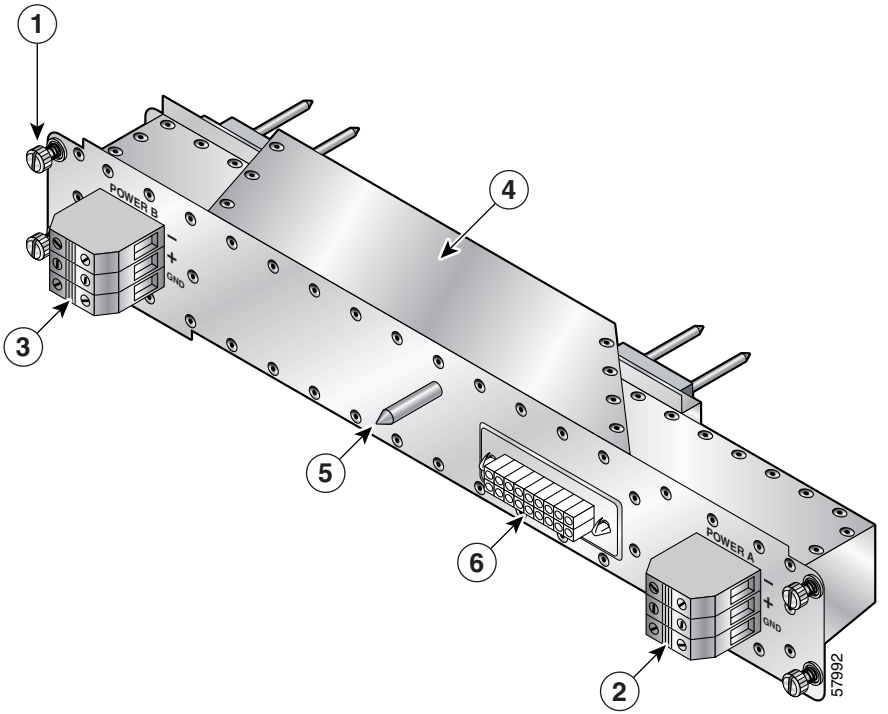
Note When operating your router on a single power module, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

Connecting to a DC Power Source

This section provides the procedure for connecting the router to a DC power source.

Warning **The circuit breaker switch on the faceplate of the DC-input PEM should be in the OFF position.**

Figure 3-19 DC PDU



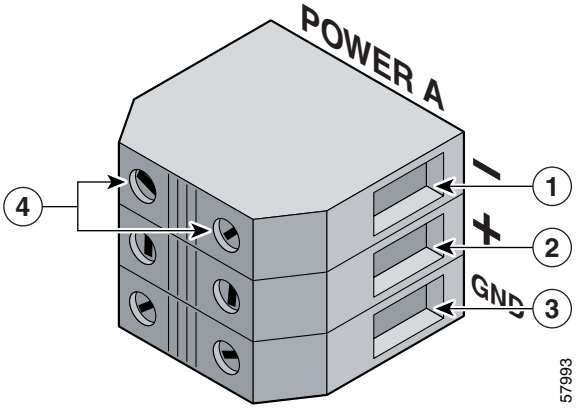
1	Captive screws (four)	**4**	DC PDU
2	DC power connector block (A)	**5**	Guide pin
3	DC power connector block (B)	**6**	Blower module connector

To connect source DC power to the DC PDU, see Figure 3-19 and Figure 3-20 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Locate the DC PDU on the back of the router. The PDU is positioned directly below and behind the blower module.

Figure 3-20 DC PDU Power Connector Block



1	Negative terminal port	**3**	Ground terminal port
2	Positive terminal port	**4**	Terminal port connector screws

Step 3 Connect the source DC power leads to the three terminal ports in the DC power connector block (see Figure 3-20) in this order:

- Ground lead first (bottom port on the connector block)
- Positive lead second (middle port on the connector block)
- Negative lead last (top port on the connector block)

a. Push the lead into the connector block port.

b. Use a flat-blade screwdriver to tighten the set screw and secure the lead.

c. Repeat Step 3a and Step 3b for the remaining leads and for the second PDU connector block.

Step 4 Verify that the source DC circuit breaker servicing the DC PDU is switched on.

Power On the Router

To power on the router, follow these steps:

Step 1 Either switch on all the circuit breakers or plug the power cord into an active power source that controls power to the PDU in the router.

During the first-time startup, the system displays the system banner information. Check the startup banner and displays to ensure that the system has restarted properly and that all the interfaces reinitialize properly.

Step 2 Check the power module LEDs. They should appear as described below:

- For a router equipped with AC-input power supplies:
  - Green LED labeled AC—When the power module is fully seated in its bay and is receiving source power within the required range, this LED should be on. It indicates that AC power is present and is within specified limits. The power supply fan should also be on.
  - Green LED labeled DC—Power supply is operating normally in a powered-on condition.
- For a router equipped with DC-input PEMs:
  - Green LED labeled INPUT OK—When the power module is fully seated in its bay and is receiving source power within the required range, this LED should be on. It indicates that DC power is present and is within specified limits. The power supply fan should also be on.
  - Green LED labeled OUTPUT OK—DC-input PEM is operating normally in a powered-on condition.
  - Amber LED labeled MISWIRE—Should be off. When it is on, it indicates that the input is wired backward at the PDU input.

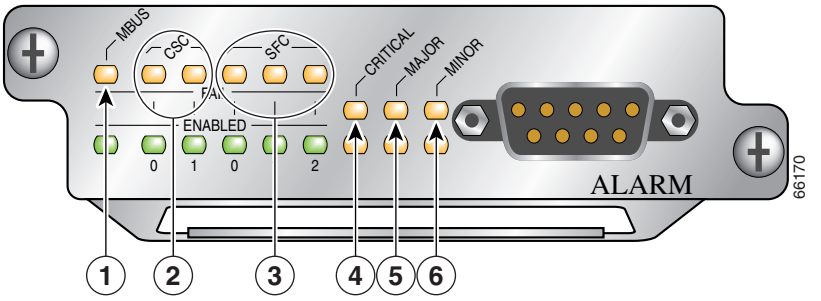
Step 3 Go to the rear of the chassis and visually check the two LEDs on the front of the blower module. They should appear as described below:

- Green LED labeled OK—Should be on
- Red LED labeled FAIL—Should be off

Step 4 Listen for the blowers in the blower module; you should immediately hear them operating.

Note In a noisy environment, the blowers might be difficult to hear; in that case, place your hand in front of the exhaust vents at the rear of the chassis to verify that the blowers are operating.

Figure 3-21 Alarm Card LEDs On/Off Conditions



1	MBus status LED	**4**	Critical alarm LED
2	CSC status LEDs (two)	**5**	Major alarm LED
3	SFC status LEDs (three)	**6**	Minor alarm LED

Step 5 Visually check the LEDs on the two alarm cards. (See Figure 3-21.) When the system is operating correctly, the following LED conditions should be true.

LEDs that normally should be off:

- One MBUS status LED labeled FAIL
- Two CSC status LEDs labeled FAIL
- Three SFC status LEDs labeled FAIL
- Three router alarm LEDs labeled CRITICAL, MAJOR, MINOR

LEDs that normally should be on:

- One MBUS status LED labeled ENABLED
- Two CSC status LEDs labeled ENABLED
- Three SFC status LEDs labeled ENABLED

Step 6 On the console terminal, verify that the console displays the system banner and that the system and all interfaces initialize successfully.

