The Cisco IOS CLI

This chapter covers

- The interfaces used to configure network devices
- How to connect to the CLI of a Cisco device via the console port
- Navigating between modes of the Cisco IOS command hierarchy
- Viewing and saving a device's configuration files
- Password-protecting a Cisco IOS device

This chapter is a break from the networking theory of the previous chapter; it's time to get hands-on with Cisco routers and switches. Understanding the theory of networking is absolutely essential, but networking is also a skill that must be practiced, and that means configuring network devices.

In the CCNA exam topics list, you will find a few different verbs, such as *explain X*, *describe Y*, and *identify Z*, indicating that Cisco expects you to have a theoretical understanding of the listed concepts and how they work. However, there are also many exam topics that state *configure X* or *configure and verify Y*. For these topics, in addition to having a theoretical understanding of their concepts, you must be able to configure them on Cisco network devices and verify their operations.

As an introduction to making configuration changes to a Cisco device and saving those changes, in this chapter, we will touch on exam topic 5.3: Configure and verify device access control using local passwords. However, this chapter is not specifically aimed at one of the CCNA exam topics but rather lays a necessary foundation for all of the exam topics that require you to configure and verify various protocols.

5.1 Shells: GUI and CLI

A shell is a computer program that allows a user to interact with the computer. It's the interface between the computer and the user, and it's called a shell because it's the outer layer of the operating system. To configure a Cisco router or switch, you use a shell to give commands to the device. In this section we will look at the two types of shells we will use in this book.

5.1.1 GUI and CLI

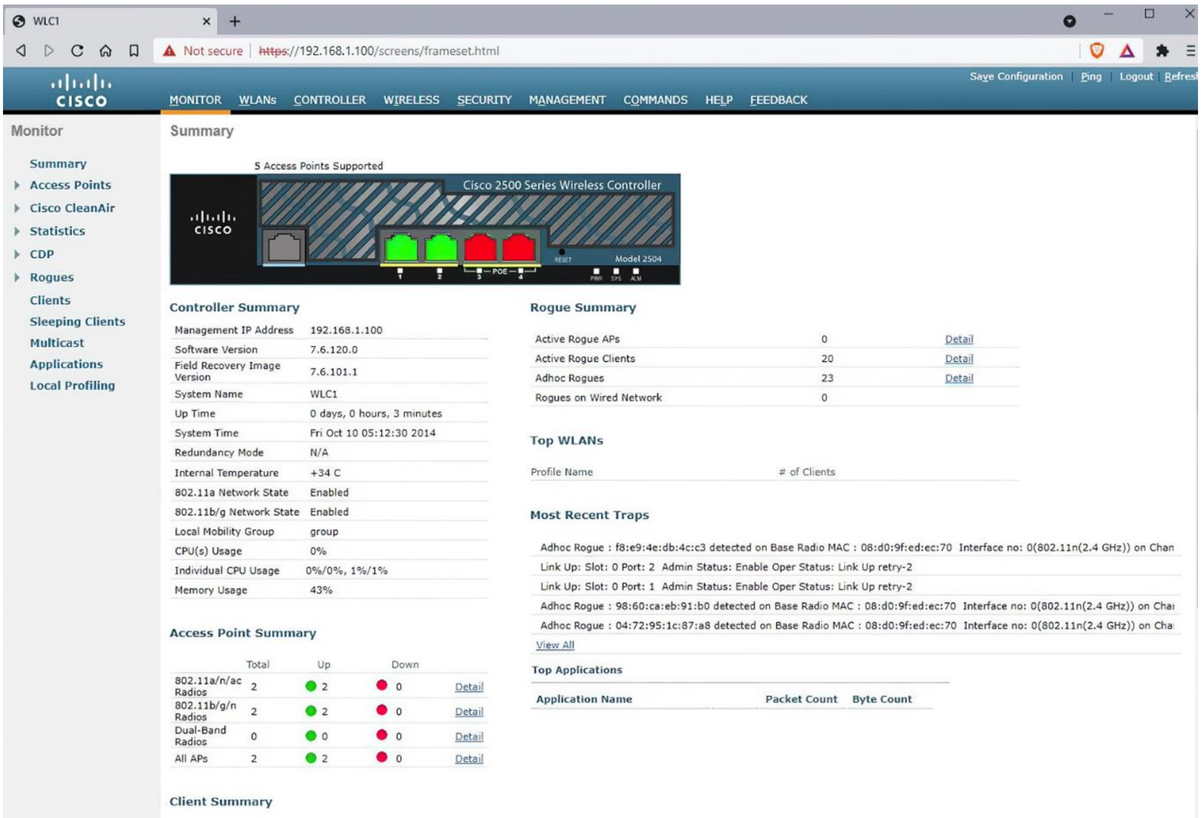
There are two main kinds of shells: *graphical user interface* (GUI, pronounced "G-U-I" or "gooey") and *command-line interface* (CLI). Let's examine these two types.

Graphical user interfaces

A GUI allows a user to manipulate the computer via a graphical interface. Regardless of your degree of experience or inexperience with computers, I'm certain you've used a GUI before. If you have a Windows PC, the GUI is what you're interacting with when you open, close, and move windows, or when you open the *Start menu* to search for a program, etc. This is the *Windows shell*. If you have a smartphone, you use a GUI to interact with the phone and its apps

Although most of the CCNA exam does not focus on GUIs, there is one GUI you are expected to be familiar with for the exam: the Cisco *wireless LAN controller* (WLC) GUI. We will cover wireless LANs and how to configure a WLC via the GUI in part 11 of this book. Figure 5.1 shows a screenshot of the GUI of a Cisco WLC.

Figure 5.1 The GUI of a Cisco wireless LAN controller, accessed via a web browser



Controller Summary

Management IP Address	192.168.1.100
Software Version	7.6.120.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 0 hours, 3 minutes
System Time	Fri Oct 10 05:12:30 2014
Redundancy Mode	N/A
Internal Temperature	+34 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	group
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 1%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	2	● 2	● 0	Detail
Dual-Band Radios	0	● 0	● 0	Detail
All APs	2	● 2	● 0	Detail

Client Summary

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	20	Detail
Adhoc Rogues	23	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

Most Recent Traps

```
Adhoc Rogue : f8:e9:4e:db:4c:c3 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Chan
Link Up: Slot: 0 Port: 2  Admin Status: Enable Oper Status: Link Up retry-2
Link Up: Slot: 0 Port: 1  Admin Status: Enable Oper Status: Link Up retry-2
Adhoc Rogue : 98:60:ca:eb:91:b0 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Chai
Adhoc Rogue : 04:72:95:1c:87:a8 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Cha
```

