

Cisco Press

Brought to you by:



Buy this book at:



This chapter covers the following topics that you will need to master as a CCNA:

- **The IOS and Its User Interface** This section examines the types of memory used by the IOS, in addition to the commands used to examine and change the contents. This section also describes the basic functions and help for the command-line interface (CLI), and discusses how syslog messages are treated.
- **Configuration Processes and the Configuration File** The configuration file used for a router contains all the configuration for that router. This section covers all commands used to change the configuration and manipulate the configuration file.
- **Managing IOS Images** This section covers in detail the processes for upgrading the IOS in Flash memory, as well as the commands used to tell the router which IOS image to use. Password recovery is included as well.

Permission and Copyright

This material is reprinted from *Cisco CCNA: Exam #640-507 Certification Guide*, ©2000 by Cisco Press. Used with permission.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Cisco Internetwork Operating System (IOS) Fundamentals

The CCNA exam requires that you understand the basics of the Cisco Internetwork Operating System (IOS). In fact, the only operating system and user interface covered on the CCNA exam is the IOS and its user interface. The omission of other user interfaces, in particular the Catalyst 5000/5500 series user interface, is one of the most important facts to note when determining what to study for the CCNA exam.

The IOS runs on some Cisco switch models and provides the familiar IOS command-line interface (CLI). This chapter is geared toward the IOS CLI on a router. Chapter 4, “Bridges/Switches and LAN Design,” covers some details of IOS CLI on LAN switches. The user interface is the same, but some commands are different.

The exam also includes questions on both router and LAN switch usage of the IOS. No one should be surprised that the CCNA exam covers IOS running on routers. Also covered on the exam is the use of IOS running on Cisco 1900 series switches. User interfaces on other switch platforms might seem to be like IOS and have similar features, but these details are not covered on the exam. That should be particularly helpful for those of you with less hands-on experience.

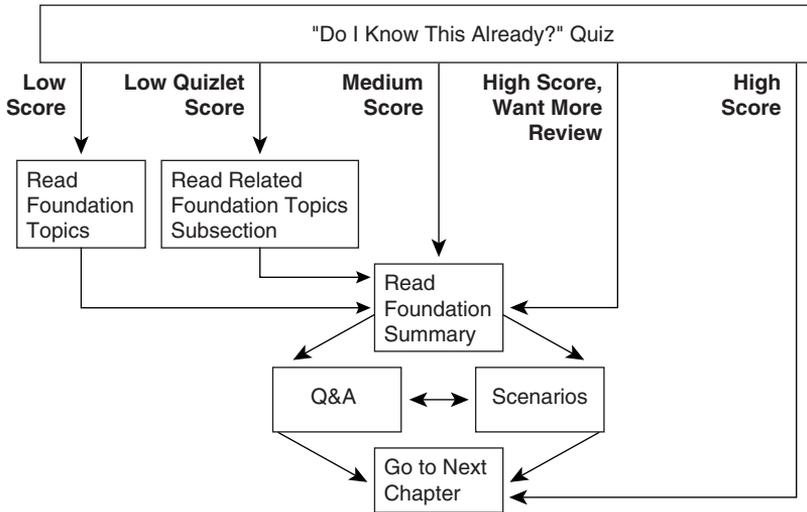
Cisco requires that CCNAs exhibit a solid recollection of the many details of the CLI. Of course, the best way to learn about any user interface is to use it. If you can spend time using a Cisco router, the knowledge and recall you gain will be of significant value. This chapter is designed to remind you of details you might not notice when practicing and will provide a reference for those of you who do not have access to routers for practice. Still, there is no substitute for hands-on practice.

How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and the answers for all your work with this book in one place, for easy reference.
- Take the “Do I Know This Already?” quiz, and write down your answers. Studies show that retention is significantly increased through writing down facts and concepts, even if you never look at the information again.
- Use the diagram in Figure 2-1 to guide you to the next step.

Figure 2-1 *How to Use This Chapter*



“Do I Know This Already?” Quiz

The purpose of the “Do I Know This Already?” quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

This 12-question quiz helps you determine how to spend your limited study time. The quiz is sectioned into three smaller four-question “quizlets,” which correspond to the three major topic headings in the chapter. Figure 2-1 outlines suggestions on how to spend your time in this chapter based on your quiz score. Use Table 2-1 to record your scores.

Table 2-1 *Scoresheet for Quiz and Quizlets*

Quizlet Number	Foundation Topics Section Covering These Questions	Questions	Score
1	The IOS and Its User Interface	1 to 4	
2	Configuration Processes and the Configuration File	5 to 8	
3	Managing IOS Images	9 to 12	
All questions		1 to 12	

- 1 What are the two different names for the router’s mode of operation that, when accessed, enables you to issue commands that could be disruptive to router operations?

- 2 What command would you use to receive command help if you knew that a **show** command option begins with a **c**, but you cannot recall the option?

- 3 After typing **show ip route**, which is the only command you issued since logging in to the router, you now want to issue the **show ip arp** command. What steps would you take to execute this command by using command recall keystrokes?

- 4 What is the name of the user interface mode of operation used when you cannot issue disruptive commands?

- 5 What configuration command causes the router to require a password from a user at the console? What configuration mode context must you be in—that is, what command(s) must be typed before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.

- 6 What does CDP stand for?

7 What does the NV stand for in NVRAM?

8 Name two commands used to view the configuration that is currently used in a router. Which one is a more recent addition to the IOS?

9 What two methods could a router administrator use to cause a router to load the IOS stored in ROM?

10 What is the process used to update the contents of Flash memory so that a new IOS in a file called c4500-d-mz.120-5.bin, on TFTP server 128.1.1.1, is copied into Flash memory?

11 Two different IOS files are in a router's Flash memory: one called c2500-j-1.111-3.bin and one called c2500-j-1.112-14.bin. Which one does the router use when it boots up? How could you force the other IOS file to be used? Without looking at the router configuration, what command could be used to discover which file was used for the latest boot of the router?