If the power modules do not power up, or if the system or any interfaces do not initialize properly, see Chapter 4, "Troubleshooting the Installation." If you are still unable to resolve the problem, contact your Cisco service representative for assistance.

IOS Software Configuration for the Router

This section explains how to configure your system so that it can access the network or enable other hosts on the network to access your system remotely by means of a Telnet connection. You can find more information in the configuration publications listed in the "If You Need More Information" section on page 3-82.

The system startup process and a procedure for performing a basic configuration of your router are presented in the following sections:

Cisco IOS Software Images

A default Cisco IOS software image for your system is available through any of the internal or external sources described in Table 3-11.

Table 3-11 Cisco IOS Software Image Sources

Onboard Flash Memory on the Gigabit Route Processor (GRP)	The latest Cisco IOS software image is loaded into the Flash memory, a single inline memory module (SIMM) that is preloaded at the factory before the router is shipped. The Flash memory SIMM is also referred to as nonvolatile random access memory (NVRAM). This type of memory retains its contents when system power is off.
Flash Memory Card	A Flash memory card inserted in a PCMCIA slot on the GRP, and loaded with the default software image, can serve as an external storage medium for the default Cisco IOS software image shipped with your router.
TFTP Server	You can download and store a valid Cisco IOS software image via a Trivial File Transfer Protocol (TFTP) using a Telnet connection.

Conditions to Check Before System Startup

Ensure that the following conditions are met before starting up the router:

- All cards are completely inserted into their card cage slots
- All captive screws are tightened
- All interface cable connections are secure
- All the power source cables are secured to the PDU
- All power cables are connected to the appropriate power source
- A terminal device is connected, powered on, and configured to 9600 bps, 8 data bits, no parity, and 2 stop bits (9600,8N2)
- A Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 (zero)

By default, the software configuration register is set to 0x0102, causing the system to boot automatically from the Cisco IOS software image stored on the Flash memory card. New Flash memory cards must be formatted before use. To format a new Flash memory card, refer to the section "Formatting a Flash Memory Card, page 3-67".

Overview of the Boot Process

The example below assumes that the router is plugged into a power source and the router is running, blower module fans are audible, and alarm card ENABLED LEDs are lit up.

The following is an example of a typical boot process:

- The RP MBus module receives the correct DC voltage and starts executing MBus software.
- The RP determines the router configuration by sending a message via the alarm card requesting all installed devices to identify themselves. Their responses provide slot numbers and card and component types. The RP, line cards, CSCs, and SFCs are then powered up.
- The power-on-reset logic of the RP is delayed long enough to allow power and both local and CSC clocks to stabilize.
- After the power-on reset logic is released, the RP begins to execute the ROM monitor software.
- If the ROM monitor is configured to autoboot, it automatically loads and boots the Cisco IOS software.
- If the ROM monitor is not configured to autoboot, boot the Cisco IOS software manually. See the "Manually Booting the System" section on page 3-47.
- When the Cisco IOS software boots, it polls all other cards in the system, powers them up, and loads the Cisco IOS software they require.

Starting the Router and Observing Initial Conditions

Observe the following conditions the first time you start your router:

- Power cables to the PDU are fully connected to both the PDU and the power source, and are secured with appropriate strain relief.
- Empty card slots or card bays are filled with card blanks. This ensures proper air flow through the chassis and electromagnetic compatibility (EMC).
- All cards are fully inserted in their cages and bays.
- All captive screws are tightened.

- Line card cable-management brackets are attached to their respective line cards.
- Interface cables are completely seated in their line card connectors.
- Interface cables are routed neatly through the chassis cable-management bracket.

Caution Do not overtighten the captive screws on the cards; you might strip the threads on the screw or in the insert in the component faceplate.

- Power modules are fully inserted in their bays and the ejector levers are completely closed and secured.
- Check the power module LEDs:

  For a router equipped with AC-input power supplies, when a power supply is seated in its bay and is receiving the required power source:

  - The green LED labeled AC should be on. It indicates that AC power source is present and is within specified limits.
  - The green LED labeled DC should be on. It indicates that the power supply is operating normally in a powered-on condition.

  For a router equipped with DC-input PEMs—When a PEM is seated in its bay and is receiving the required power source:

  - The green LED labeled INPUT OK should be on. It indicates that DC power source is present and is within specified limits.
  - The green LED labeled OUTPUT OK should be on. It indicates that the PEM is operating normally in a powered-on condition.
  - The amber LED labeled MISWIRE should be off. When it is on, it indicates that the input is wired backward at the PDU input.
- Each power module fan should also be on.

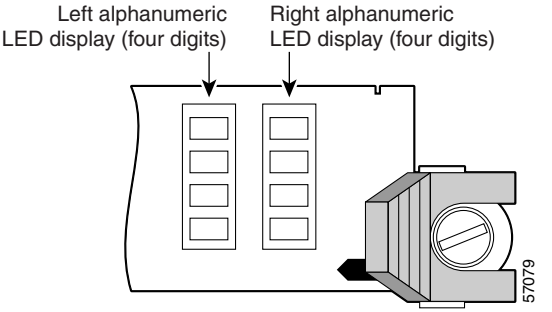
At the rear of the chassis, observe the status of the two LEDs on the blower module. When the blower module is operating correctly, the left LED should should be on (green) and the right LED (red) should be off.

Listen for the blowers in the blower module; they should be running. In a noisy environment, the blower might be difficult to hear. In that case, place your hand near the exhaust vents at the top and bottom rear of the chassis to verify that the blower is operating.

RP Alphanumeric LED

RP alphanumeric LEDs are located at one end of the RP faceplate, near the ejector lever. Figure 3-22 shows the RP LED displays.

Figure 3-22 RP Alphanumeric LED Displays



Each four-digit display shows part of a two-line system message. During the RP boot process, the LED displays present a sequence of messages similar to that shown in Table 3-12.

Table 3-12 LED Display Meaning and Signal Source

LED Display	Meaning	Source
MROM *nnnn*	The MBus microcode begins to execute; *nnnn* is the microcode version number. For example, microcode version 1.17 displays as 0117.[1] Note This display might not be visible because it occurs for only a brief time.	MBus controller
LMEM TEST	Low memory on the RP is being tested.	RP ROM monitor
MEM INIT	The size of main memory on the RP is being discovered.	RP ROM monitor
RP RDY	The system is operational and ready to execute basic Cisco IOS software commands at the ROM monitor prompt (`rommon>`).	RP ROM monitor

Table 3-12 LED Display Meaning and Signal Source (continued)

LED Display	Meaning	Source
RP UP	A valid Cisco IOS image is running.	RP IOS software
PRI RP	The RP is enabled and recognized as the system primary. A valid Cisco IOS image is running.	RP IOS software
SEC RP	The RP is enabled and recognized as the system secondary. A valid Cisco IOS image is running.	RP IOS software

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

RP Interfaces Using the RP LEDs

Two types of RPs are available for Cisco 12006 and Cisco 12406 Routers: the Gigabit Route Processor (GRP) and the Performance Route Processor (PRP).

Each of these route processor types is reviewed in the following sections:

- GRP Interfaces Using the GRP LEDs, page 3-43
- PRP Interfaces Using the PRP LEDs, page 3-44

Note When not explicitly specified, this publication uses the term route processor (RP) to indicate either the GRP or the PRP.

The RJ-45 port LEDs on the RP indicate the following conditions:

- System and RP status
- Which Flash memory card slot is active
- Which Ethernet connection is in use
- What is occurring on the Ethernet interface

The alphanumeric LED displays indicate a successful RP boot.