View All

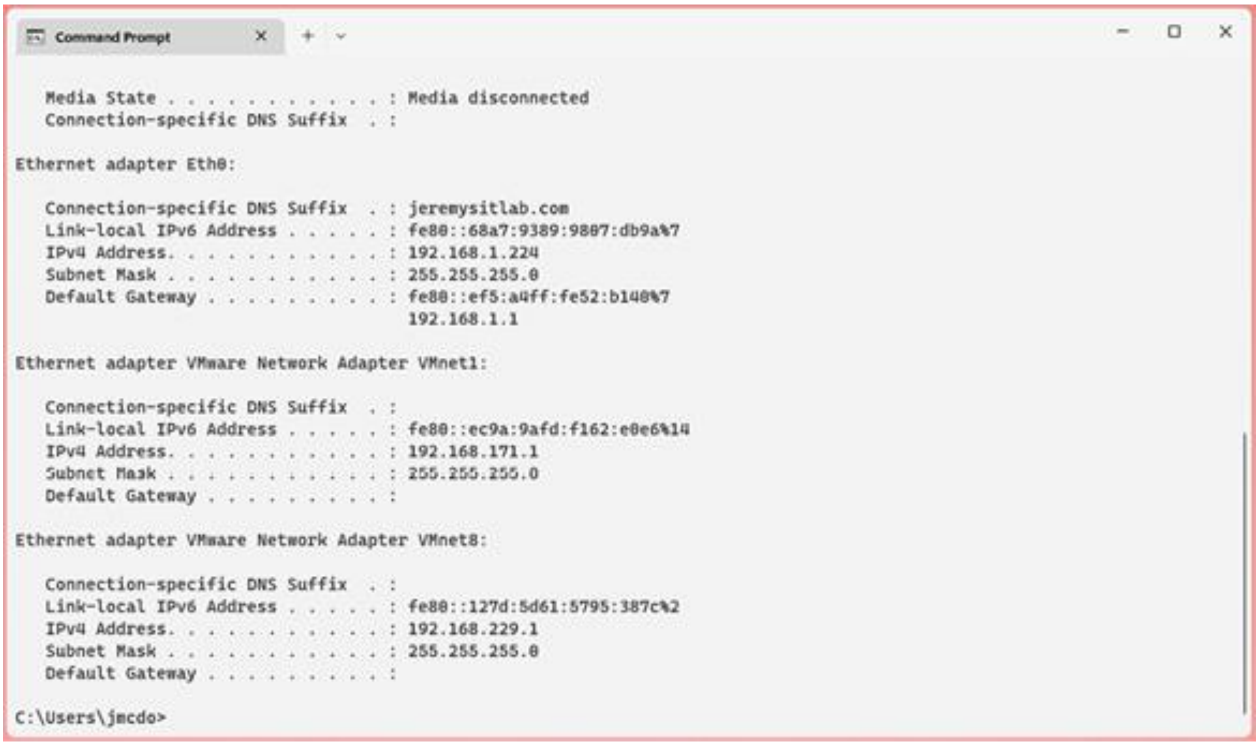
Top Applications

Application Name	Packet Count	Byte Count

Command-line interfaces

A CLI is a text-based interface that allows you to control and interact with a device by entering *commands*, which are lines of text. A famous CLI you might have seen before is the Windows *Command Prompt*, as pictured in figure 5.2. Although the vast majority of users use the GUI exclusively (or almost exclusively), the Command Prompt CLI provides an alternative way to interact with the PC.

Figure 5.2 The Command Prompt CLI of a Windows PC, accessed from within the Windows shell GUI



```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Eth0:

   Connection-specific DNS Suffix  . : jeremysitlab.com
   Link-local IPv6 Address . . . . . : fe80::68a7:9389:9807:db9a%7
   IPv4 Address. . . . . . . . . . . : 192.168.1.224
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::ef5:a4ff:fe52:b140%7
                                       192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ec9a:9afd:f162:e0e6%14
   IPv4 Address. . . . . . . . . . . : 192.168.171.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::127d:5d61:5795:387c%2
   IPv4 Address. . . . . . . . . . . : 192.168.229.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\jmcdo>
```

For the CCNA exam you must be familiar with the CLI of Cisco routers and switches running Cisco IOS. For those with no prior experience with a CLI (such as myself when I started my CCNA studies in 2018), this can seem intimidating. However, by the end of this chapter I hope you will see that navigating around the Cisco IOS CLI isn’t so complicated

Exam Tip

Throughout this book I will introduce various CLI commands to configure the protocols you must know for the CCNA exam. Hands-on practice with these commands, for example using Cisco Packet Tracer, is an essential part of preparing for the CCNA exam

5.1.2 Accessing the CLI of a Cisco device

In order to configure Cisco devices, you first have to connect your computer to the device to access the CLI. There are two main methods to do so:

- Connect a PC/laptop to the *console port* of the device with a *console cable*.
- Connect to the device over the network using a protocol like *Telnet* or *Secure Shell* (SSH).

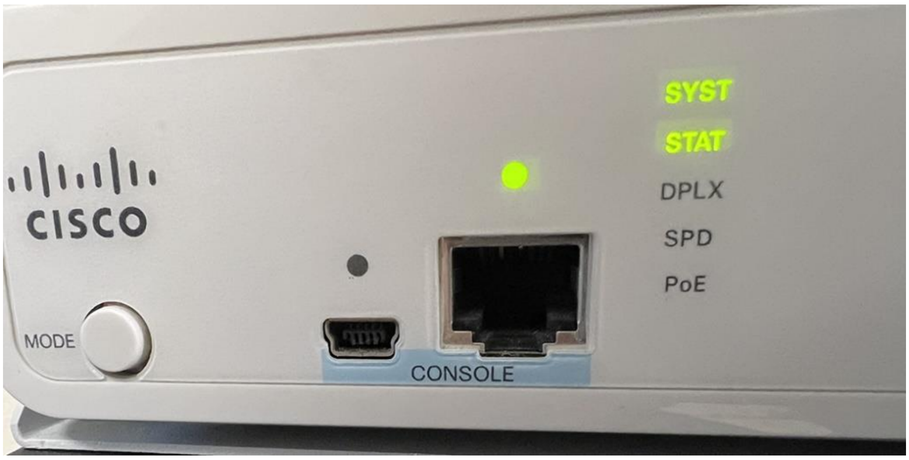
We will cover Telnet and SSH in chapter 35. Until then, we will focus on connections via the console port of the device. The console port is a physical port that allows you to connect a computer directly to the device (as opposed to connecting via the network infrastructure). In order to do so, you must be physically near the device; a console cable is typically only a few feet in length

Note

Console ports cannot be used to communicate over the network. They are dedicated for configuring the device via the CLI.

Figure 5.3 shows two console ports on a Cisco switch: USB Mini-B and RJ45. The exact types of console ports available depends on the model of the device, but USB Mini-B and RJ45 are common across many different Cisco router and switch models. You can connect to either port, but not both; only one console connection is supported at a time.

Figure 5.3 Two console ports on a Cisco switch: USB Mini-B (left) and RJ45 (right)



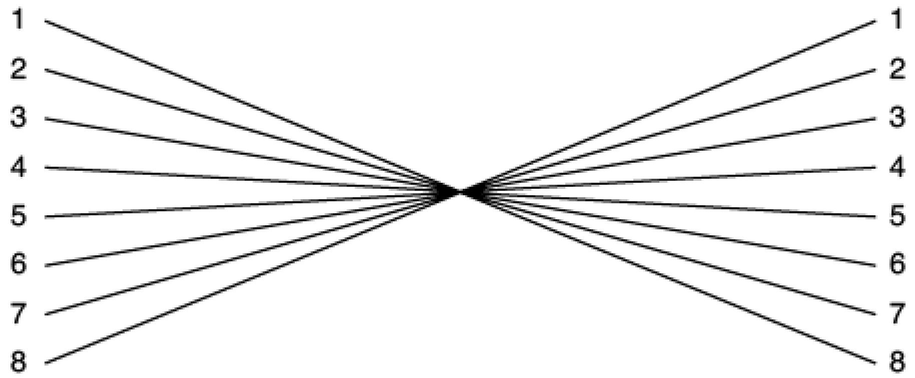
Console cables come in a variety of types with a variety of different connectors. The type used depends on the ports available on the device itself, the PC connecting to it. Perhaps the simplest option is to use a standard USB cable to connect your PC to the device's USB console port (make sure the cable has the correct USB connector types for your PC and the device you want to connect to).

To connect to the RJ45 console port you must use a *rollover cable*. This is a different pattern than the *straight-through* and *crossover* cables we covered in chapter 3; rollover cables are wired like this

- Pin 1 to pin 8
- Pin 2 to pin 7
- Pin 3 to pin 6
- Pin 4 to pin 5
- Pin 5 to pin 4
- Pin 6 to pin 3
- Pin 7 to pin 2
- Pin 8 to pin 1

The wiring of a rollover cable is illustrated in figure 5.4.

Figure 5.4 The wiring of a rollover cable, used to connect a PC to the RJ45 console port of a network device. Pin 1 on one end connects to pin 8 on the other end, pin 2 to pin 7, pin 3 to pin 6, pin 4 to pin 5, pin 5 to pin 4, pin 6 to pin 3, pin 7 to pin 2, pin 8 to pin 1.