12 What are the primary purposes of Flash memory in a Cisco router?

The answers to the “Do I Know This Already?” quiz are found in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections,” on page 701. The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. This includes the “Foundation Topics” and “Foundation Summary” sections, the Q&A section, and the scenarios at the end of the chapter.
- **2 or less on any quizlet**—Review the subsection(s) of the “Foundation Topics” part of this chapter, based on Table 2-1. Then move into the “Foundation Summary” section, the Q&A section, and the scenarios at the end of the chapter.
- **7, 8, or 9 overall score**—Begin with the “Foundation Summary” section and then go to the Q&A section and the scenarios at the end of the chapter.
- **10 or more overall score**—If you want more review on these topics, skip to the “Foundation Summary” section and then go to the Q&A section and the scenarios at the end of the chapter. Otherwise, move to the next chapter.

Foundation Topics

The IOS and Its User Interface

IOS, a registered trademark of Cisco Systems, is the name of the operating system found in most of Cisco's routers. The majority of Cisco routers run the IOS, with its familiar command-line interface (CLI). Also, some routing cards in other devices run IOS. For example, the Route/Switch Module (RSM) card for the Catalyst 5000 series LAN switches performs routing functions and executes the IOS.

Fixes and code updates to the IOS can include new features and functions. To learn more about the code release process, features added at particular IOS revision levels, and other terminology that will help you talk to the Cisco Technical Assistance Center (TAC), check out a current Cisco Product Bulletin describing the Software Release Process. One such example is Product Bulletin #537 (http://www.cisco.com/warp/public/cc/cisco/mkt/ios/rel/prodlit/537_pp.htm).

The exam topics covered in this section will become second nature to you as you work with Cisco routers and switches more often. In fact, because this book purposefully was written for an audience that already has some training and experience with Cisco routers, several of the details in this chapter might already be ingrained in your memory. If you would like more review, or if you are still new to the IOS, read on—the details in this section are important to using Cisco routers and switches. This chapter reviews such topics as router components, the CLI, and how to navigate the IOS command set using Help and key sequences for command edit and recall.

Router Components

Before examining the IOS, a review of hardware and hardware terminology is useful. In addition to handling the logic of routing packets, the IOS controls the use of different physical components, which includes memory, processor, and interfaces. This section of the book reviews common hardware details.

All Cisco routers have a console port, and most have an auxiliary port. The console port is intended for local administrative access from an ASCII terminal or a computer using a terminal emulator. The auxiliary port, missing on a few models of Cisco routers, is intended for asynchronous dial access from an ASCII terminal or terminal emulator; the auxiliary port is often used for dial backup.

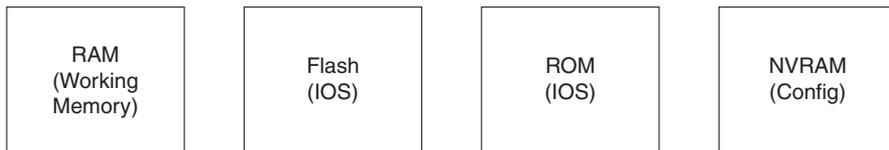
Each router has different types of memory, as follows:

- **RAM**—Sometimes called DRAM for *dynamic* random-access memory, RAM is used by the router just as it is used by any other computer: for working storage.

- **ROM**—This type of memory (read-only memory) stores a bootable IOS image, which is not typically used for normal operation. ROM contains the code that is used to boot the router until the router knows where to get the full IOS image.
- **Flash memory**—Either an EEPROM or a PCMCIA card, Flash memory stores fully functional IOS images and is the default where the router gets its IOS at boot time. Flash memory also can be used to store configuration files on Cisco 7500 series platforms.
- **NVRAM**—Nonvolatile RAM stores the initial or *startup* configuration file.

All these types of memory are permanent memory except RAM. No hard disk or diskette storage exists on Cisco routers. Figure 2-2 summarizes the use of memory in Cisco routers.

Figure 2-2 Cisco Router Memory Types



The processors in the routers vary from model to model. Although they are not specifically listed as requirements for the CCNA exam, some reference to terminology is useful. In most routers, only one processor option is available; thus, you would not order a specific processor type or card. The exception to this is the 7200 and 7500 families of routers. For instance, on the 7500 series, you choose either a Route Switch Processor 1 (RSP-1), RSP-2, or RSP-4 processor. In any case, all 7200 and 7500 routers, as well as most of the other Cisco router families, run IOS. This commonality enables Cisco to formulate exams, such as CCNA, that cover the IOS features without having to cover many hardware details.

Interfaces are used by a router for routing packets and bridging frames through a router. The types of interfaces available change over time due to new technology. For example, packet-over-SONET and voice interfaces are relatively recent additions to the product line. However, some confusion exists about what to call the actual cards that house the physical interfaces. Table 2-2 summarizes the terminology that might be referred to on the test.

Table 2-2 Samples of Router Interface Terminology

Model Series	What the IOS Calls Interfaces	What the Product Catalog Calls the Cards with the Interfaces on Them
2500	Interface	Modules and WAN interface cards
3600	Interface	Network modules and WAN interface cards
4500	Interface	Network processor modules
7200	Interface	Port adapters and service adapters
7500	Interface	Interface processors, and versatile interface processors with port adapters

Physical interfaces are referred to as *interfaces* by the IOS commands, as opposed to *ports* or *plugs*. IOS commands familiar on one platform will be familiar on another. Some nuances are involved in numbering the interfaces, however. In some smaller routers, the interface number is a single number. However, with some other families of routers, the interface is numbered first with the slot in which the card resides, followed by a slash and then the port number on that card. For example, port 3 on the card in slot 2 would be interface 2/3. Numbering starts with 0 for card slots and 0 for ports on any card. In some cases, the interface is defined by three numbers: first the card slot, then the daughter card (typically called a port adapter), and then a number for the physical interface on the port adapter. The 2600 and 3600 families also use a slot/port numbering scheme.

In this book, the single-digit interface numbers are used simply for consistency and readability.