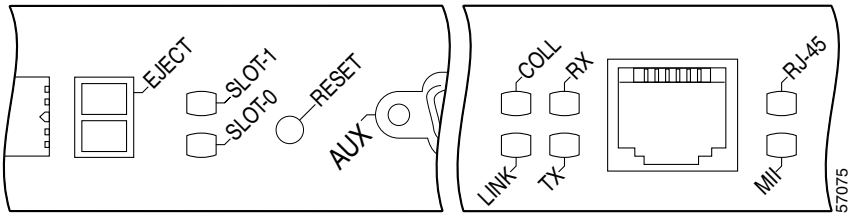
GRP Interfaces Using the GRP LEDs

The GRP faceplate has eight device or port LED activity indicators. Each LED goes on when its corresponding PCMCIA slot is accessed. The ports are as follows:

- Two PCMCIA slot activity LEDs labeled SLOT-0 and SLOT-1.
- Four RJ-45 Ethernet port activity LEDs. These LEDs are used only by the RJ-45 Ethernet connector, and are disabled when the MII Ethernet port is in use.
- Two Ethernet port-selection LEDs labeled MII and RJ-45.

When the Ethernet port LEDs are lit, they identify which of the two Ethernet connections is selected. When the RJ-45 port is selected, that LED is on and the MII LED is off. When the MII port is selected, that LED is on and the RJ-45 LED is off. (See Figure 3-23.)

Figure 3-23 RP RJ-45 and MII Ports LEDs



LINK	Indicates link activity
COLL	Indicates collision detection
TX	Indicates data transmission
RX	Indicates data reception

When you start an unconfigured system for the first time, the console screen displays a system banner and then automatically starts the System Configuration Dialogue. Observe the Cisco IOS banner on the console screen. If a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 and the software configuration register is set to 0x0102 (the factory default setting), the router automatically boots using this image.

As the router boots the Cisco IOS software image, the console screen displays a system banner similar to the following:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
.
.
.
```

Note The system banner that appears depends on the image version of the Cisco IOS software that the system is running.

If the ROM monitor prompt (`rommon>`) appears on the system console, your router did not find a valid system image, or the boot sequence was otherwise interrupted, and the system entered read-only memory (ROM) monitor mode.

To boot a Cisco IOS software image manually, enter the **boot** command on the system console. For information on using the various forms of the **boot** command, see the following sections:

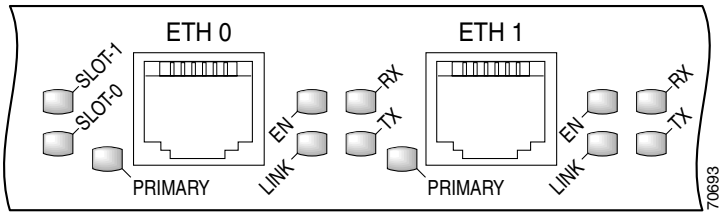
- Locating a Valid Cisco IOS Software Image, page 3-47
- Booting from the Cisco IOS Software Image, page 3-48

PRP Interfaces Using the PRP LEDs

The PRP faceplate has eight device or port LED activity indicators. (See Figure 3-24.) Each LED goes on when its corresponding PCMCIA slot is accessed. The ports are as follows:

- Two PCMCIA slot activity LEDs labeled SLOT-0 and SLOT-1.
- Four RJ-45 Ethernet port activity LEDs. These LEDs are used by the RJ-45 Ethernet connectors. Each connector includes four LEDs that indicate link activity (LINK), port enabled (EN), data transmission (TX), and data reception (RX).
- Two Ethernet port-selection LEDs labeled PRIMARY. These two LEDs, when on, identify which of the two Ethernet connections is selected. Because both ports are supported on the PRP, the LED on port ETH0 is always on. The ETH1 LED goes on when it is selected.

Figure 3-24 PRP LEDs



LINK	Indicates link activity
EN	Indicates the port is enabled
TX	Indicates data transmission
RX	Indicates data reception

When you start an unconfigured system for the first time, the console screen displays a system banner and then automatically starts the System Configuration Dialogue. Observe the Cisco IOS banner on the console screen. If a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 and the software configuration register is set to 0x0102 (the factory default setting), the router automatically boots using this image.

As the router boots the Cisco IOS software image, the console screen displays a system banner similar to the following:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
.
.
.
```

Note The system banner that you see depends on the image version of the Cisco IOS software that the system is running.

If the ROM monitor prompt (`rommon>`) appears on the system console, your router did not find a valid system image, or the boot sequence was otherwise interrupted, and the system entered read-only memory (ROM) monitor mode.

To boot a Cisco IOS software image manually, enter the **boot** command on the system console. For information on using the various forms of the **boot** command, see the following sections:

- Locating a Valid Cisco IOS Software Image, page 3-47
- Booting from the Cisco IOS Software Image, page 3-48

System Configuration Dialogue

The following information is an example of a System Configuration Dialog interactive script message that appears on the system console. This interactive script prompts you through the steps to create a router configuration database file defining basic system operation parameters.

```
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

External Network Interface

After configuration, the RP and line cards can communicate with external networks. You do not need to configure the network interfaces immediately, but you cannot connect to a network until you configure the interfaces for operation in your networking environment. For configuration information, see the "Router Configuration" section on page 3-49.

Note The interface-specific LEDs on the line cards go on when the line card interfaces are configured.

To verify correct operation of each line card interface, complete the first-time setup procedures and configuration, then check the status of the interfaces against the LED descriptions in the configuration notes for each line card.

If the system does not complete each of the boot process steps, see Chapter 4, "Troubleshooting the Installation."

Manually Booting the System

If your router does not find a valid system configuration image, or if you interrupt the boot sequence, the system might enter read-only memory (ROM) monitor mode and display the ROM monitor prompt (`rommon>`). From ROM monitor mode, you have access to a number of commands to locate and boot a valid system image.

Locating a Valid Cisco IOS Software Image

To locate a Cisco IOS software image for manually booting the router from the ROM monitor prompt (`rommon>`), follow the steps below:

Step 1 Use the ROM monitor mode **dir bootflash** command to examine the contents of the onboard Flash memory SIMM (NVRAM) on the RP:

```
rommon 1> dir bootflash:
   File size                  Checksum      File name
   3277967 bytes (0x32048f)   0x6b331e30    gsr-p-mz.120-7.4.5
rommon 2>
```

Step 2 If the onboard Flash memory SIMM contains the desired Cisco IOS boot image, proceed to the "Booting from the Cisco IOS Software Image" section on page 3-48. Otherwise, continue looking for a valid image by examining the contents of the Flash memory card in either PCMCIA slot 0 or slot 1 on the RP.

You can determine the content of the card by issuing the ROM monitor mode **dir slot*n*:** command, where *n* represents either 0 (slot 0) or 1 (slot 1). The following example of the command lists the contents of the Flash memory card in slot 0:

```
rommon 2> dir slot0:
   File size                  Checksum      File name
   3277967 bytes (0x32048f)   0x6b331e30    gsr-p-mz.120-7.4.5
rommon 3>
```

Booting from the Cisco IOS Software Image

After locating a valid Cisco IOS software image, you can boot from that image manually by issuing the appropriate ROM monitor mode **boot** commands from the list in Table 3-13.

Table 3-13 ROM Monitor Boot Commands

Command	Description
boot	(No argument.) Boots the default image found in the onboard Flash memory SIMM. The image is loaded into the SIMM at the factory.
boot flash	Attempts to boot the router using the first file found in the Flash memory card inserted in slot 0 of the RP.
boot slot0: *filename*	Boots the router using the specified file from the Flash memory card in slot 0 of the RP.
boot slot1: *filename*	Boots the router using the specified file from the Flash memory card in slot 1 of the RP.
boot bootflash: *filename*	Boots the router using the specified file from the onboard Flash memory SIMM (NVRAM) on the RP.
boot tftp: *filename* [*host*]	Boots the router using the specified file from a host TFTP server in the network.

Ensure that the Flash memory card inserted in PCMCIA slot 0 contains a valid Cisco IOS software image. Otherwise, the system will boot an invalid image from the Flash memory card. To examine the contents of a Flash memory card, enter the **dir slot***n***:** command.

If you did not change the contents of the software configuration register, the factory default setting of 0x0102 in the software configuration register causes the system to boot Cisco IOS software from a Flash memory card inserted in PCMCIA slot 0 the next time you boot the router.

Router Configuration

You can perform a basic configuration for your router by using either the **setup** command automatic prompt method, or the global configuration method in which you enter each option and parameter manually. Configuration is described in these sections:

Before You Begin

Before you begin the configuration process for your router, you should have the following information available:

- Interfaces the router will use
- Routing protocols the router will support
- Network addresses for the protocols being configured
- Password scheme for your environment

setup Command

One option is to use the **setup** command, also known as the **setup** command utility. During the first startup of an unconfigured router, the system automatically starts the **setup** command utility, which enables you to begin configuring your router. The **setup** command utility presents a structured, interactive script that guides you through the process.

You can invoke the **setup** command utility at any time by issuing the **setup** command at the privileged EXEC mode prompt (`Router#`), which invokes the same configuration script that appears automatically during the first startup of an unconfigured router. You can enter the **setup** command at any time to alter previously entered configuration information.

The advantage in using the **setup** command utility is that the system uses an interactive script to guide you through the configuration process.

Global Configuration Mode

The router can be configured manually using the global configuration mode through the Cisco IOS command line interface (CLI). This method requires you to enter configuration commands on a line-by-line basis at the system console, without being prompted by the **setup** command configuration script.

Cisco IOS User Interface

The Cisco IOS software provides a command line interface by which you can configure and manage your router. If you are unfamiliar with the Cisco IOS command line interface, refer to the "Using the Command Line Interface" chapter in the Cisco *Configuration Fundamentals Configuration Guide*, which discusses different command modes, context-sensitive help, and editing features.

User Interface Command Modes

The Cisco IOS user interface is organized into many different modes. The commands that are available depend on which mode you are currently in. Entering a question mark (?) at the system prompt displays a list of commands available for the current command mode.

When you start a session on the router, you begin in user mode, often called EXEC mode. Only a limited subset of commands are available in EXEC mode. To have access to all commands, enter privileged EXEC mode, which requires that you enter a password. From privileged EXEC mode, you can enter any EXEC command or enter global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the router.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored and can be used when you reboot your router. Starting at global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and other protocol-specific modes.

ROM monitor mode is a separate mode used when the router cannot boot properly. If the router does not find a valid system image when it is booting, or if the router configuration file is corrupt at startup, the system might enter ROM monitor mode.

User EXEC Mode

After the router boots successfully and loads the Cisco IOS software, the system software displays the user EXEC mode prompt on the system console. The user EXEC mode prompt consists of the assigned router host name plus the greater than bracket (>). The default host name is `router` unless it has been changed during initial configuration using the **setup** command facility. The user EXEC mode prompt for a router with the factory default name is Router.

```
Router>
```

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access should be password protected to prevent unauthorized use. To enter privileged EXEC mode, enter the **enable** command at the user EXEC mode prompt. If the **enable** secret password was set and saved in memory, the system prompts you to enter the **enable** secret password. The password is not displayed on the screen and is case sensitive. When the system accepts the password, it changes the prompt to the privileged EXEC mode prompt, which consists of the assigned router host name followed by the pound sign (#). The following example shows the change from user EXEC mode to privileged EXEC mode on the router named Router.

```
Router> enable
password: <password>
Router#
```

For information about using passwords, see the "Configuring Global Parameters" section on page 3-57.

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just one protocol or interface. Use the **configure terminal** privileged EXEC command to enter global configuration mode. Commands to enable a particular routing or bridging function are global configuration commands.

Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface, such as Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as bandwidth or clock rate, refer to the "Interface Commands" chapter in the *Configuration Fundamentals Command Reference*. For protocol-specific commands, see the appropriate Cisco IOS software command reference.

Subinterface Configuration Mode

You can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. Subinterfaces appear to be distinct physical interfaces to the various protocols. For detailed information on how to configure subinterfaces, see the appropriate module for a specific protocol in the Cisco IOS software documentation.

ROM Monitor Mode

If your router does not find a valid system image, or if you interrupt the boot sequence, the system might enter read-only memory (ROM) monitor mode. From ROM monitor mode, you can boot the system or perform diagnostic tests. You also can enter ROM monitor mode by entering the **reload** EXEC command and then pressing the Break key during the first 60 seconds of startup.

Configuration Changes

This section describes how to configure the router. It includes information on the following topics:

During the first-time startup of an unconfigured router, the system automatically starts the **setup** command utility and begins displaying the interactive System Configuration Dialog on the system console screen. The System Configuration Dialog guides you through the configuration process with prompts for global (system-wide) parameters and interface (line card) parameters.

The System Configuration Dialog prompts and the order in which they appear on the screen vary depending on the platform, interfaces installed, router, and the Cisco IOS software image the router is running.

Let the entire System Configuration Dialogue script run, until you come to the item that you want to change. To accept default settings for items that you do not want to change, press the console keyboard **Return** key. To return to the privileged EXEC prompt without making changes, press **Ctrl-C**. To access help text in the setup command utility, press the question mark key (?) at any prompt.

When you complete your changes, the **setup** command utility displays the configuration command script that was created as a result of the changes entered during the setup session. It also queries if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

The "setup Command Interactive Script Example" section on page 3-54, shows a setup session automatically invoked during the first-time startup of the router. During first-time startup, the system displays the system banner information, then starts the System Configuration Dialog.

The output shown in this example depends on the image version of the Cisco IOS software and the way your router is equipped. Your configuration dialog might be different.

The **setup** command script is a self-guiding interactive script that prompts you for responses and provides default or alternative values wherever possible.

setup Command Interactive Script Example

```
Cisco Internetwork Operating System Software
.
.
.
          --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: Yes

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 '[]'.

Basic setup only configures enough connectivity
for management of the system, extended setup will ask you
to configure each interface of the system.