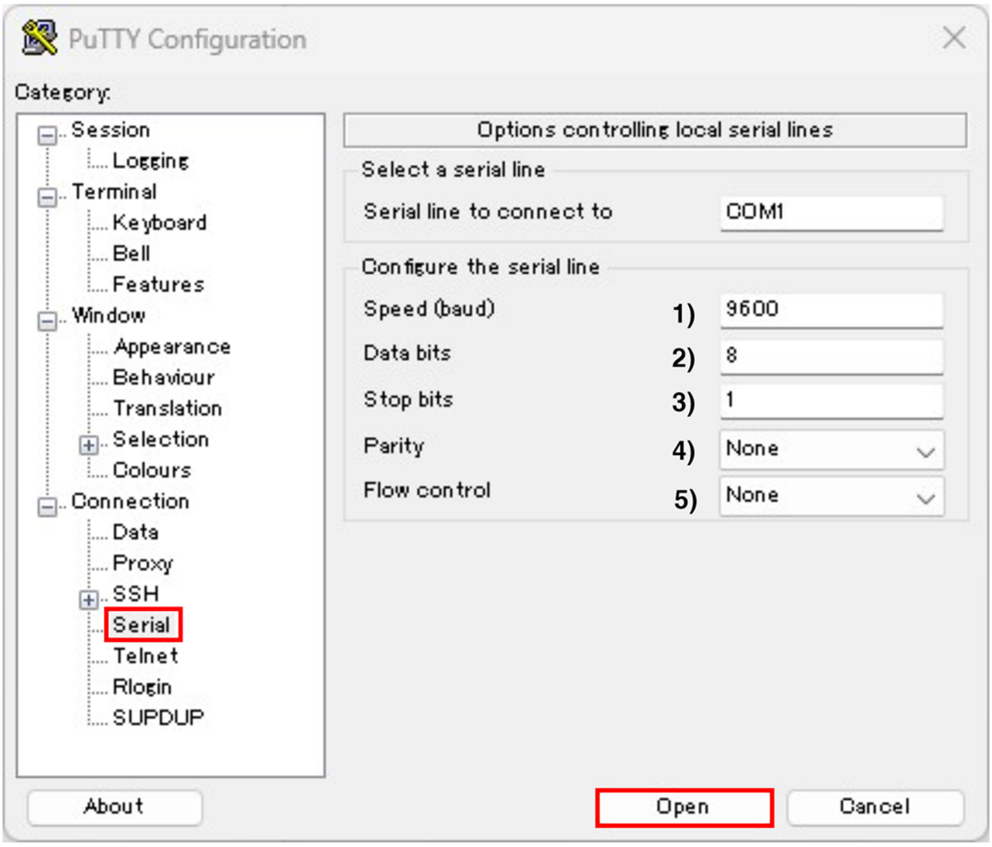
After physically connecting your PC to the device's console port, you then need to use a type of application called a *terminal emulator* to access the CLI. A terminal emulator is a software application that replicates the functions of a *computer terminal* – an old hardware device consisting of a monitor and keyboard that was used to input data into (and receive and display data from) a computer. A popular (and free) terminal emulator on Windows is PuTTy (www.putty.org), but there are many options available for a variety of platforms.

When using a terminal emulator to connect from a PC to a device's console port, there are a few settings you will have to configure. Those are:

- Speed: the rate at which data is sent
- Data bits: the number of bits of information used for each character of text sent to the device
- Stop bits: sent after every character to allow the receiving device to detect the end of the character
- Parity: an extra bit sent with each character to be used for error detection
- Flow control: provides support for circumstances where a device sends data faster than the receiver can handle

The appropriate value for each setting depends on the device you are configuring; to learn the appropriate settings for a particular device, you will have to check manufacturer's documentation for that device. Figure 5.4 shows how to initiate a console connection to a Cisco device in PuTTy: from the *Serial* tab, use the following configurations, and then click *Open* to access the CLI of the connected device:

Figure 5.5 How to use PuTTY to access a Cisco device's CLI via the console port. From the Serial tab, configure the following settings, and then click Open: (1) Speed (baud): 9600 bits per second, (2) Data bits: 8, (3) Stop bits: 1, (4) Parity: None, (5) Flow control: None.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud) 1) 9600

Data bits 2) 8

Stop bits 3) 1

Parity 4) None

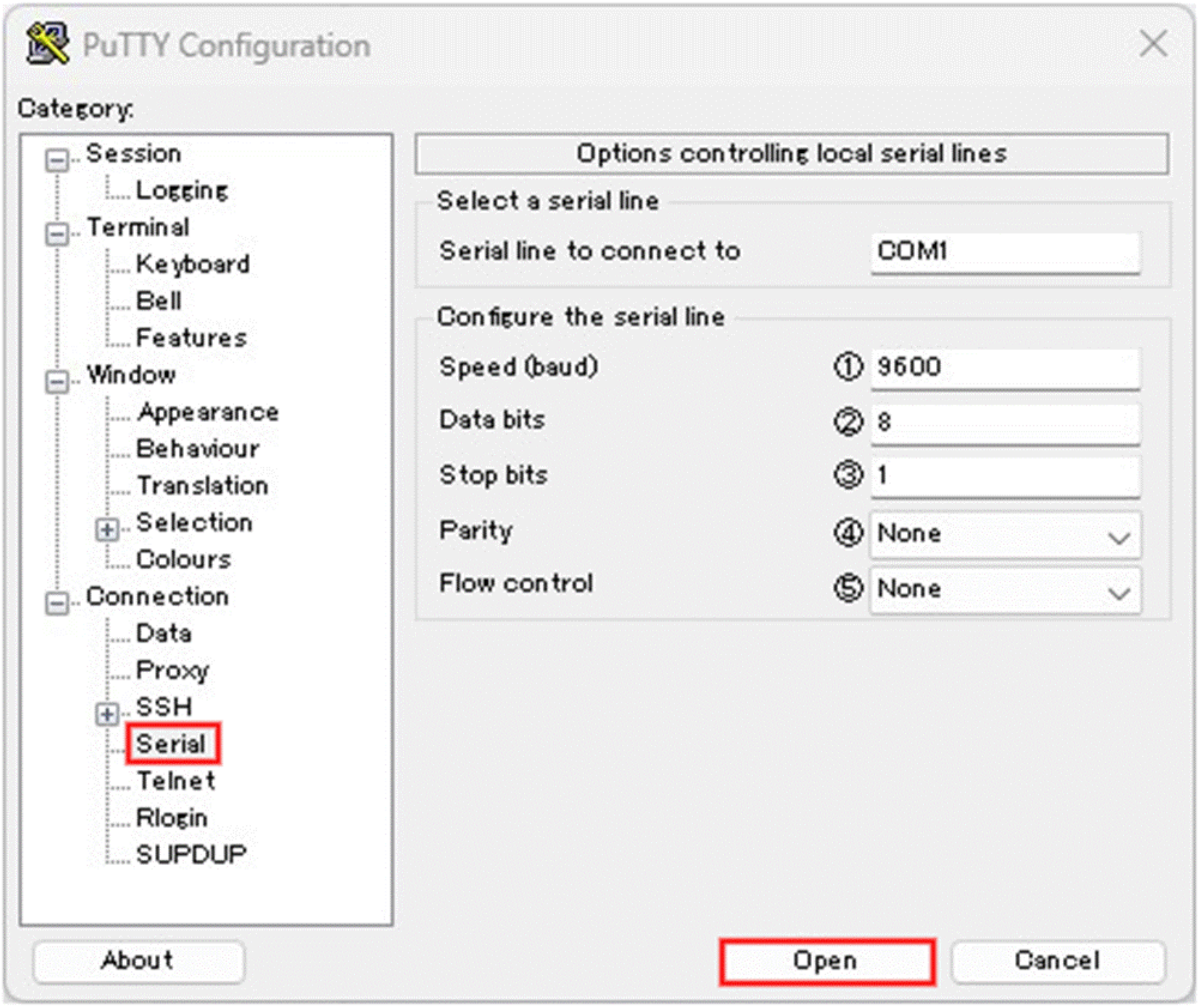
Flow control 5) None

Note

5.2 Navigating the Cisco IOS CLI

Flow control: None

Figure 5.5 How to use PuTTy to access a Cisco device's CLI via the console port. From the Serial tab, configure the following settings and then click Open: 1) Speed (baud): 9600 bits per second, 2) Data bits: 8, 3) Stop bits: 1, 4) Parity: None, 5) Flow control: None