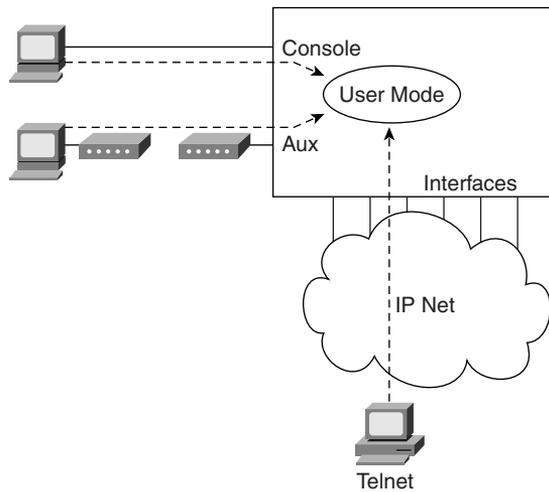
If you want to dig deeper, you might want to read about processors and interfaces in the Cisco Product Catalog (<http://www.cisco.com/univercd/cc/td/doc/pcat/>).

Command-Line Interface

Cisco uses the acronym CLI to refer to the terminal user command-line interface to the IOS. The term CLI implies that the user is typing commands at a terminal, terminal emulator, or Telnet connection. Although you can pass the CCNA exam without ever having used the CLI, actually using the CLI will greatly enhance your chances.

To access the CLI, use one of three methods, as illustrated in Figure 2-3.

Figure 2-3 CLI Access



Regardless of which access method is used, a CLI user initially is placed in user mode, or user EXEC mode, after logging in. *EXEC* refers to the fact that the commands typed here are executed, and some response messages are displayed onscreen. The alternative mode is *configuration mode*, which is covered in the next section.

Passwords can be required when accessing the CLI. In fact, the default configuration at IOS 12.x requires a password for Telnet and auxiliary port access, but no password is set—therefore, you must configure passwords from the console first. Table 2-3 reviews the different types of passwords and the configuration for each type.

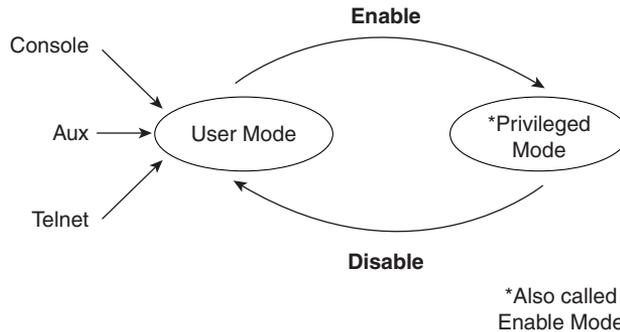
Table 2-3 CLI Password Configuration

Access From . . .	Password Type	Configuration
Console	Console password	line console 0 login password <i>faith</i>
Auxiliary	Auxiliary password	line aux 0 login password <i>hope</i>
Telnet	vtty password	line vty 0 4 login password <i>love</i>

The **login** command actually tells the router to display a prompt. The **password** commands specify the text password to be typed by the user to gain access. The first command in each configuration is a context-setting command, as described in the section “Configuration Processes and the Configuration File,” later in this chapter. Typically, all three passwords have the same value.

Several concurrent Telnet connections to a router are allowed. The **line vty 0 4** command signifies that this configuration applies to vtys (virtual teletypes—terminals) 0 through 4. Only these five vtys are allowed by the IOS unless it is an IOS for a dial access server, such as a Cisco AS5300. All five vtys typically have the same password, which is handy because users connecting to the router via a Telnet cannot choose which vty they get.

User EXEC mode is one of two command EXEC modes in the IOS user interface. *Enable* mode (also known as *privileged* mode or *privileged EXEC* mode) is the other. Enable mode is so named because of the command used to reach this mode, as shown in Figure 2-4; privileged mode earns its name because powerful, or privileged, commands can be executed there.

Figure 2-4 *User and Privileged Modes*

Navigating the IOS CLI

Several references are available for help when you are using the IOS. IOS documentation is available on CD and is free from Cisco if you own one router or switch under a current maintenance agreement. Paper documentation is also available from Cisco. If you prefer, Cisco Press offers the Cisco Documentation series (more information at www.ciscopress.com). In addition, all Cisco documentation is available online at Cisco's Web site (www.cisco.com/univercd/home/home.htm); the IOS command reference is found at www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/index.htm.

No matter which documentation you use, it is incredibly unlikely that you will remember all IOS commands. (The command reference manuals stack 14 inches high.) Therefore, you will find tools and tricks to recall commands particularly useful. Table 2-4 summarizes command recall help options available at the CLI. Note that in the first column, "Command" represents any command. Likewise, "parm" represents a command's parameter. For instance, the third row lists "command ?," which means that commands such as **show ?** and **copy ?** would list help for the **show** and **copy** commands, respectively.

Table 2-4 *IOS Command Help*

What You Type	The Help You Get
?	Help for all commands available in this mode.
help	Text describing how to get help. No actual command help is given.
command ?	Text help describing all the first parameter options for the command command .
com?	A list of commands that start with "com."
command parm?	This style of help lists all parameters beginning with "parm." (Notice, no spaces exist between "parm" and the ?.)

Table 2-4 *IOS Command Help (Continued)*

What You Type	The Help You Get
command parm<Tab>	If the user presses the Tab key midword, the CLI will either spell the rest of this parameter at the command line for the user, or do nothing. If the CLI does nothing, it means that this string of characters represents more than one possible next parameter, so the CLI does not know which to spell out.
command parm1 ?	If a space is inserted before the question mark, the CLI lists all next parameters and gives a brief explanation of each.
* When you type the ?, the IOS's CLI reacts immediately; that is, you don't need to press the Enter key or any other keys. The router also redisplay what you typed before the ? to save you some keystrokes. If you press Enter immediately after the ?, the IOS tries to execute the command with only the parameters you have typed so far.	
** "Command" represents any command, not the word "command." Likewise, "parm" represents a command's parameter, not the word "parameter."	

The context in which help is requested is also important. For example, when ? is typed in user mode, the commands allowed only in privileged EXEC mode are not displayed. Also, help is available in configuration mode; only configuration commands are displayed in that mode of operation.

Commands you use at the CLI are stored in a command history buffer that retains the last 10 commands you typed. You can change the history size with the **terminal history size x** command, where *x* is the number of commands for the CLI to recall; this can be set to a value between 0 and 256.