Would you like to enter basic management setup? [yes/no]: Yes
Configuring global parameters:

  Enter host name [Router]: Router

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret [<Use current secret>]: alpha

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: bravo

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: charlie
  Configure SNMP Network Management? [no]:
```

```
Current interface summary
Interface   IP-Address      OK? Method Status                Protocol
Ethernet0   unassigned      YES unset  administratively down down
POS1/0      unassigned      YES unset  administratively down down
SDCC1/0     unassigned      YES unset  administratively down down
POS2/0      unassigned      YES unset  administratively down down
SDCC1/0     unassigned      YES unset  administratively down down
.
.
.
POS15/0     unassigned      YES unset  administratively down down
SDCC15/0    unassigned      YES unset  administratively down down

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0

Configuring interface Ethernet0:
Configure IP on this interface? Yes
  IP address for this interface: 172.99.99.2
  Subnet mask for this interface: 255.85.89.000
Class B network is 172.88.9.0, 8 subnet bits; mask is /24

The following configuration command script was created:

hostname Router
enable secret 5 $1$krIg$emfYm/1OwHVspDuS8Gy0K1
enable password wilma
line vty 0 4
password charlie
no snmp server
!
no ip routing
!
interface Ethernet0
no shutdown
ip address 172.88.99.2 255.888.255.0
!
interface POS1/0
shutdown
no ip address
!
interface SDCC1/0
shutdown
no ip address
.
.
.
```

```
interface POS15/0
shutdown
no ip address
!
interface SDCC15/0
shutdown
no ip address
!
end
[0] Go to the IOS command prompt without saving this script.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:

Building configuration ...

Use the enabled mode 'configure' command to modify this configuration.

router#
```

You can enter the **setup** command at any time at the privileged EXEC prompt to activate the **setup** command utility.

The only observable difference between the configuration script displayed when the **setup** command utility starts automatically on startup, and the script displayed when you enter the **setup** command, is that the existing script displays any previously entered system configuration defaults within square brackets ([ ]).

For example, during the configuration of a POS interface that has not been previously configured, when using the **setup** command utility at startup, you will see a display in the following form as you proceed through the script and respond to the prompts:

```
Configuring interface POS1/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
```

In this example, the script does not display default or current conditions in square brackets ([ ]), because the **setup** command utility ran automatically at startup and there was no prior configuration information.

When you enter the **setup** command at the privileged EXEC mode prompt, assuming that the POS interface *has been* configured previously and you are being queried by the system for changes, you will see a display in the following form:

```
Configuring interface POS1/0:
  Is this interface in use?[yes]:
```

```
Configure IP on this interface?[yes]:
```

The script displays the default or current conditions of the interface in square brackets, ([ ]) because you invoked the **setup** command utility using the **setup** command and there is previous configuration information. When a system prompt contains an existing default value in square brackets, press **Return** to accept the default value, or type an alternate value and press **Return**.

Configuring Global Parameters

When you first enter the **setup** utility or invoke the **setup** command, the system prompts you to configure global parameters for your router. The global parameters are used for controlling system-wide settings, including the following:

- Host name for the router
- Passwords for the enable secret, enable, and virtual terminal security parameters
- Protocols used by the router

Host Name

The name you assign the router must follow the rules for ARPANET host names. It must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The name must consist of 63 or fewer characters. For more information, refer to *Requests For Comments (RFC) 1035, Domain Names—Implementation and Specifications*.

Upper- and lowercase characters look the same to many Internet software applications; therefore, computer names should appear in all lowercase. For more information, refer to *RFC 1178, Choosing a Name for Your Computer.*

Passwords

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Many privileged EXEC commands are used to set system parameters. You should password-protect these commands to prevent their unauthorized use. For information on how to establish password protection or configure privilege levels, refer to the “Configuring Passwords and Privileges”

chapter in the *Security Configuration Guide*. This document is part of the Cisco IOS software configuration documentation set that corresponds to the Cisco IOS software release installed on your Cisco hardware.

The ***enable secret*** password functionality is available for Cisco 12006 and Cisco 12406 Routers. You must enter the correct password on the system console to gain access to privileged-level commands. When you are running from the ROM monitor, you can use the ***enable*** password, depending on your boot ROM level.

For maximum security, the **enable secret** and the **enable** passwords should be different. If you use the same password for both functions during the **setup** process, the system accepts it but warns that you should enter a different password.

An **enable secret** password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an **enable** password can contain any number of uppercase and lowercase alphanumeric characters. A number cannot be used as the first character. Spaces, however, are valid password characters. For example, `two words` is a valid password. Leading spaces are ignored, but trailing spaces are recognized. Make a note of all passwords you set, and store that information in a secure location for future reference.

Protocols

For complete information on protocol configuration for your router, refer to the appropriate software configuration publications, which are listed in the "If You Need More Information" section on page 3-82.

Configuring Network Interfaces

This section summarizes information about configuring the network interfaces for the RP and the installed line cards by using the **setup** command utility or **setup** command. Once configured, the RP and line cards can communicate with external networks.

To configure the interface parameters for the RP and installed line cards, you need the following information:

- Interface network addresses
- Subnet mask values

- Protocols to be configured

To obtain this information, consult your network administrator. For additional interface configuration information for the RP and each of the line cards installed in your router, refer to the configuration note that shipped with each card.

GRP Ethernet Interfaces

The RJ-45 and MII receptacles on the faceplate of the GRP are IEEE 802.3u-compliant interfaces. These IEEE interfaces provide connectivity to Ethernet networks. You can use either interface, but not both at the same time.

The following configuration dialog example shows the system being configured for an Ethernet interface that will use the IP network layer protocol. (The Ethernet interface does not support external routing functions.) The IP address and subnet mask value below are examples. The actual IP address and subnet mask value would be different.

```
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 255.888.0.0
  Configure CLNS on this interface?: yes
```

PRP Ethernet Interfaces

The IEEE 802.3 Ethernet interfaces on the PRP allow connections to external Ethernet networks and can transmit data rates of 10 Mbps and 100 Mbps. The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

Caution The Ethernet ports are primarily used as Telnet ports into the 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.

Line Card Interfaces

Because of the wide variety of line cards supported by Cisco 12006 and Cisco 12406 Routers, you should see the configuration note that shipped with a particular card for interface configuration information. This section provides several examples to show the general way the **setup** command utility handles line card interface configuration.

The following sample excerpt from a System Configuration Dialog session for a Quad OC-3cPOS line card shows settings for a typical configuration:

```
Configuring interface POS3/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
  Configure IP unnumbered on this interface?: no
    IP address for this interface: 2.1.1.1
    Number of bits in subnet field: 0
    Class A network is 2.0.0.0, 0 subnet bits; mask is 255.9.0
  Configure CLNS on this interface?: yes
```

Note By default, POS interfaces use the 32-bit cyclic redundancy check (CRC) and high-level data link control (HDLC) as the encapsulation protocol.

The following sample shows the same Quad OC-3c POS line card interface being configured for IP unnumbered:

```
Configuring interface POS3/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
  Configure IP unnumbered on this interface?: yes
    Assign to which interface: ethernet0
  Configure CLNS on this interface?: yes
```

In the following sample, an ATM line card is being configured to use IP:

```
Configuring interface parameters:

Configuring interface ATM1/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
    IP address for this interface: 1.1.1.2
    Number of bits in subnet field: 0
    Class A network is 1.0.0.0, 0 subnet bits; mask is 255.9.8.0
```

Note You might have to establish additional configuration parameters for the installed ATM line cards if you want to use all their capabilities. For example, additional steps are required to configure permanent virtual circuits (PVCs).

After you have manually configured the network interface parameters using the **setup** command utility or the **setup** command, your RP and line card interfaces are available for limited use. To modify the currently saved configuration information, enter the **setup** command at the privileged EXEC mode prompt (`Router#`) at any time to start another System Configuration Dialog session.

To perform more complex configuration tasks, enter the **configure terminal** command at the privileged EXEC mode prompt (`Router#`) to invoke the global configuration mode [`Router(config)#`].

Checking the Software Version

To determine the current version of the Cisco IOS software running on your router, enter the **show version** command at the user EXEC prompt. The Cisco IOS software version number is displayed, as well as other information, including the hardware installed in the system, the names and sources of system image files, and the contents of the software configuration register. The **show version** command also identifies the type of router.

The example in the show version Command section that follows below shows typical results from the **show version** command. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show version** command might be different.

show version Command

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
Image text-base: 0x60010950, data-base: 0x61C00000

ROM: System Bootstrap, Version 11.2(17)GS2, [name 180] EARLY
DEPLOYMENT RELEA)
```

```
BOOTFLASH: GS Software (GSR-BOOT-M), Version 11.2(18)GS4, EARLY
DEPLOYMENT RELE

Getty uptime is 22 hours, 15 minutes
System returned to ROM by reload
System image file is "tftp://xxx.xx.xx.xxx/directory/name/gsr-p-mz"

cisco 12406/GRP (R5000) processor (revision 0x05) with 262144K bytes
of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on

1 Route Processor Card
.
.
.
Configuration register is 0x0
.
.
.

router#
```