Serial line to connect to: COM1

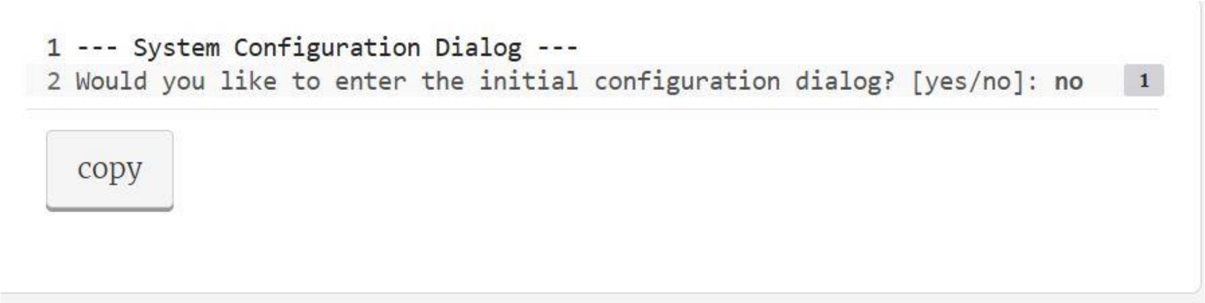
① Speed (baud): 9600

② Data bits: 8

③ Stop bits: 1

④ Parity: None

⑤ Flow control: None

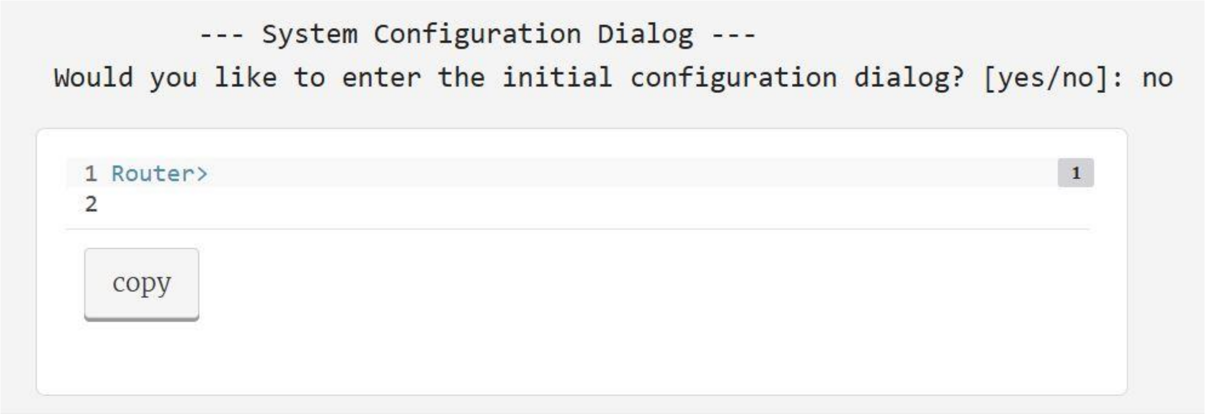


```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
```

5.2 Navigating the Cisco IOS CLI

Now we will finally get hands-on in the Cisco IOS CLI, navigating through different modes and giving commands to a Cisco device. I want to emphasize once again that networking is not just theory, but also a practical skill. It will be difficult to absorb this information without putting it into practice yourself, so I highly recommend following along in Packet Tracer (or the CLI of a real Cisco router or switch) as you read, and trying out the different commands and shortcuts we cover.

5.2.1 The EXEC modes



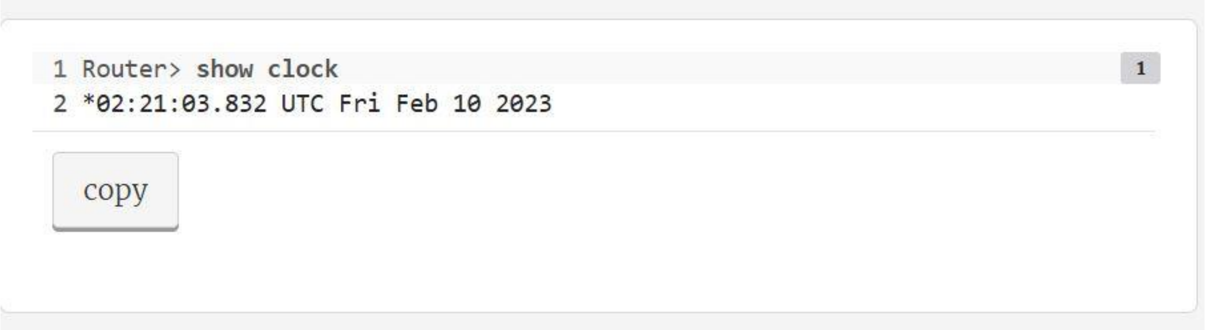
```
          --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Router>

```

Note

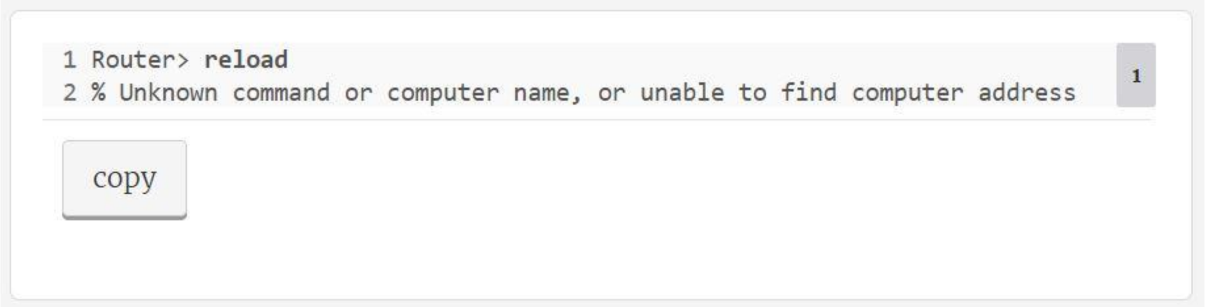
The system configuration dialog is a step-by-step configuration wizard that allows you to do a simple setup of the device without having to know Cisco IOS CLI commands. This feature is typically not used and it’s not something you need to know for the CCNA, so I recommend skipping it by typing no and hitting the Enter key (the options [yes/no] are shown in square brackets).



```
Router> show clock
*02:21:03.832 UTC Fri Feb 10 2023
```

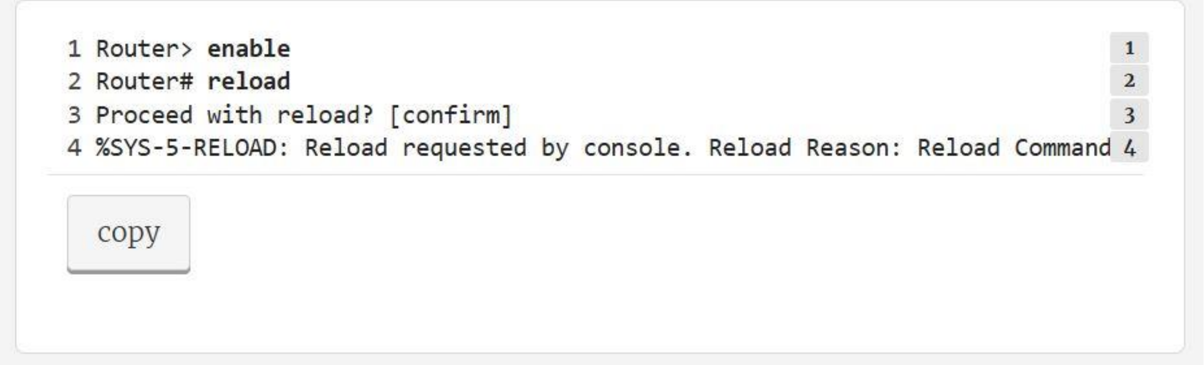
Note

All of the commands we cover in this chapter apply to both Cisco routers and switches - they both run the same operating system: Cisco IOS.



```
Router> reload
% Unknown command or computer name, or unable to find computer address
```

Router> show clock *02:21:03.832 UTC Fri Feb 10 2023



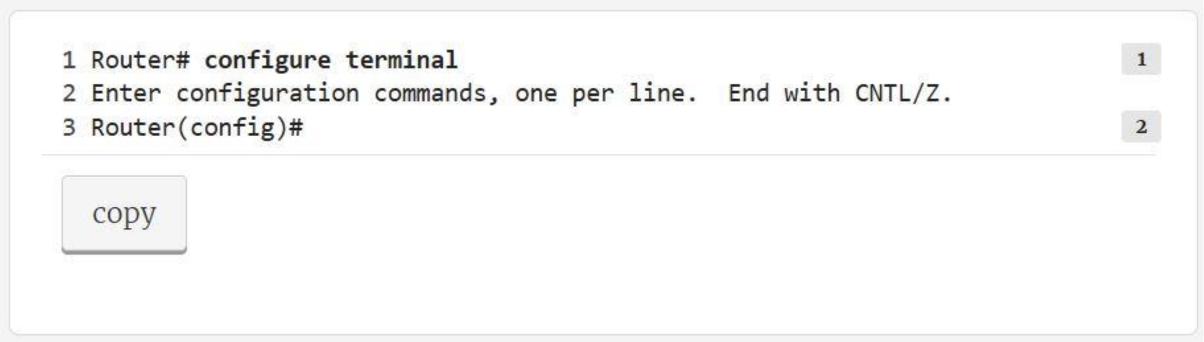
```
Router> enable
Router# reload
Proceed with reload? [confirm]
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command
```

Note

Checking the time is clearly not intrusive, so the show clock command is available in user EXEC mode. However, a more intrusive command like reload, which restarts the device, does not work in user EXEC mode, as shown in the example below. The router displays an error message instead (a percent sign indicates a message from IOS).