Of course, most people want to use a previously typed command (perhaps with a different parameter). Commands you have previously used during the current console/aux/Telnet can be retrieved and then edited to save you some time and effort. This is particularly useful when you are typing long configuration commands. Table 2-5 lists the commands used to manipulate previously typed commands.

Table 2-5 *Key Sequences for Command Edit and Recall*

Keyboard Command	What the User Gets
Up-arrow or Ctrl+p	This displays the most recently used command. If pressed again, the next most recent command appears, until the history buffer is exhausted. (The p stands for <i>previous</i> .)
Down-arrow or Ctrl+n	If you have gone too far back into the history buffer, these keys will go forward, in order, to the more recently typed commands. (The n is for <i>next</i> .)
Left-arrow or Ctrl+b	This moves the cursor backward in the currently displayed command without deleting characters. (The b stands for <i>back</i> .)

continues

Table 2-5 *Key Sequences for Command Edit and Recall (Continued)*

Keyboard Command	What the User Gets
Right-arrow or Ctrl+f	This moves the cursor forward in the currently displayed command without deleting characters. (The f stands for <i>forward</i> .)
Backspace	This moves the cursor backward in the currently displayed command, deleting characters.
Ctrl+a	This moves the cursor directly to the first character of the currently displayed command.
Ctrl+e	This moves the cursor directly to the end of the currently displayed command.
Esc+b	This moves the cursor back one word in the currently displayed command.
Esc+f	This moves the cursor forward one word in the currently displayed command.
Ctrl+r	This creates a new command prompt, followed by all the characters typed since the last command prompt was written. This is particularly useful if system messages confuse the screen and it is unclear what the user has typed so far.

NOTE One goal of this book is to help you learn more and solidify your understanding of the materials on the CCNA exam. Hopefully, Table 2-5 will further your understanding. Beware—these details are covered on the exam questions.

Syslog and Debug

The IOS creates messages when different events occur and, by default, sends them to the console. These messages are called *syslog* messages. If you have used the console of a router for any length of time, you likely have noticed these messages—and when they are frequent, you probably became a little frustrated.

The **debug** command is one of the key diagnostic tools for troubleshooting difficult problems on a router. **debug** enables monitoring points in the IOS and generates messages that describe what the IOS is doing and seeing. When any debug command option is enabled, the router processes the messages with the same logic as other syslog messages. Beware—some **debug** options create so many messages that the IOS cannot process them all, possibly crashing the IOS.

NOTE

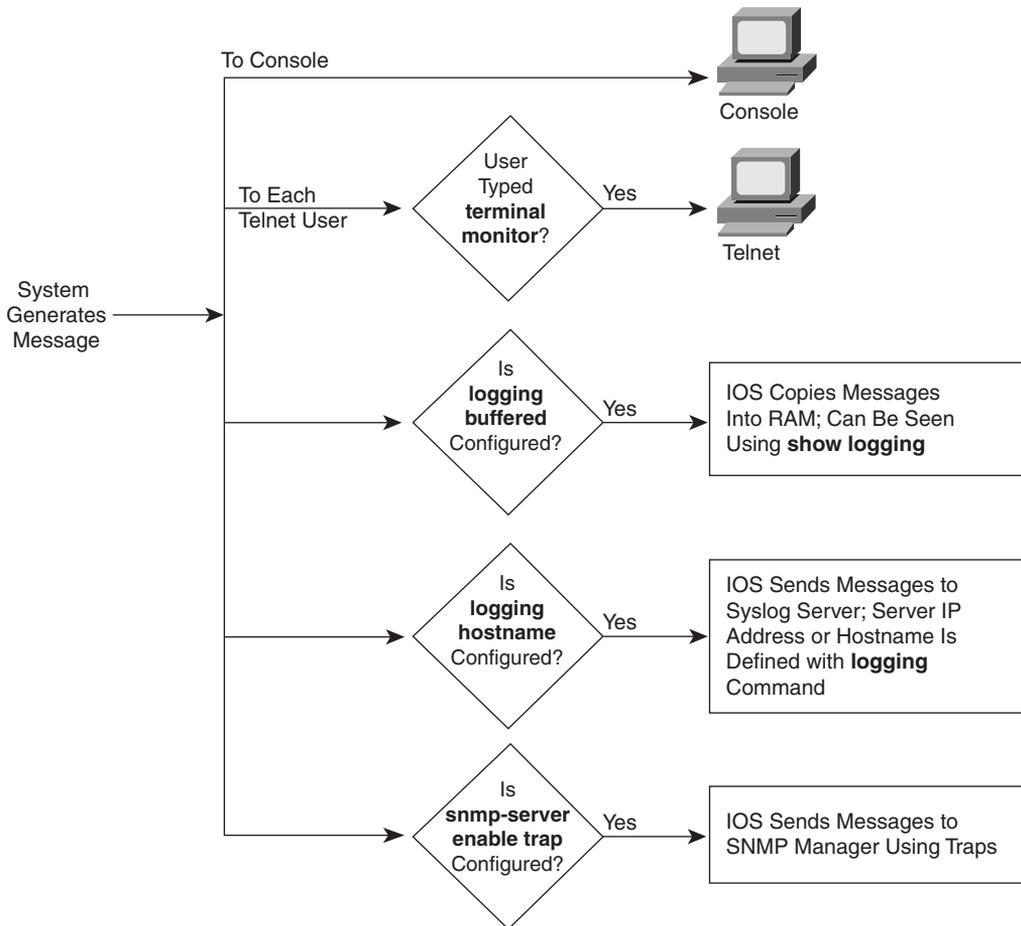
The **no debug all** command disables all debugs. Before enabling an unfamiliar **debug** command option, issue a **no debug all** and then issue the **debug** you want to use; then, quickly retrieve the **no debug all** command. If the messages are voluminous, press Enter immediately to try to prevent the router from crashing by immediately disabling all debugs.