Verifying the Running Configuration Settings

To check the running configuration settings or any changes made to settings before you save them, enter the **show running-config** command at the privileged EXEC mode prompt. For a Quad OC-3c/STM-1c POS interface installed in slot 1, the **show running-config** command typically displays output in the form shown in the example below. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show running-config** command might be different.

show running Config Command Example

```
router# show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
no service udp-small-servers
```

```
no service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$W6K5$W/p5Bq6IPLGJ/hS9VVP1g.
enable password twink

interface POS1/0
 ip address 10.1.1.1 255.888.255.0
 crc 32
 clock source internal
!
interface POS1/1
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
!
interface POS1/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
!
interface POS1/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
```

Note For more information on a specific line card, see the line card installation and configuration note that came with your line cards.

You can access Cisco IOS software documentation and hardware installation and maintenance documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Saving the Running Configuration Settings to NVRAM

To save the running configuration changes to NVRAM, enter the **copy running-config startup-config** command at the privileged EXEC mode prompt as follows:

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

You can also use the following command to save the running configuration settings:

```
Router# write memory
```

Either command saves to NVRAM the configuration settings that you created while in the global configuration mode. If you do not save the running configuration settings to NVRAM, your configuration settings will be lost the next time you reload the system.

Reviewing the Running Configuration Settings

To display the running configuration settings stored in NVRAM, enter the **show startup-config** command at the privileged EXEC mode prompt on the system console. This command displays output in the form shown in the example that follows below. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show startup-config** command might be different.

show startup-config Command

```
Router# show startup-config
Using 5560 out of 520184 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$/5HX$OOvyhG2JYhNaCbPa45Wmn/
enable password wilma
```

```
ip cef distributed switch
ip host biff 10.3.3.254
!
interface Ethernet0
 ip address 10.3.1.1 255.888.0.0
 no ip mroute-cache
!
interface POS1/0
 ip address 10.1.1.1 255.8.9.0
 no keepalive
 crc 16
 no cdp enable
.
.
.
interface ATM3/0
 ip address 10.0.0.15 255.8.8.0 secondary
 ip address 10.1.1.2 255.8.8.0
 atm pvc 1 0 64 aal5snap
 atm pvc 2 0 72 aal5mux ip 155000 155000 1
 atm pvc 3 1 90 aal5snap 312000 312000 1
 atm pvc 4 0 108 aal5snap
 atm pvc 10 0 144 aal5mux ip 155000 155000 1
 atm pvc 11 1 91 aal5snap 310000 310000 1
 map-group atm1
!
no ip classless
ip route 10.5.8.254 255.888.255.255 Ethernet0
!
map-list atm1
 ip 10.1.1.1 atm-vc 1
 ip 10.1.1.3 atm-vc 2
 ip 10.1.1.4 atm-vc 4
 ip 10.0.0.1 atm-vc 3
 ip 10.0.0.5 atm-vc 10
 ip 10.0.0.6 atm-vc 11
no logging trap
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password bambam
 login
!
end
Router#
```

Using Flash Memory Cards in the RP

This section describes how to use Flash memory cards in the RP and includes information on the following topics:

Installing the Flash Memory Card in a RP

If there are dual RPs, the PCMCIA slots in the primary RP are designated slot 0 and slot 1. If there is a second RP, the PCMCIA slots in the second RP are designated sec-slot 0 and sec-slot 1. PCMCIA slot 0 is the bottom slot and slot 1 is the top slot. Both Flash memory card slots on each RP can be used at the same time. The following generic procedure can be used to install a Flash memory card in either slot position.

Step 1 Facing the RP faceplate, hold the Flash memory card with the connector end of the card toward the slot and the label facing up. (See Figure 3-10 on page 3-21.)

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.

Removing the Flash Memory Card from an RP

To remove a Flash memory card, follow these steps:

Step 1 Press the appropriate ejector button until the card is free of the connector at the back of the slot.

Step 2 Pull the card from the slot and place it in an antistatic sack to protect it from ESD damage.

The Flash memory card is keyed for proper insertion. The ejector button will not pop out unless the card is inserted correctly. Part of the card remains outside the slot even when the card is properly seated. Do not attempt to force the card deeper into the slot after the ejector button pops out.

Formatting a Flash Memory Card

The Flash memory card that shipped with your router contains the default Cisco IOS software image you need to boot your router.

Warning **This procedure erases all information on a Flash memory card. To prevent the loss of important data that might be stored on a Flash memory card, proceed carefully.**

If you want to save the data on a Flash memory card, copy the data to a server before you format the card. In some cases, you might need to insert a new Flash memory card and copy images or backup configuration files to the card. Before you can use a new Flash memory card, you must format it. Use only Type I or Type II Flash memory cards.

Caution The following formatting procedure presumes you have already booted your router.

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

Step 1 Insert the Flash memory card into slot 0 or slot 1 on the RP. (This example uses slot 0.)

Step 2 Enter the **format slot0:** command at the privileged EXEC mode prompt on the system console:

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

The console displays the "Formatting sector *n*" line in the sample output shown above. When the count reaches 1, the formatting process is complete and the new Flash memory card is ready for use.

For complete command descriptions and configuration information, refer to the *Configuration Fundamentals Command Reference* and the *Configuration Fundamentals Configuration Guide* in the Cisco IOS documentation set. For information on obtaining these publications, see the "If You Need More Information" section on page 3-82.

Specify a Boot Image

Use the procedure in this section to identify a sample Cisco IOS software image (*new.image* in this example) that is to be made bootable from a Flash memory card. The software configuration register must be set to 0x2102 during this procedure to boot the image from a Flash memory card; therefore, the **config-register** command must be included in the command sequence, as shown in this example:

```
Router# configure terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:new.image
Router(config)# config-register 0x2102
Ctrl-Z
Router# copy running-config startup-config
Router# reload
```

When you enter the **reload** command, the specified file (*new.image*) on the Flash memory card inserted in PCMCIA slot 0 is used to boot the system.

If one of the following software configuration register settings were specified in the preceding example, the system would behave accordingly:

- 0x2000—If the network boot fails, the system boots a default Cisco IOS software image from a Flash memory card.
- 0x0100—The system ignores the Break function.
- 0x0101—The system boots the default image (the first image found) from the onboard Flash memory SIMM on the RP. This setting also tells the system that it should *not* reset the Break disable function, nor should it check for a default filename for booting over the network.
- 0x0002—The system looks in the Flash memory SIMM on the RP for a default Cisco IOS software image.
- 0x0102—The system disables the Break function and checks for a default TFTP server filename. If the network boot operation fails, the system boots from a Flash memory card.

