



CHAPTER 1

Using Cisco IOS Software

This chapter provides information to prepare you to configure a SPA interface processor (SIP) or shared port adapter (SPA) using the Cisco IOS software. It includes the following sections:

- [Accessing the CLI Using a Router Console, page 1-1](#)
- [Using Keyboard Shortcuts, page 1-6](#)
- [Using the History Buffer to Recall Commands, page 1-7](#)
- [Understanding Command Modes, page 1-7](#)
- [Getting Help, page 1-9](#)
- [Using the no and default Forms of Commands, page 1-9](#)
- [Saving Configuration Changes, page 1-9](#)
- [Finding Support Information for Platforms and Cisco Software Images, page 1-10](#)

Accessing the CLI Using a Router Console

The following sections describe how to access the command-line interface (CLI) using a directly-connected console or by using Telnet to obtain a remote console:

- [Accessing the CLI Using a Directly-Connected Console, page 1-1](#)
- [Accessing the CLI from a Remote Console Using Telnet, page 1-5](#)

For more detailed information about configuring and accessing a router through various services, refer to the *Cisco IOS Terminal Services Configuration Guide* and *Cisco IOS Terminal Services Command Reference* publications.

For more information about making the console cable connections, refer to the *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide*.

Accessing the CLI Using a Directly-Connected Console

This section describes how to connect to the console port on the router and use the console interface to access the CLI.

The PRE module on the Cisco uBR10012 router has two asynchronous serial (EIA/TIA-232) RJ-45 ports that provide connections for a console (an ASCII terminal or PC running terminal emulation software) and a modem for remote access.

Recommended Tools and Supplies

The Cisco uBR10012 router arrives with a console and auxiliary cable kit, which contains the cable and adapters you need for the most common connections to these devices.

You need the following tools and supplies to connect to the console port:

- RJ-45 to RJ-45 crossover cable
- RJ-45-to-DB-9 adapter
- ESD-preventive wrist strap

**Note**

A crossover cable reverses pin connections from one end to the other. In other words, it connects pin 1 (at one end) to pin 8 (at the other end), pin 2 to pin 7, pin 3 to pin 6, and so on. You can identify a crossover cable by comparing the two modular ends of the cable. Hold the cable ends in your hand, side-by-side, with the tabs at the back. Ensure that the wire connected to the outside (left) pin of the left plug (pin 1) is the same color as the wire connected to the outside (right) pin of the right plug (pin 8).

For more information about RJ-45 crossover cables and the console port connectors, see the *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide*.

Connecting to the Console Port

The console port provides local administrative access to the router and its command-line interface (CLI).

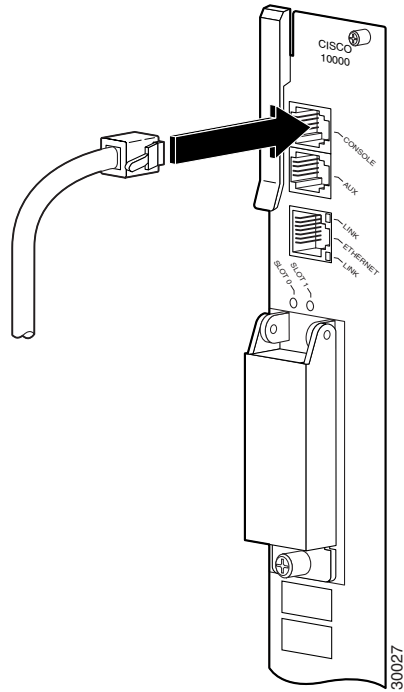
**Note**

Each PRE module must have a console port connection (typically to a terminal server) when running a redundant configuration in the chassis.

Step 1

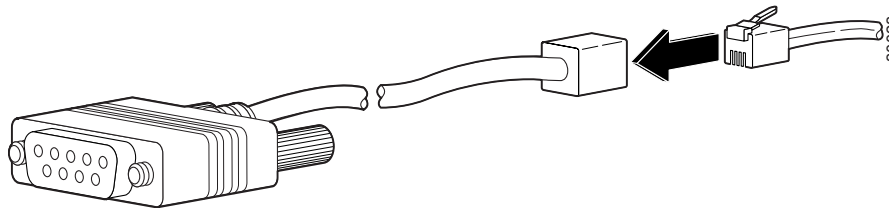
Connect one end of the RJ-45 crossover cable to the serial RJ-45 port (labeled CONSOLE) on the PRE module ([Figure 1-1](#)).

Figure 1-1 Console Port Connection on the PRE Module



- Step 2** Run the other end of the crossover cable through the square hole at the left front side of the chassis, and connect it to the RJ-45-to-DB-9 adapter (see [Figure 1-2](#)).

Figure 1-2 Connecting an RJ-45-to-DB-9 Console Cable Adapter



- Step 3** Connect the adapter to the appropriate serial port on the PC or terminal to complete the console port cable connection.
- Step 4** Power on the PC or terminal.

Step 5 Configure the PC terminal emulation software or the terminal for the following default settings:

- 9600 baud
- 8 data bits
- No parity generation or checking
- 1 stop bit
- No flow control



Note

These are the default serial communication parameters on the router. For information about how to change the default settings to meet the requirements of your terminal or host, refer to the *Cisco IOS Terminal Services Configuration Guide*.