Users might or might not be interested in seeing the messages as they occur. The console port always receives syslog messages. When a user telnets to the router, however, no syslog messages are seen unless the user issues the **terminal monitor** command. This command simply means that this terminal is monitoring syslog messages. Another alternative for viewing syslog messages is to have the IOS record the syslog messages in a buffer in RAM, and then use the **show logging** command to display the messages. For Telnet users, having the messages buffered using the global config command **logging buffered** is particularly useful. Because Telnet users do not get syslog messages by default anyway, these users can wait and look at syslog messages when desired. Finally, the **logging synchronous** line configuration subcommand can be used for the console and vtys to tell the router to wait until the user's last command output is displayed before showing any syslog messages onscreen. That provides a little less interruption for the user.

Syslog messages also can be sent to another device. Two alternatives exist: sending the messages to a syslog server, and sending the messages as SNMP traps to a management station. The **logging host** command, where *host* is the IP address or host name of the syslog server, is used to enable sending messages to the external server. After SNMP is configured, the **snmp-server enable trap** tells the IOS to forward traps, including syslog messages.

Figure 2-5 summarizes the flow of syslog messages, including debug messages. For a more detailed view of syslog messages, including restricting messages based on message severity, refer to the IOS documentation CD manual called "Troubleshooting Commands."

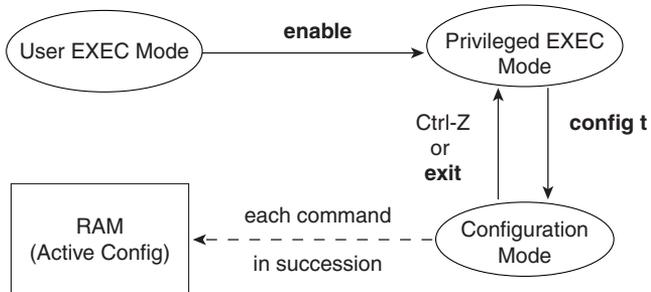
Figure 2-5 Syslog Message Flows



Configuration Processes and the Configuration File

Cisco requires that CCNAs master the process of changing and manipulating the configuration files in the IOS. This includes initially setting up an IOS device, handling ongoing configuration, and moving configuration files.

As mentioned in Chapter 1, “All About the Cisco Certified Network Associate Certification” configuration mode is another mode for the Cisco CLI. Changing the configuration of the router by typing various configuration commands is the purpose of configuration mode. Figure 2-6 illustrates the relationships among configuration mode, user EXEC mode, and privileged EXEC mode.

Figure 2-6 CLI Configuration Mode Versus EXEC Modes

Commands typed in configuration mode update the active configuration file. Changes are moved into the active configuration file each time the user presses the Enter key and are acted upon immediately by the router.

In configuration mode, context-setting commands are used before most configuration commands. These context-setting commands tell the router the topic about which you will type commands. More importantly, they tell the router what commands to list when you ask for help. After all, the whole reason for these contexts is to make online help more convenient and clear for you.

NOTE

Context setting is not a Cisco term—it's just a term used here to help make sense of configuration mode.

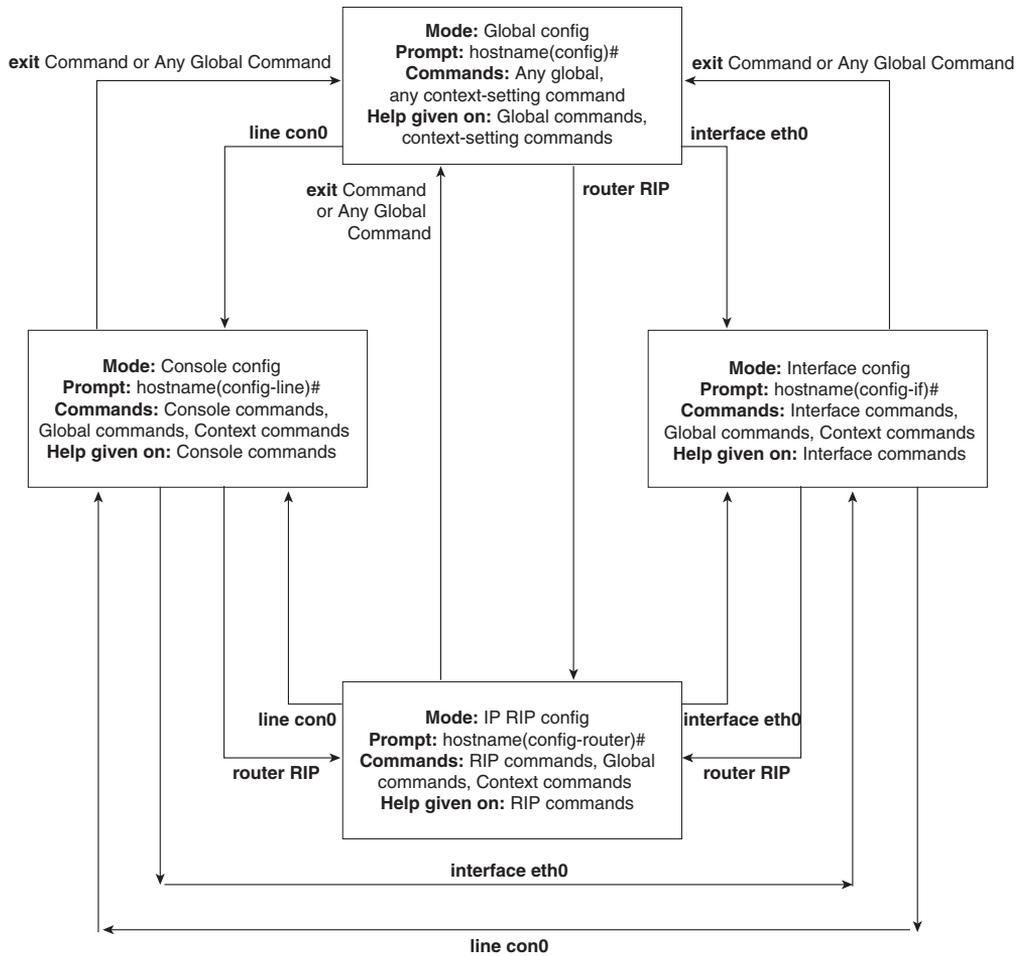
The **interface** command is the most commonly used context-setting configuration command. As an example, the CLI user could enter interface configuration mode after typing the **interface ethernet 0** configuration command. Command help in Ethernet interface configuration mode displays only commands that are useful when configuring Ethernet interfaces. Commands used in this context are called *subcommands*—or, in this specific case, *interface subcommands*. Figure 2-7 shows several different configuration mode contexts, including *interface configuration mode*, and illustrates the relationships and methods of moving among them.