Router> reload % Unknown command or computer name, or unable to find computer address

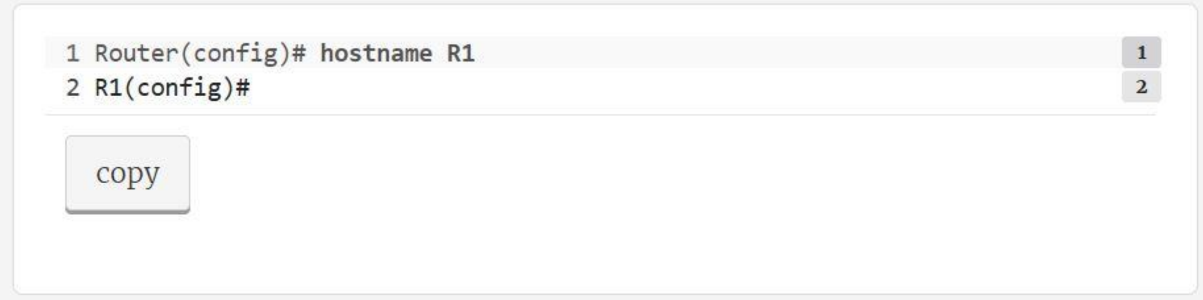
To access more powerful commands you must enter the next mode in the IOS command hierarchy: *privileged EXEC mode*. To access privileged EXEC mode, use the enable command. From privileged EXEC mode, the reload command now works.



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

Privileged EXEC mode gives unlimited access to the available show commands as well as many other commands to control various features of the device. To return to user EXEC mode from privileged EXEC mode, you can use the disable command. However, there is nothing you can do in user EXEC mode that you can’t do in privileged EXEC mode, so disable is not often used.

Although privileged EXEC mode is more powerful than user EXEC mode, both modes are limited in that they do not allow you to make changes to the device’s configuration. The EXEC modes only allow you to view the device’s status and configuration, as well as execute operational commands to perform actions like restart the device, save the configuration, move and delete files, etc.



```
Router(config)# hostname R1
R1(config)#
```

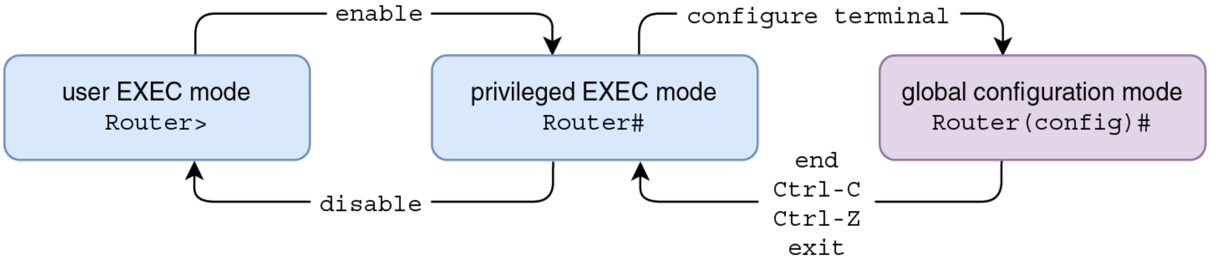
Note

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

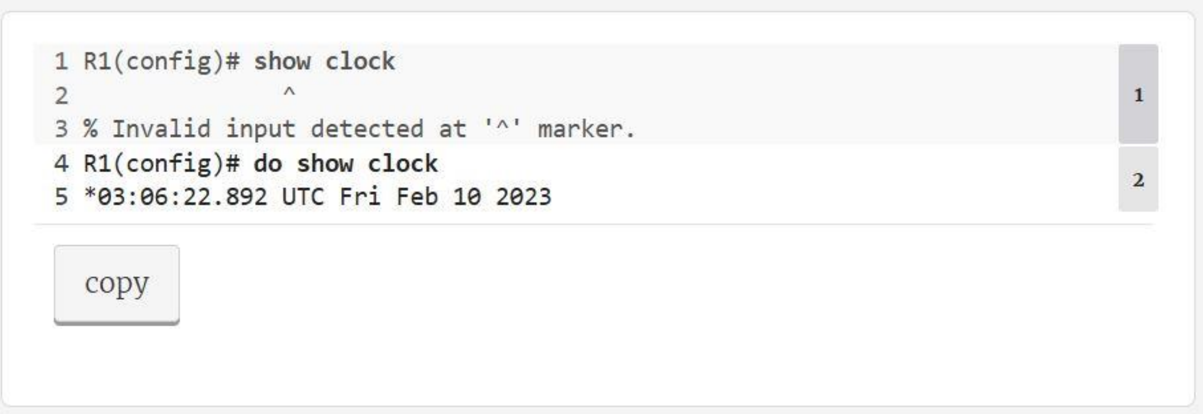
Note

Although there are only two EXEC modes in the Cisco CLI (*user EXEC mode* and *privileged EXEC mode*), there are several configuration modes which we will examine throughout this book. In this chapter we will only look at the first one, global configuration mode. From global configuration mode you can configure various features like the device’s hostname and passwords. From this mode you can also access the other configuration modes we will look at in later chapters of this book

Figure 5.6 How to navigate between user EXEC mode, privileged EXEC mode, and global configuration mode in the Cisco IOS command hierarchy



Router(config)# hostname R1 R1(config)#

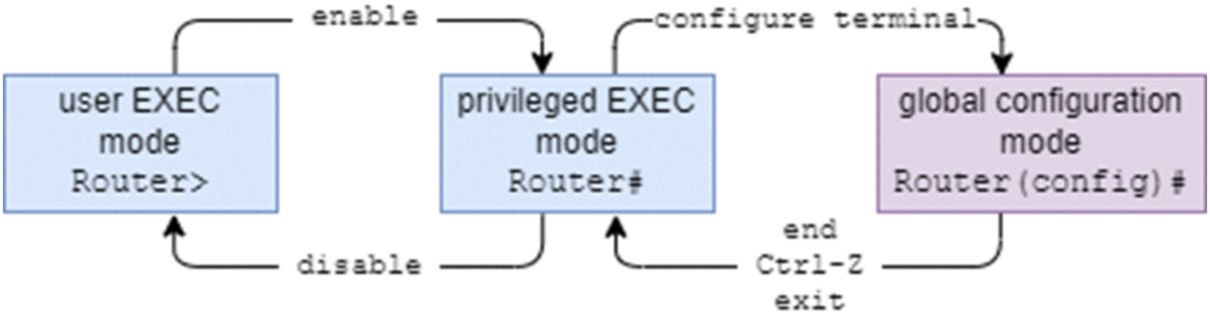


```
R1(config)# show clock
              ^
% Invalid input detected at '^' marker.
R1(config)# do show clock
*03:06:22.892 UTC Fri Feb 10 2023
```

5.2.3 Keyboard shortcuts

To return from global configuration mode to privileged EXEC mode, there are a few options. The end command or the Ctrl-Z keyboard shortcut will return you to privileged EXEC mode from global configuration mode or any other configuration mode. The exit command will return you to privileged EXEC mode from global configuration mode. However, if you're in another configuration mode, it will return you to global configuration mode. Figure 5.6 shows how to navigate between user EXEC mode, privileged EXEC mode, and global configuration mode.

Figure 5.6 How to navigate between user EXEC mode, privileged EXEC mode, and global configuration mode in the Cisco IOS command hierarchy


enable
configure terminal
user EXEC mode Router>
privileged EXEC mode Router#
global configuration mode Router(config)#
disable
end
Ctrl-Z
exit

Configuration modes such as global configuration mode allow you to configure the device, but EXEC mode commands like show do not work. However, the do command allows you to use EXEC mode commands from a configuration mode, so you don't have to return to privileged EXEC mode. This can speed up your workflow when you are configuring a device but also want to use show commands to check its status. The example below demonstrates this; the show clock command results in an error message, but the do show clock command displays the time of the device.

```
R1(config)# show clock

^

% Invalid input detected at '^' marker.

R1(config)# do show clock

*03:06:22.892 UTC Fri Feb 10 2023
```

5.2.3 Keyboard shortcuts

There are several keyboard shortcuts that can help you more smoothly navigate through the CLI and enter commands. We covered one in the previous section; Ctrl-Z can be used to return to privileged EXEC mode from any configuration mode. There are many others, and we will look at a few of them below.

