



Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) that you can use to configure the wireless device. It contains these sections:

- [Cisco IOS Command Modes, page 4-2](#)
- [Getting Help, page 4-3](#)
- [Using no and default Forms of Commands, page 4-3](#)
- [Understanding CLI Messages, page 4-4](#)
- [Accessing the CLI, page 4-4](#)

Cisco IOS Command Modes

The Cisco IOS user interface is divided into modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the wireless device, you begin in user mode, often called *user EXEC mode*. A subset of the Cisco IOS commands are available in user EXEC mode. For example, most of the user 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 user EXEC commands are not saved when the wireless device reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the wireless device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 4-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *ap*.

Table 4-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with the wireless device.	ap>	Enter logout or quit .	Use this mode to: <ul style="list-style-type: none"> Change terminal settings Perform basic tests Display system information
Privileged EXEC	While in user EXEC mode, enter the enable command.	ap#	Enter disable to exit.	Use this mode to verify commands. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	ap(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire wireless device.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	ap(config-if)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet and radio interfaces. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in [Table 4-2](#).

Table 4-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Obtains a list of commands that begin with a particular character string. For example: ap# di? dir disable disconnect
<i>abbreviated-command-entry<Tab></i>	Completes a partial command name. For example: ap# sh conf<tab> ap# show configuration
?	Lists all commands available for a particular command mode. For example: ap> ?
<i>command ?</i>	Lists the associated keywords for a command. For example: ap> show ?
<i>command keyword ?</i>	Lists the associated arguments for a keyword. For example: ap(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet

Using no and default Forms of Commands

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a *default* form. The default form of a command returns the command setting to its default. Most commands are disabled by default, so the default form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the default command enables the command and sets variables to their default values.

Understanding CLI Messages

Table 4-3 lists some error messages that you might encounter while using the CLI to configure the wireless device.

Table 4-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the wireless device to recognize the command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Incomplete command.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Accessing the CLI

You can open the CLI using Telnet or Secure Shell (SSH).

Opening the CLI with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.



Note In Windows 2000, the Telnet window does not contain drop-down menus. To start the Telnet session in Windows 2000, type **open** followed by the wireless device IP address.

Step 3 In the Host Name field, type the wireless device IP address and click **Connect**.

- Step 4** At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.
-

Opening the CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices set up to use it. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: <http://www.ssh.com/>

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. See the “[Configuring the Access Point for Secure Shell](#)” section on page 5-25 for detailed instructions on setting up the wireless device for SSH access.