The labels on the lines in Figure 2-7 represent the action or command that moves the user from one mode to another. For example, from console configuration mode (left box), the **interface ethernet 0** command could move you to the box on the right, which represents interface configuration mode.

If you have significant experience using the CLI in configuration mode, much of this will be second nature. From a CCNA exam perspective, recalling whether popular commands are global commands or subcommands will be useful. No set rules exist for what commands are global or subcommands, but generally, when multiple instances of a parameter can be set in

a single router, the command used to set the parameter is likely to be a configuration sub-command. Items that are set once for the entire router are likely to be global commands. For instance, the **hostname** command is a global command because there is only one host name per router. The **interface ethernet 0** command is a global configuration command because there is only one such interface in this router. Finally, the **ip address** command is an interface subcommand that sets the IP address on the interface; each interface will have a different IP address.

Figure 2-7 Relationships Among Context-Setting Commands



Use Ctrl+z from any part of configuration mode (or use the **exit** command from global configuration mode) to exit configuration mode and return to privileged EXEC mode. The configuration mode **end** command also exits from any point in the configuration mode back to privileged EXEC mode. The **exit** commands from submodes or contexts of configuration mode back up one level toward global configuration mode.

Example Configuration Process

Example 2-1 illustrates how the console password is defined; provides banner, host name, prompt, and interface descriptions; and shows the finished configuration. The lines beginning with “!” are comment lines that highlight significant processes or command lines within the example. The **show running-config** command output also includes comment lines with just a “!” to make the output more readable—many comment lines in the examples in this book were added to explain the meaning of the configuration.

Example 2-1 Configuration Process Example

```
This Here's the Rootin-est Tootin-est Router in these here Parts!

User Access Verification

Password:
Yosemite>enable
Password:
Yosemite#configure terminal
Yosemite(config)#enable password lu
Yosemite(config)#line console 0
Yosemite(config-line)#login
Yosemite(config-line)#password cisco
Yosemite(config-line)#hostname Critter
Critter(config)#prompt Emma
Emma(config)#interface serial 1
Emma(config-if)#description this is the link to Albuquerque
Emma(config-if)#exit
Emma(config)#exit
Emma#
  Emma#show running-config
Building configuration...

Current configuration:
!
version 11.2
! Version of IOS on router, automatic command

no service udp-small-servers
no service tcp-small-servers
!
```

continues

Example 2-1 *Configuration Process Example (Continued)*

```
hostname Critter
prompt Emma
! Prompt overrides the use of the hostname as the prompt
!
enable password lu

! This sets the privilege exec mode password
!
no ip domain-lookup
! Ignores all names resolutions unless locally defined on the router.
!
ipx routing 0000.3089.b170
! Enables IPX rip routing
!
interface Serial0
ip address 137.11.12.2 255.255.255.0
ipx network 12
!
interface Serial1
description this is the link to Albuquerque
ip address 137.11.23.2 255.255.255.0
ipx network 23
!
interface TokenRing0
ip address 137.11.2.2 255.255.255.0
ipx network CAFE
ring-speed 16
!
router rip
network 137.11.0.0
!
no ip classless
!
!
!
banner motd ^C This Here's the Rootin-est Tootin-est Router in these here Parts! ^C
! Any text between the Ctl+C keystrokes is considered part of the banner, including
!the Enter key.!

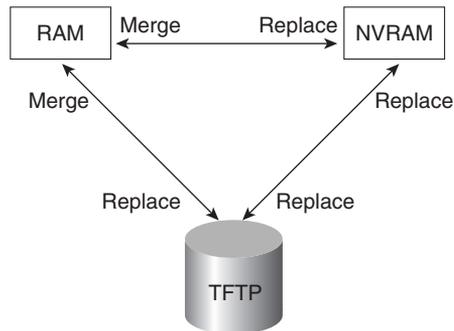
line con 0
password cisco
login
! login tells the router to supply a prompt; password defines what the user must
!type!
!
line aux 0
line vty 0 4
password cisco
Login
!
End
```

Managing Configuration Files

The CCNA exam requires that you be able to distinguish between the configuration file used at startup and the active configuration file. The startup configuration file is in NVRAM; the other file, which is in RAM, is the one the router uses during operation. The router copies the stored configuration file from NVRAM into RAM as part of the boot process. Exterior to the router, configuration files can be stored as ASCII text files anywhere using TFTP.

Cisco provides several methods of manipulating configuration files. CiscoWorks and other management products let you create configurations for one or many routers without logging on to those routers. NetSys Connectivity Tools actually check all the configuration files in your network, make suggestions for improvements, and uncover errors. The most basic method for manipulating configuration files and moving them into and out of a router, however, is by using a TFTP server. The **copy** command is used to move configuration files among RAM, NVRAM, and a TFTP server. The files can be copied between any pair, as Figure 2-8 illustrates.

Figure 2-8 Locations for Copying and Results from Copy Operations



The commands can be summarized as follows:

```
copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}
```

The first parameter is the “from” location; the next one is the “to” location. (Of course, choosing the same option for both parameters is not allowed.)

Confusion about what these commands actually do is pervasive. Any **copy** command option moving a file into NVRAM or a TFTP server replaces the existing file. Any **copy** command option moving the file into RAM, however, is effectively an *add* or *merge* operation. For example, only one host name *Siberia* configuration command is allowed. Therefore, a config file copied into RAM with **hostname Siberia** in it replaces the previous **hostname** command (if any). However, if the file being copied has the **access-list 1 permit host 1.1.1.1** command in it, and if an access list number 1 already exists in the RAM configuration file, then **access-list 1 permit host 1.1.1.1** is placed at the end of that existing access list (access lists are comprised of a list of configuration commands referencing the same list number or name). The

old entries in **access-list 1** are not deleted. This is because many **access-list 1** commands are allowed in the same access list. Effectively, any copy into RAM works just as if you typed the commands in the order listed in the config file.