When typing commands in the CLI there is a cursor indicating where the next character will be inserted when typed. By default this will be after the previous character, as you would probably expect. You can also move the cursor, for example to fix an error in a previously typed word. Below are some keyboard shortcuts than can be used to move the cursor and edit the current command you are typing:

- Left arrow: moves the cursor left
- Right arrow: moves the cursor right

- Backspace: moves the cursor left and deletes the previous character
- Ctrl-A: moves the cursor to the beginning of the command you are typing

5.2.4 Context-sensitive help

Ctrl-U: deletes all characters to the left of the cursor

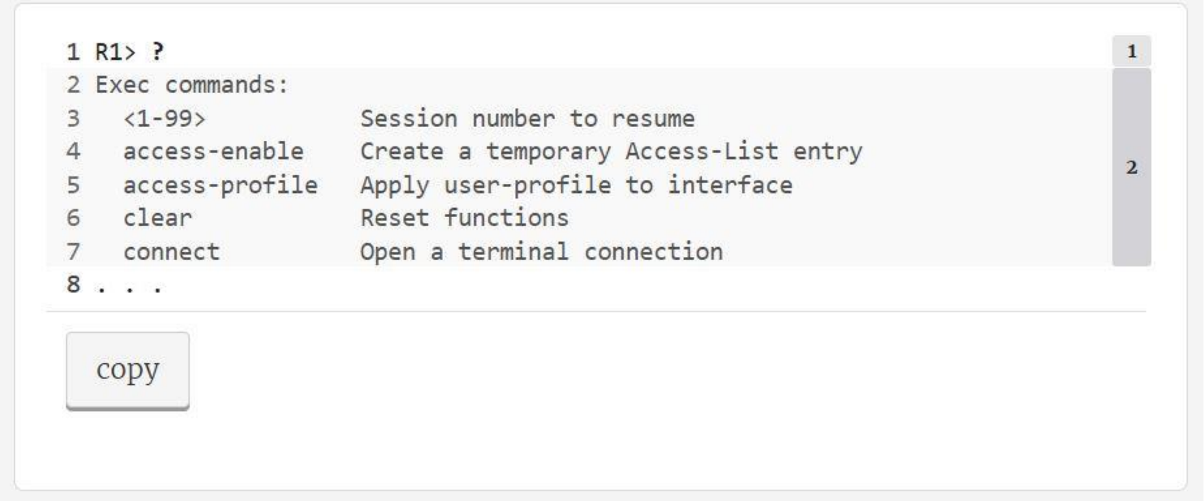
Viewing the available commands

Up arrow: previous command

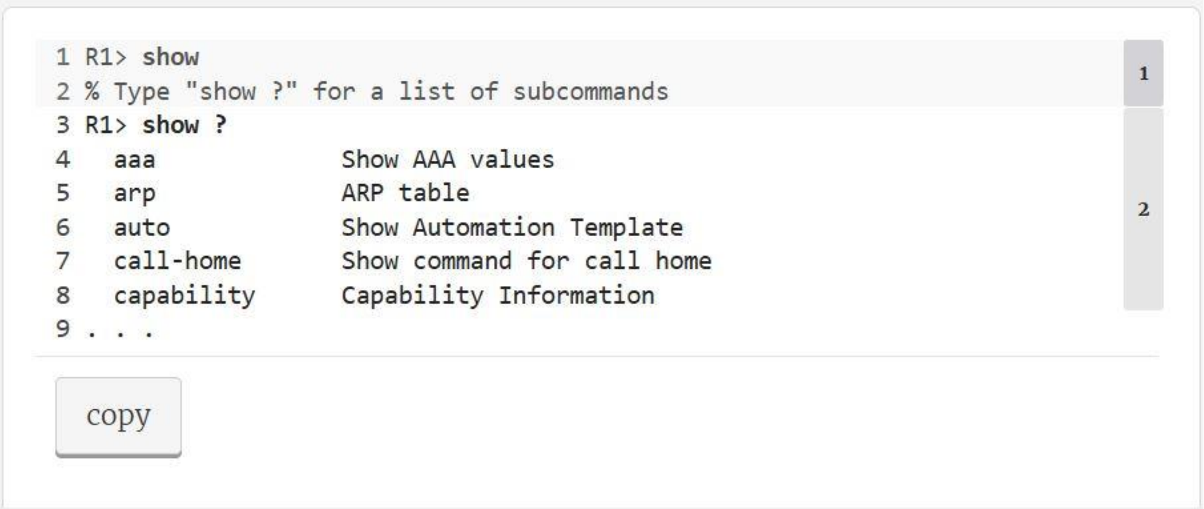
- Down arrow: next command

5.2.4 Context-sensitive help

You will have to learn many different commands to prepare for the CCNA, and those commands are only a fraction of all of the available commands in Cisco IOS. For the purpose of the CCNA exam, it is important to practice and become familiar with the various commands we will look at in this book. However, Cisco IOS has a feature called *context-sensitive help* that can help you if you have forgotten a command.

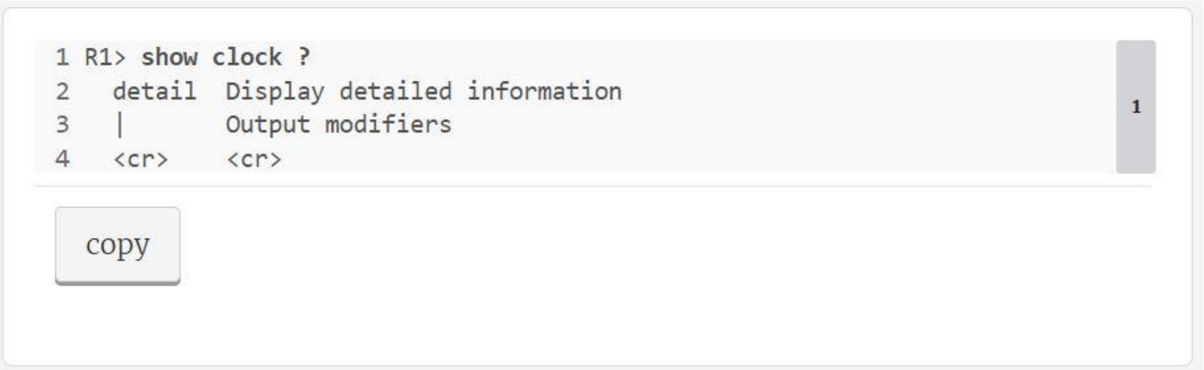


```
R1> ?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
. . .
```



```
R1> show
% Type "show ?" for a list of subcommands
R1> show ?
  aaa             Show AAA values
  arp             ARP table
  auto            Show Automation Template
  call-home       Show command for call home
  capability      Capability Information
. . .
```

to list the possible completions of a partially-typed command or keyword

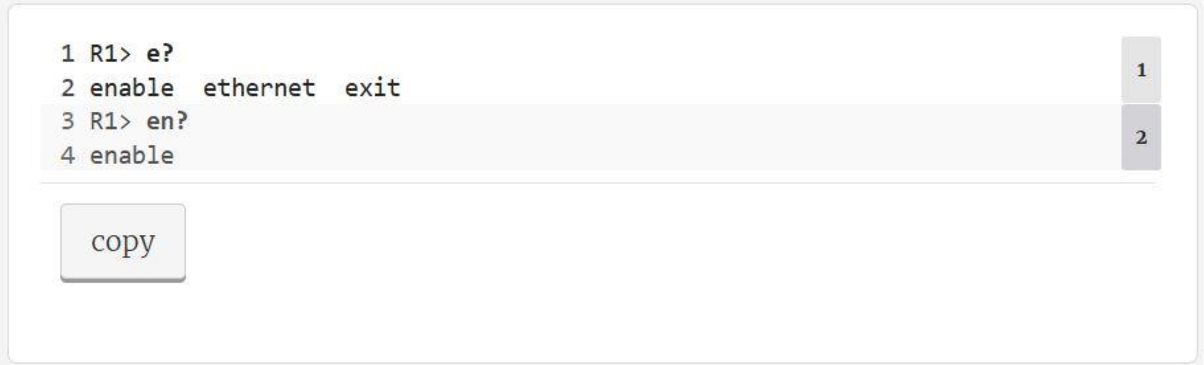


```
R1> show clock ?
  detail  Display detailed information
  |       Output modifiers
  <cr>    <cr>
```

The other two options displayed are also worth mentioning:

- Few Cisco IOS commands are a single word; most commands include one or more *keywords*, which are further parameters typed after the initial command. The show command we looked at previously is an example of this; show on its own is not a valid command, but show clock is. In the second use case of the question mark, you can use it after a command to view the available keywords. The example below demonstrates this:
- R1> show % Type "show ?" for a list of subcommands R1> show ? aaa Show AAA values arp ARP table auto Show Automation Template call-home Show command for call home capability Capability Information . . .