Using the Console Interface

To access the CLI using the console interface, complete the following steps:

Step 1 After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the initial prompt should appear.

Step 2 Press **Return** to enter user EXEC configuration mode. The following prompt appears:

```
Router>
```

Step 3 From user EXEC configuration mode, enter the **enable** command as shown in the following example:

```
Router> enable
```

Step 4 At the password prompt, enter your system's password. The following example shows entry of the password called "enablepass":

```
Password: enablepass
```

Step 5 When your enable password is accepted, the privileged EXEC configuration mode prompt appears:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC configuration mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the console session, enter the **quit** command as shown in the following example:

```
Router# quit
```

Accessing the CLI from a Remote Console Using Telnet

This section describes how to connect to the console interface on a router using Telnet to access the CLI.

Preparing to Connect to the Router Console Using Telnet

Before you can access the router remotely using Telnet from a TCP/IP network, you need to configure the router to support virtual terminal lines (vty) using the **line vty** global configuration command. You also should configure the vty lines to require login and specify a password.

**Note**

To prevent disabling login on the line, be careful that you specify a password with the **password** command when you configure the **login** line configuration command. If you are using authentication, authorization, and accounting (AAA), you should configure the **login authentication** line configuration command. To prevent disabling login on the line for AAA authentication when you configure a list with the **login authentication** command, you must also configure that list using the **aaa authentication login** global configuration command. For more information about AAA services, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

In addition, before you can make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, refer to the *Cisco IOS Terminal Services Configuration Guide*.

Using Telnet to Access a Console Interface

To access a console interface using Telnet, complete the following steps:

Step 1 From your terminal or PC, enter one of the following commands:

- **connect** *host* [*port*] [*keyword*]
- **telnet** *host* [*port*] [*keyword*]

In this syntax, *host* is the router hostname or an IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information, refer to the *Cisco IOS Terminal Services Command Reference*.

**Note**

If you are using an access server, then you will need to specify a valid port number such as **telnet 172.20.52.40 2004**, in addition to the host name or IP address.

The following example shows the **telnet** command to connect to the router named “router”:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

- Step 2** At the password prompt, enter your login password. The following example shows entry of the password called “mypass”:

```
User Access Verification

Password: mypass
```



Note If no password has been configured, press **Return**.

- Step 3** From user EXEC configuration mode, enter the **enable** command as shown in the following example:

```
Router> enable
```

- Step 4** At the password prompt, enter your system’s password. The following example shows entry of the password called “enablepass”:

```
Password: enablepass
```

- Step 5** When the enable password is accepted, the privileged EXEC configuration mode prompt appears:

```
Router#
```

- Step 6** You now have access to the CLI in privileged EXEC configuration mode and you can enter the necessary commands to complete your desired tasks.

- Step 7** To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

```
Router# logout
```

Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

[Table 1-1](#) lists the keyboard shortcuts for entering and editing commands.

Table 1-1 Keyboard Shortcuts

Keystrokes	Purpose
Ctrl-B or the Left Arrow key ¹	Move the cursor back one character
Ctrl-F or the Right Arrow key ¹	Move the cursor forward one character
Ctrl-A	Move the cursor to the beginning of the command line
Ctrl-E	Move the cursor to the end of the command line

Table 1-1 Keyboard Shortcuts (continued)

Keystrokes	Purpose
Esc B	Move the cursor back one word
Esc F	Move the cursor forward one word

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

Table 1-2 lists the history substitution commands.

Table 1-2 History Substitution Commands

Command	Purpose
Ctrl-P or the Up Arrow key ¹	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the Down Arrow key ¹	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.
Router# show history	While in EXEC mode, list the last several commands you have just entered.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1-3 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1-3 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the logout command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal privileged EXEC command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the exit or end command.
Interface configuration	From global configuration mode, specify an interface using an interface command.	Router(config-if)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
Controller configuration	From global configuration mode, specify a controller using the controller command.	Router(config-controller)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
Cable fiber-node configuration	From global configuration mode, specify a fiber node using the cable fiber-node command.	Router(config-fiber-node)#	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
ROM monitor	From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the continue command.

For more information on command modes, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.

Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Table 1-4 Help Commands and Purpose

Command	Purpose
<code>help</code>	Provides a brief description of the help system in any command mode.
<code>abbreviated-command-entry?</code>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<code>abbreviated-command-entry<Tab></code>	Completes a partial command name.
<code>?</code>	Lists all commands available for a particular command mode.
<code>command ?</code>	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the command **default command-name**, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function of the **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

The command writes the configuration data to the router's nonvolatile random-access memory (NVRAM). It might take a few seconds to save the configuration.

Finding Support Information for Platforms and Cisco Software Images

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS software image, you can use Cisco Feature Navigator or the software release notes.

Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

The channel-bonding functionality of the Cisco Cable Wideband Solution, Release 1.0, has the feature name “DOCSIS 3.0 Downstream.” The Cisco uBR10012 router, Cisco Wideband SIP, and Cisco Wideband SPA are key components of the DOCSIS 3.0 Downstream Solution, Release 2.0.

Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- New feature information
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.