So, why did Cisco not include a replace action, similar to the action used to copy to NVRAM or TFTP? Who knows? A replace action probably would require you to empty all routing tables, which might cause an outage. Possibly, this particular nuance is a result of some Cisco programmer who decided years ago to take the loaded gun out of users' hands. However, advanced users can accomplish the effect of a replace action by entering configuration mode and issuing commands until the running config is changed as desired. This requires that the user know whether each command will replace another that is like it in the RAM configuration file, or whether each command will simply be added to the configuration, as with an **access-list** command.

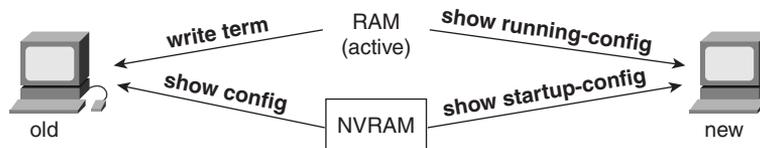
Two key commands can be used to erase the contents of NVRAM. The **write erase** command is the older command, and the **erase startup-config** command is the newer command. Both simply erase the contents of the NVRAM configuration file. Of course, if the router is reloaded at this point, there will be no initial configuration.

Viewing the Configuration and Old-Style Configuration Commands

Once upon a time, commands that were used to move configuration files among RAM, NVRAM, and TFTP did not use easy-to-recall parameters such as **startup-config** and **running-config**. In fact, most people could not remember the commands or got the different ones confused.

Figure 2-9 shows both the old and new commands used to view configurations.

Figure 2-9 Configuration *show* Commands



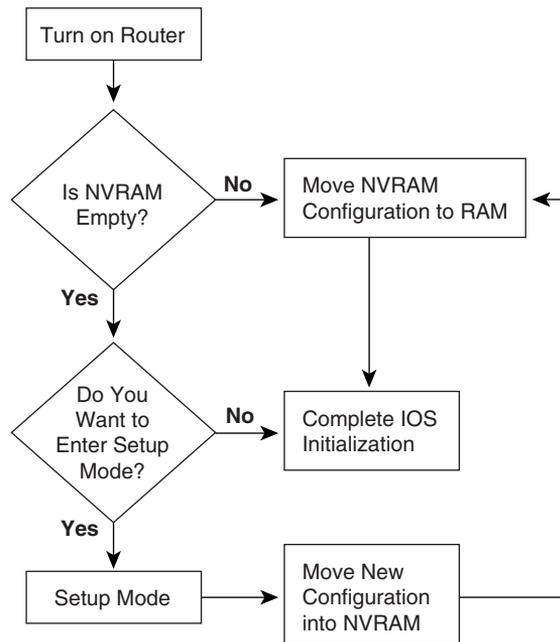
Initial Configuration (Setup Mode)

To pass the CCNA exam, you will need to be familiar with the differences between configuration mode and setup mode. Setup mode is a router configuration mode that prompts the user for basic configuration parameters. A Cisco router can be configured using the CLI in configuration mode without using setup mode. Some users like to use setup mode, however, particularly until they become more familiar with the CLI.

NOTE If you plan to work with Cisco routers much, you should become accustomed with the CLI configuration mode discussed earlier. Setup mode allows only basic configuration.

Setup mode is a topic covered on the CCNA exam, so regardless of whether you plan to use it, you must remember how it works. Figure 2-10 and Example 2-2 describe the process. Setup mode is most frequently used when the router comes up with no configuration in NVRAM; setup mode can be entered by using the **setup** command from privileged mode.

Figure 2-10 *Getting into Setup Mode*



Example 2-2 shows a screen capture of using setup mode after booting a router with no configuration in NVRAM.

Example 2-2 *Router Setup Configuration Mode*

```

Notice: NVRAM invalid, possibly due to write erase.
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use Ctrl+C to abort configuration dialog at any prompt.
Default settings are in square brackets '['].Would you
like to enter the initial configuration dialog? [yes]:
  
```

continues

Example 2-2 Router Setup Configuration Mode (Continued)

```

First, would you like to see the current interface summary? [yes]:
Any interface listed with OK? value "NO" does not have a valid configuration

Interface          IP-Address      OK? Method Status          Protocol
Serial0            unassigned     NO  unset  down            down
Serial1            unassigned     NO  unset  down            down

Ethernet0          unassigned     NO  unset  reset           down

Configuring global parameters:

  Enter host name [Router]: fred
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
  Enter enable secret: cisco
The enable password is used when there is no enable secret
and when using older software and some boot images.
  Enter enable password: cisco2

Enter virtual terminal password: cisco
Configure SNMP Network Management? [yes]: n
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]: n
Configuring interface parameters:
Configuring interface Serial0:
  Is this interface in use? [yes]:
Configure IP on this interface? [yes]:
IP address for this interface: 163.4.8.3
Number of bits in subnet field [0]: 0
Class B network is 163.4.0.0, 0 subnet bits; mask is /16

Configuring interface Serial1:
  Is this interface in use? [yes]: n
Configuring interface Ethernet0:
  Is this interface in use? [yes]: y

Configure IP on this interface? [yes]:
IP address for this interface: 163.5.8.3
Number of bits in subnet field [0]: 0
Class B network is 163.5.0.0, 0 subnet bits; mask is /16

The following configuration command script was created:

hostname fred
enable secret 5 $1$aMyk$eUxp9JmrPgK.vQ.nA5Tge.
enable password cisco
line vty 0 4
password cisco
no snmp-server
!

```

Example 2-2 Router Setup Configuration Mode (Continued)

```

ip routing
!
interface Serial0
ip address 163.4.8.3 255.255.0.0
!
interface Serial1
shutdown
no ip address
!
interface Ethernet0
ip address 163.5.8.3 255.255.0.0
!
end

Use this configuration? [yes/no]: y

Building configuration...[OK]
Use the enabled mode 'configure' command to modify this configuration.

Press ENTER to get started!