You can also use the question mark in this manner after a keyword to display any further keywords. For example, show clock ? lists the keyword detail which can be used to view more information about the device's clock. This is shown in the following example:

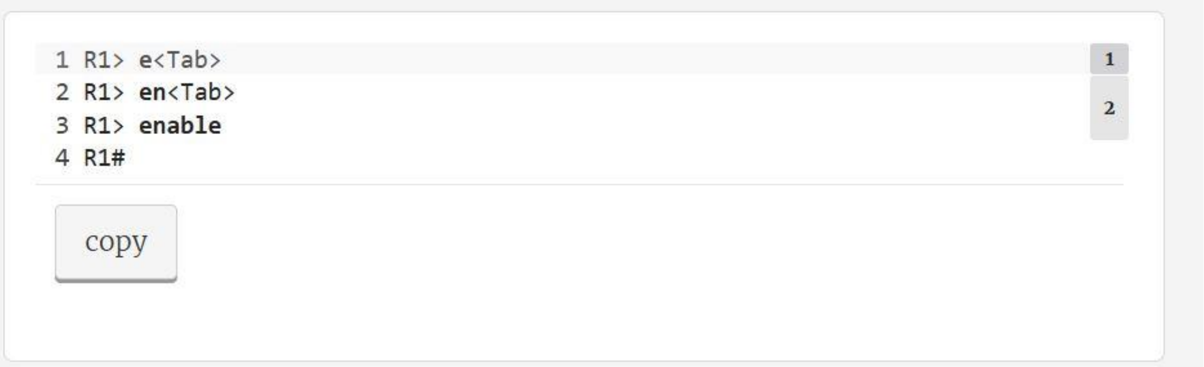


```
R1> e?
enable  ethernet  exit
R1> en?
enable
```

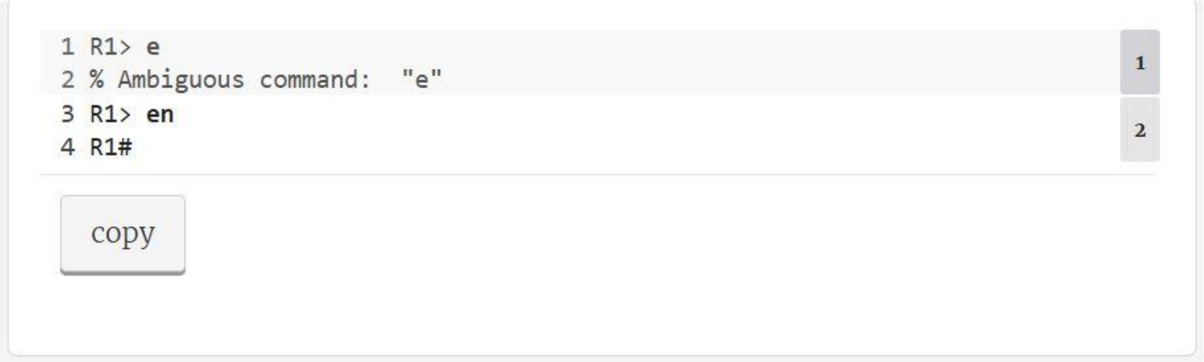
Auto-completing commands

The pipe (|) can be used to filter the output of a show command. I will show an example of this later in this chapter.

<cr> means carriage return, which refers to the Enter key. This means that you can simply press Enter to execute the command. Although a keyword (detail) is available, show clock on its own is a valid command.



```
R1> e<Tab>
R1> en<Tab>
R1> enable
R1#
```



```
R1> e
% Ambiguous command:  "e"
R1> en
R1#
```

Note

If you type enough characters so that there is only one possible command beginning with those characters and then press the Tab key, IOS will automatically complete the command for you. For example, typing en and then pressing Tab will automatically complete the command to enable. Then you can simply press Enter to execute the command. However, if you don't type enough characters and there are multiple possible commands beginning with the character(s) you have typed, the command won't work; it will simply print the character(s) again on a new line. This is shown in the example below. Note that <Tab> indicates where I pressed the Tab key.

R1> e<Tab>

R1> en<Tab>

R1> enable

R1#

Table 5.1 summarizes the above context-sensitive help features. Spend some time experimenting with them in the CLI; once you get used to them, you will probably find yourself using them quite often as you practice configuring and verifying the various IOS features you need to know for the CCNA.

Table 5.1 Cisco IOS context-sensitive help features (view table figure)

Command	**Description**
?	Lists the available commands in the current mode
command **?**	Lists the available keywords for the command

Command	**Description**
partial-command **?**	Lists the possible commands beginning with the currently typed characters
partial-command<Tab>	Automatically completes the command if there is only one option beginning with the currently typed characters
partial-command<Enter>	Executes the command if there is only one option beginning with the currently typed characters

5.3 IOS configuration files

Cisco IOS devices make use of two different text files that store the device's configurations: the *running-config* and the *startup-config*. The two files are each stored in different hardware memory and serve different purposes. You can view each configuration file with the show running-config and show startup-config commands.

Definition

The configurations in the *running-config* file determine the current operations of the device. When you enter a configuration command in the CLI, you are modifying the running-config file. Changes take effect instantly; as shown previously, after the hostname command is executed, the hostname of the device changes immediately.

The running config file is stored in *random-access memory* (RAM). It is important to note that the contents of RAM are lost when the device is powered off or restarted; therefore changes to the running-config are lost in either event. To save configuration changes so they persist even if the device is powered off or restarted, the startup-config is used.

- **write**
- **write memory**
- **copy running-config startup-config**

Note

There are a few different commands (entered in privileged EXEC mode) that can be used to copy the contents of the running-config file to the startup-config file. The effect of each of these commands is the same, so it doesn't matter which one you use:

write

- **write erase**
- **erase nvram:**
- **erase startup-config**

5.4 Password-protecting privileged EXEC mode

If you want to return a device to its factory-default configuration, you can erase the startup-config and then restart the device with the reload command. Just as with saving the configuration, there are a few different commands you can use to delete the startup-config:

5.4.1 Configuring the enable password

erase nvram:

Note

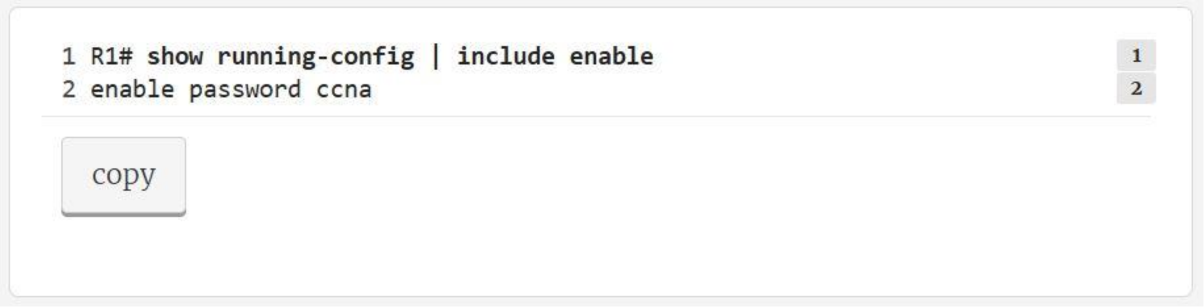
5.4 Password-protecting privileged EXEC mode

Privileged EXEC mode not only allows a user to execute any of the available show commands to gather information about the device's configuration and status, it also allows the user to access global configuration mode and make configuration changes to the device. Because of this, it's always a good idea to configure a password to prevent unauthorized users from accessing privileged EXEC mode. In this section we will look at the *enable password* and its more secure version, the *enable secret*.

```
R1(config)# enable password ccna
R1(config)# exit
R1# disable
R1> enable
Password:
R1#
```

copy

The *enable password* is a password that you must enter to access privileged EXEC mode. It’s also the name of the command used to configure the password; you configure it with the enable password command in global configuration mode.