Flash Memory Console Commands

To determine whether the present working device you are accessing is the onboard Flash SIMM on the RP or a PCMCIA Flash memory card in a slot on the RP, enter the **pwd** command at the privileged EXEC mode prompt on the system console as follows:

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

In this example, the present working device you are accessing is on a PCMCIA Flash memory card inserted in slot 0 of the RP.

To change from one type of Flash memory device access to another, enter the **cd** *device-name* command, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**.

Sample uses of the **cd** command include:

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

```
slot1:/
Router# cd slot0:
Router# pwd
slot0:/
Router# cd bootflash:
Router# pwd
bootflash:/
Router#
```

To list the directory contents of the Flash memory media in use, enter the **dir** [*device-name*] command at the privileged EXEC mode prompt, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**.

A sample use of the **dir** command follows.

```
Router# dir
Directory of slot0:/

  1  -rw-     122015   Sep 30 2002 15:03:55 myfile1
  2  -rw-    2054979   Sep 30 2002 15:17:33 gsr-diag-mz.RELEASE28
  3  -rw-    6670560   Sep 30 2002 15:22:49 gsr-p-mz.p7
  4  -rw-       5560   Oct 08 2002 16:54:53 info

20578304 bytes total (9661756 bytes free)
Router#
```

To delete a file from a Flash memory media, use the **cd** command to select the Flash memory media and enter the **delete** *filename* command at the privileged EXEC mode prompt, where *filename* is any file within the selected Flash memory media.

An example of deleting the file *info* from the current Flash memory directory follows:

```
Router# delete slot0:info
Router# dir
Directory of slot0:/

  1  -rw-     122015   Sep 30 2002 15:03:55 myfile1
  2  -rw-    2054979   Sep 30 2002 15:17:33 gsr-diag-mz.RELEASE28
  3  -rw-    6670560   Sep 30 2002 15:22:49 gsr-p-mz.p7

20578304 bytes total (9661756 bytes free)
Router#
```

Files that are deleted from the current Flash memory directory are removed from the directory list, but are not erased; they still occupy space in Flash memory. This feature allows you to recover a deleted file later using the **undelete** command.

To remove deleted files from a Flash memory directory permanently, but leave undeleted files intact, enter the **squeeze** *device-name* command at the privileged EXEC mode prompt on the system console, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**. The **squeeze** command permanently removes deleted files and makes all other undeleted files contiguous, thus conserving storage space.

To prevent loss of data due to sudden power loss, the squeezed data is temporarily saved to another Flash memory area reserved specifically for system use.

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

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

In the preceding example command display, the characters in the final line (ebESZ) represent the Flash memory operations performed during the execution of the **squeeze** command. Table 3-14 describes these indicators.

Table 3-14 Squeeze Command Functions Example

e	The special Flash memory area has been erased. This erase operation must be accomplished before any write operation to the special Flash memory area can begin.
b	The data about to be written to the special Flash memory area has been temporarily copied.
E	The sector temporarily occupied by the data has been erased.
S	The data has been written to its permanent location in Flash memory.
Z	The log has been erased following the successful **squeeze** operation.

During the squeeze operation, the system maintains a log identifying which of the squeeze functions has been accomplished, so that the system can return to the proper place and continue the operation in the event of a power failure.

Booting from Flash Memory

To enable booting from Flash memory, set the boot field in the software configuration register (bits 3 through 0) to a value between 2 and 15. These values are used with the **boot system flash** *device:filename* configuration command, where *device* is **bootflash:**, **slot0:**, or **slot1:**, and *filename* is the name of the file from which you want to boot the system.

To enter global configuration mode while the system is running and specify a Flash filename from which to boot the system, enter the **configure terminal** command at the privileged EXEC mode prompt on the system console, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash device:filename
```

To disable the Break function and enable the **boot system flash** *device*:*filename* command, enter the **config-register** command at the global configuration mode prompt with the configuration register value, as shown below:

```
Router(config)# config-reg 0x0102
Ctrl-Z
Router#
```

Copying Files

Copy a new Cisco IOS software image to Flash memory when a new image becomes available or when you want to back up the image. This section explains how to copy any type of file to the Flash memory SIMM on the RP or to a PCMCIA Flash memory card inserted in either slot 0 or slot 1.

Caution You cannot copy a new Cisco IOS software image into the onboard Flash memory SIMM (also referred to as bootflash) while the system is running from onboard Flash memory.

To avoid losing valid Cisco IOS images, upgrade your Cisco IOS software images in Flash memory one at a time. Upgrade your PCMCIA-based Flash memory separately from the onboard Flash SIMM (bootflash) on the RP.

To copy a file to Flash memory, enter the following command at the privileged EXEC mode prompt on your system console:

Router# copy tftp:*filename* [**bootflash:**|**slot0:**|**slot1:**] *filename*

where:

tftp:*filename*	Specifies the source and name of the file to be copied.
[**bootflash: | slot0: | slot1:**] *filename*	Specifies the destination Flash medium and name for the new file. The destination Flash medium can be one of the following: **bootflash:**—The file will be copied to the onboard Flash memory SIMM on the RP. **slot0:**—The file will be copied to the PCMCIA Flash memory card in slot 0. **slot1:**—The file will be copied to the PCMCIA Flash memory card in slot 1.

Example of output generated by a **copy tftp:***filename* command:

```
Router# copy tftp:myfile1 slot0:myfile1
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]
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `ccccc` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Copying a Cisco IOS Software Image

You can copy a Cisco IOS software image into a Flash memory card at any time for later use, but you must first format the Flash memory card that you will use in the copy operation. If you have not already formatted the card, see the "Formatting a Flash Memory Card" section on page 3-67.

To ensure access to the network TFTP server, you must configure one network interface using the **setup** command facility. For instructions on using this facility, see the "Configuration Changes" section on page 3-53 or refer to the *Configuration Fundamentals Configuration Guide* for the IOS software release running on this router.

To copy a bootable image into the Flash memory card, follow these steps:

Step 1 Boot the router and allow it to initialize.

Step 2 Enter the **enable** command at the user EXEC mode prompt to enter privileged EXEC mode:

```
Router> enable
Password: <password>
Router#
```

Step 3 Copy the file named *new.image* in this example to the Flash memory card inserted in PCMCIA slot 0 by using the following command:

```
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]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `CCCCC` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Step 4 Reboot the system.

Copying Cisco IOS Software Updates

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

This section explains how to use a newly released Cisco IOS software image on a Flash memory card in a system that has an older Cisco IOS image residing on a Flash memory card inserted in PCMCIA slot 0 and a default Cisco IOS software boot image stored in the onboard Flash memory SIMM on the RP.

In this procedure, you will copy an updated Cisco IOS software image from a new Flash memory card onto a Flash memory card containing an old Cisco IOS software image. In this example, the following filenames apply:

- *image.new*—The new image on the new Flash memory.
- *image.old*—The old image on the old Flash memory card inserted in PCMCIA slot 0.
- *image.boot*—The bootable Cisco IOS software image stored in the onboard Flash memory SIMM. (This image is used by default to boot the system if no other bootable image is available.)

This procedure assumes that there is sufficient space on the old Flash memory card inserted in slot 0 for both the new Cisco IOS software image and the old image. If there is not enough space for both images on the old Flash memory card, use the **delete** command to delete files from the old Flash memory card, but *do not* delete the *image.old* file. After deleting files, use the **squeeze** command to remove the deleted files from the old Flash memory card permanently. For information on the **squeeze** command, see the "Flash Memory Console Commands" section on page 3-69.

If the two files still will not fit on the Flash memory card in slot 0 after you delete files and use the **squeeze** command, remove this card, place it in an antistatic bag for ESD protection, and store it in a safe place. Insert the Flash memory card containing *image.new* in slot 0. Proceed to Step 5 in the following procedure and enter the command **boot system flash slot0:image.new** to designate the file *image.new* as the new default Cisco IOS software boot image.

To copy a bootable Cisco IOS software image between Flash memory cards, follow these steps:

Step 1 Boot the router. For this example, the file named *image.boot* is the default boot image.

Step 2 Enter the **enable** command to enter privileged EXEC mode as follows:

```
Router> enable
Password: <password>
Router#
```

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

Step 4 Enter the following command to copy the file *image.new* in slot 1 to the Flash memory card in PCMCIA slot 0.

Note Take this step only if sufficient space is available on the Flash memory card in slot 0 to hold both the new image and the old image already resident on the Flash memory card.

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

Entering this command in the following form will achieve the same result:

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

Step 5 Enter the following commands to designate the file named *image.new* in the Flash memory card in slot 0 as the new default system image for boot purposes:

```
Router# configure terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:image.new
Ctrl-Z
Router# copy running-config startup-config
Router# reload
```

When the system reloads, the file *image.new* is booted from the Flash memory card in slot 0.

Copying Files Between RP Memory and a Flash Memory Card

If you do not have access to a TFTP server where you can temporarily store a configuration file, you will need to copy a configuration file to a Flash memory card inserted in PCMCIA slot 0 or slot 1. You can then copy the configuration file back to NVRAM at any time. You can copy either your startup configuration file (from NVRAM) or your running configuration file (from DRAM).

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

- Copying Configuration Files from RP NVRAM to a Flash Memory Card, page 3-77
- Copying a Configuration File from RP DRAM to a Flash Memory Card, page 3-80
- Copying a Configuration File from a Flash Memory Card to RP NVRAM, page 3-81

Note You cannot copy files directly into DRAM.

Copying Configuration Files from RP NVRAM to a Flash Memory Card

Use the command **copy startup-config** [**slot0: | slot1:**] *filename* for the copy procedure, where **startup-config** is the source of the file (NVRAM), [**slot0: | slot1:**] is one of the Flash memory card slots, and *filename* is the name of the configuration file to be copied. Note that the environmental variable CONFIG_FILE must point to NVRAM (the system default).

To copy a configuration file named *myfile2* from the NVRAM on the RP to a Flash memory card in slot 0, follow these steps:

Step 1 Enter the **show bootvar** command at the privileged EXEC mode prompt to display the current setting for the CONFIG_FILE environmental variable, as follows:

```
Router# show bootvar
.
.
.
CONFIG_FILE variable =
Current CONFIG_FILE variable =
.
.
.
Router#
```

The absence of any notation following the CONFIG_FILE variable statement in this sample display indicates that the environmental variable points to NVRAM (the system default).

Step 2 To begin the copy operation, enter a **copy** command in the following form at the privileged EXEC mode prompt:

copy startup-config [**slot0:** | **slot1:**]*filename*

where

startup-config	Specifies the source of the file to be copied (NVRAM).
[**slot0:** | **slot1:**]*filename*	Specifies the destination of the file (the Flash memory card slot number) and the name of the new file.

An example of the **copy startup-config slot0:***filename* command follows:

```
Router# copy startup-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):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `CCCCC` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

You can also copy the running configuration (located in DRAM) to a Flash memory card, as shown in the "Copying a Configuration File from RP DRAM to a Flash Memory Card" section on page 3-80."

Step 3 To further verify that the configuration file was copied correctly to the Flash memory card in slot 0, enter the **dir** command:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  May 10 2002 19:24:12 gsr-p-mz.112-8
3   1215     May 10 2002 20:30:52 myfile1
4   6176844  May 10 2002 23:04:10 gsr-p-mz.112-8.1
5   1186     May 10 2002 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

Copying a Configuration File from RP DRAM to a Flash Memory Card

To copy the running configuration file from DRAM to a Flash memory card, follow these steps:

Step 1 Enter the command for copying a running configuration file from DRAM to a Flash memory card. The command takes the following form:

copy running-config [**slot0:**|**slot1:**]*filename*

where:

running-config	Specifies the DRAM source of the file to be copied.
[**slot0:** | **slot1:**]*filename*	Specifies the destination of the configuration file to be copied (the Flash memory card inserted in either slot 0 or slot 1) and the name of the new file.

An example of the **copy running-config slot0:***filename* command 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):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `CCCCC` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Step 2 To further verify that the file was copied correctly, enter the **dir** command at the privileged EXEC mode prompt:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  May 10 2002 19:24:12 gsr-p-mz.112-8
3   1215     May 10 2002 20:30:52 myfile1
4   6176844  May 10 2002 23:04:10 gsr-p-mz.112-8.1
```

```
5   1186     May 10 2002 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

Copying a Configuration File from a Flash Memory Card to RP NVRAM

To copy a configuration file from a Flash memory card in PCMCIA slot 0 or slot 1 to NVRAM, follow these steps:

Step 1 Enter the command for copying a configuration file from a Flash memory card to NVRAM. This command takes the following form:

copy [**slot0:**|**slot1:**]*filename* **startup-config**

where:

[**slot0:** | **slot1:**]*filename*	Specifies the source of the configuration file to be copied (the Flash memory card in either PCMCIA slot 0 or slot 1) and the name of the new file.
startup-config	Specifies the destination (NVRAM) of the file to be copied.

To start the copy operation, enter the following command at the privileged EXEC mode prompt:

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

Step 2 Use the following command to ensure that the startup configuration file, now stored in NVRAM, becomes the default running configuration file:

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

Locked Blocks in Flash Memory Cards

A locked block in Flash memory cards occurs when power is lost or a Flash memory card is removed from its PCMCIA slot on the RP during a write or erase operation.

When a block of Flash memory is locked, it cannot be written to or erased. Any attempt to do so will consistently fail at the block location. The only way to recover from locked blocks in a Flash memory card is to reformat the Flash memory card using the **format** command.

Caution Formatting a Flash memory card erases all existing data on the card.

If You Need More Information

If your router is not fully functional, you may need to perform additional configuration tasks. For more detailed information about configuring the router and its interfaces, see the publications listed in the following section.

The Cisco IOS software running your router contains extensive features and functionality. For information on Cisco IOS software and general installation and maintenance information for your router, use the following resources.

Cisco IOS Software Configuration Information and Support

The modular configuration and modular command reference publications in the Cisco IOS software configuration documentation set correspond to the Cisco IOS software release installed on your Cisco hardware. You can also see the Cisco IOS software release notes for the version of Cisco IOS software you are using on your router.

You can access Cisco IOS software documentation and hardware installation and maintenance documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** on the toolbar, and then select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

We appreciate your comments.

For information on regulatory compliance and safety, refer to *Regulatory Compliance and Safety Information for the Cisco 12000 Series Routers*, Document Number 78-4347-xx.

For additional line card information, refer to the installation and configuration note that accompanied your line card.

For additional GRP information, refer to the configuration note *Gigabit Route Processor (GRP) Installation and Configuration* (Document Number 78-4339-xx) that accompanied your GRP.

For additional PRP information, refer to the configuration note *Performance Route Processor (PRP) Installation and Configuration* (Document Number 78-13302-xx) that accompanied your PRP.