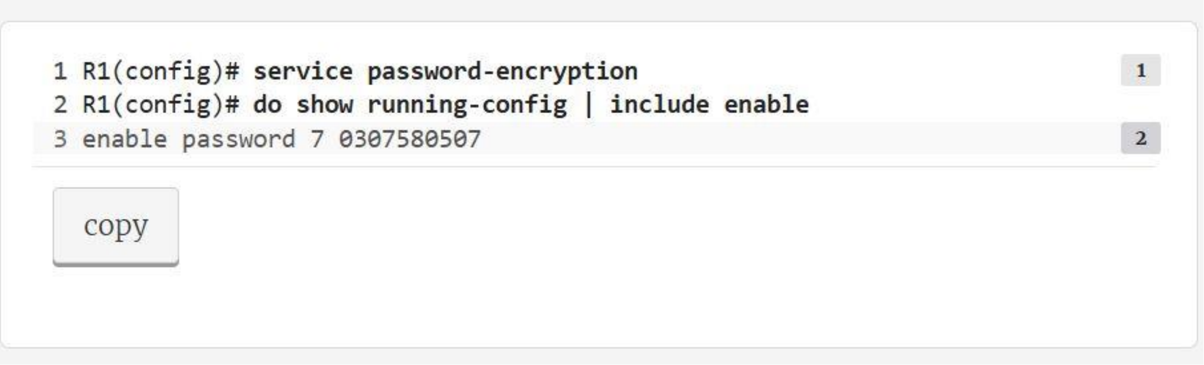


```
R1# show running-config | include enable
enable password ccna
```

Note

The enable password is case-sensitive: *cisco* and *Cisco* are two different passwords

In the following example I configure an enable password of *ccna*, use exit to return to privileged EXEC mode and disable to return to user EXEC mode. When I then use enable to return to privileged EXEC mode again, I have to enter the configured enable password of *ccna* to gain access. Note that, for security purposes, passwords are not displayed as you type them in Cisco IOS.



```
R1(config)# service password-encryption
R1(config)# do show running-config | include enable
enable password 7 0307580507
```

Note

R1# show running-config | include enable

enable password ccna

Note

To improve the security of the enable password, you can use the service password-encryption command in global configuration mode. This encrypts all current passwords configured on the device, as well as passwords you configure in the future. The following example demonstrates this: after issuing the command and viewing the running-config again, the plaintext password is not shown. Instead, the password is stored as *ciphertext* (the encrypted form of the plaintext).

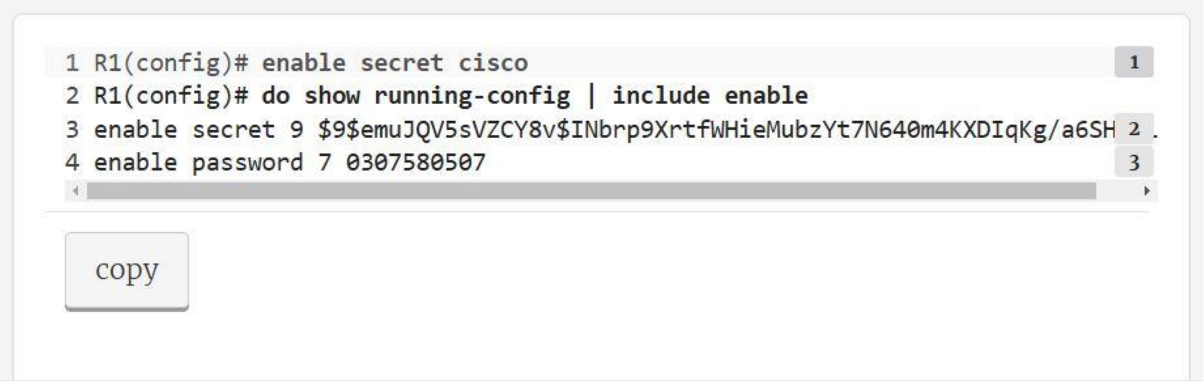
R1(config)# service password-encryption

R1(config)# do show running-config | include enable

enable password 7 0307580507

The 7 before the ciphertext string 0307580507 indicates the encryption type.

5.4.2 Configuring the enable secret



```
R1(config)# enable secret cisco
R1(config)# do show running-config | include enable
enable secret 9 $9$emuJQV5sVZCY8v$INbrp9XrtfWHieMubzYt7N640m4KXDIqKg/a6SH
enable password 7 0307580507
```

Note

If you use the no service password-encryption command to undo the encryption, currently-encrypted passwords will not be decrypted. Future passwords, however, will not be encrypted.

The enable password is an example of a *legacy* feature – something that has been replaced with a newer feature (the enable secret) but is still supported in Cisco IOS. The differences between the enable password and the enable secret are a potential exam question, but when configuring network devices you should always use the enable secret.

Summary

- A *shell* is a computer program that allows a user to interact with the computer. A *graphical user interface* (GUI) is a shell with a graphical interface, and a *command-line interface* (CLI) is a shell with a text-based interface.
- For the CCNA exam, you must be able to use the Cisco IOS CLI to configure the protocols and features listed in the exam topics list.
- The CLI of a network device can be accessed by connecting a PC to the device's *console port* with a console (crossover) cable or by connecting over the network infrastructure using *Telnet* or *Secure Shell* (SSH).
- After physically connecting a PC to the device's console port, a *terminal emulator* application (such as PuTTY) is required to access the CLI.
- To give commands to a network device, you type commands in the CLI and press Enter.
- After connecting to a device's CLI, you will be in *user EXEC mode*, which only allows you to view basic information about the device but not perform anything intrusive. The format of the prompt is hostname>.
- To access more powerful commands, use the **enable** command to access *privileged EXEC mode*, which provides unlimited access to EXEC mode commands. For example, you can view information about the device, restart it, save the configuration, move and delete files, etc. The format of the prompt is hostname#.

- Use the **disable** command to return to user EXEC mode from privileged EXEC mode.
- Use the **reload** command in privileged EXEC mode to restart the device.
- To make configuration changes to the device, use the **configure terminal** command in privileged EXEC mode to access *global configuration mode*. The prompt is hostname(config)#.
- Global configuration mode allows you to make configuration changes to the device. It also allows you to access other configuration modes for specific features.
- To change the hostname of the device, use the **hostname** command in global configuration mode.
- To undo a command, use **no** in front of the command. For example, **no hostname R1**.
- Use the **end** command, the **exit** command, or the Ctrl-C/Ctrl-Z shortcuts to return to privileged EXEC mode from global configuration mode.
- When in a configuration mode, you can use **do** in front of a command to execute EXEC mode commands.
- Keyboard shortcuts can be used to move the cursor and scroll through previously executed commands.
- *Context-sensitive help* can be used for guidance within the CLI. It can list available commands and possible completions for partially written words.
- Cisco IOS devices use two configuration files: the *running-config* file and the *startup-config* file.
- The running-config file is stored in RAM and determines the current operations of the device. Configuration commands change running-config and immediately take effect. The running-config file is lost when the device is powered off or restarted.
- The startup-config file is stored in *nonvolatile RAM* (NVRAM) and does not determine the current operations of the device. The contents of startup-config are copied to running-config when the device boots up.
- To save the running-config file to the startup-config file, use **write, write memory**, or **copy running-config startup-config** in privileged EXEC mode.
- To return the device to the factory-default configuration, delete startup-config with **write erase, erase nvram:**, or **erase startup-config**, and restart the device with **reload**.
- Privileged EXEC mode can be password-protected with an *enable password* or *enable secret*. If both the **enable password** and **enable secret** commands are configured, only the enable secret can be used to access privileged EXEC mode.
- The enable password can be configured with the **enable password** command in global configuration mode. It is stored in the configuration as cleartext by default but can be encrypted with the **service password-encryption** command (type 7).

- The enable password remains in Cisco IOS as a legacy feature, but on modern devices, the enable secret should be used instead.
- The enable secret can be configured with the **enable secret** command in global configuration mode. It is stored in the configuration as a *hash*, using one of multiple hashing algorithms. The hashing algorithms available vary depending on the IOS version.
- *Message Digest 5* (MD5) is type 5 encryption, and *scrypt* is *type 9*. *scrypt* is more secure and should be used instead of MD5 if supported by the device.