```

As Example 2-2 illustrates, you can use two methods to get into setup mode. First, if you are at the console and you power up the router, and if there is no configuration file in NVRAM, the router asks whether you want to enter the “initial configuration dialog.” Answering **y** or **yes** puts you in setup mode. Alternatively, the **setup** privileged EXEC command puts you in setup mode.

When you are finished with setup, you are asked whether you want to use this configuration. If you answer **yes**, the configuration you created is placed in RAM and NVRAM. This is the only operation in the IOS that changes both files to include the same contents based on a single action.

As of IOS version 12.0, the setup mode prompts no longer ask for the number of subnet bits. Instead, the subnet mask used is requested, which is probably a lot better for most people. Other fine details of the setup mode prompts have changed as well. Example 2-3 shows an example using IOS version 12.0 and is simply shown here for reference.

Example 2-3 Router Setup Configuration Mode—Version 12.0

```

--- System Configuration Dialog ---

Would you like to enter the initial 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 management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

```

continues

Example 2-3 Router Setup Configuration Mode—Version 12.0 (Continued)

```

Would you like to enter basic management setup? [yes/no]: no

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid configuration

Interface          IP-Address      OK? Method Status          Protocol
Serial0            unassigned     NO  unset  down            down
Serial1            unassigned     NO  unset  down            down
TokenRing0        unassigned     NO  unset  reset           down

Configuring global parameters:

  Enter host name [Router]: fred

  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: cisco

  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: cisco2

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: cisco
Configure SNMP Network Management? [yes]: n
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]:
Configure bridging? [no]:
Configuring interface parameters:
Do you want to configure Serial0 interface? [yes]: y
Configure IP on this interface? [yes]:
IP address for this interface: 163.4.8.3
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 163.4.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial1 interface? [yes]: n
Do you want to configure Ethernet0 interface? [yes]: y
Configure IP on this interface? [yes]:
IP address for this interface: 163.5.8.3
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 163.5.0.0, 24 subnet bits; mask is /24
The following configuration command script was created:

hostname fred
enable secret 5 $1$Qxix$Fi3buBVGTPeig9AIPgzxC.
enable password cisco2

```

Example 2-3 Router Setup Configuration Mode—Version 12.0 (Continued)

```

line vty 0 4
password cisco
no snmp-server
!
no deernet routing
no appletalk routing
no ipx routing
ip routing
no bridge 1
!
interface Serial0
ip address 163.4.8.3 255.255.255.0
no mop enabled
!
interface Serial1
shutdown
no ip address
!
interface Ethernet0
ip address 163.5.8.3 255.255.255.0
!
end

```

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]Use the enabled mode 'configure' command to modify this configuration._

Press ENTER to get started!

In the example, notice that an early prompt gives you the choice of performing a simpler configuration for basic management. For instance, you may have the configuration editing in a file on your PC, and all you need is enough IP working so that you can Telnet into the router to copy the configuration. Also note that you have an option to start over after answering the questions, which is very convenient for those of us who are poor typists.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is used by Cisco routers and switches to ascertain basic information about neighboring routers and switches. You can use this information to learn addresses quickly for easier Simple Network Management Protocol (SNMP) management, as well as learn the addresses of other devices when you do not have passwords to log in to the other device.

CDP is a Cisco proprietary protocol; to support forwarding CDP messages over an interface, that interface must support SNAP headers. Any LAN interface, HDLC, Frame Relay, and ATM all support CDP. The router or switch can discover Layer 3 addressing details of neighboring routers—without even configuring that Layer 3 protocol—because CDP is not dependent on any particular Layer 3 protocol.

CDP discovers several useful details from the neighboring device:

- **Device Identifier**—Typically the host name.
- **Address list**—Network and data link addresses.
- **Port Identifier**—Text that identifies the port, which is another name for an interface.
- **Capabilities list**—Information on what the device does—for instance, a router or switch.
- **Platform**—The model and OS level running in the device.

CDP is enabled in the configuration by default. The **no cdp run** global command disables CDP for the entire device, and the **cdp run** global command re-enables CDP. Likewise, the **no cdp enable** interface subcommand disables CDP just on that interface, and the **cdp enable** command switches back to the default state of CDP being enabled.

A variety of **show cdp** command options are available. Example 2-4 lists the output of the commands, with some commentary following.

Example 2-4 *show cdp Command Options*

```

Seville#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
fred           Ser 1          172      R           2500      Ser 1
Yosemite       Ser 0.2        161      R           2500      Ser 0.2

Seville#show cdp entry fred
-----
Device ID: fred
Entry address(es):
  IP address: 163.5.8.3
Platform: cisco 2500, Capabilities: Router
Interface: Serial1, Port ID (outgoing port): Serial1
Holdtime : 168 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright 1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp neighbor detail
-----
Device ID: fred
Entry address(es):

```

Example 2-4 *show cdp Command Options (Continued)*

```

    IP address: 163.5.8.3
    Platform: cisco 2500, Capabilities: Router
    Interface: Serial1, Port ID (outgoing port): Serial1
    Holdtime : 164 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright 1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye
-----
Device ID: Yosemite
Entry address(es):
  IP address: 10.1.5.252
  Novell address: 5.0200.bbbb.bbbb
Platform: cisco 2500, Capabilities: Router
Interface: Serial0.2, Port ID (outgoing port): Serial0.2
Holdtime : 146 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright 1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp interface
Ethernet0 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0.2 is up, line protocol is up
  Encapsulation FRAME-RELAY
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial1 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Seville#show cdp traffic
CDP counters :
  Packets output: 41, Input: 21
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0

```

The commands provide information about both the neighbors and the behavior of the CDP protocol itself. In the **show cdp entry fred** command in Example 2-4, all the details learned by CDP are shown and highlighted. To know that fred is the device identifier of a neighbor, the **show cdp neighbor** command can be used to summarize the information about each neighbor. **Show cdp neighbor detail** lists the detail of all neighbors, in the same format as **show cdp entry**. In addition, **show cdp traffic** lists the overhead that CDP introduces to perform its functions.

Managing IOS Images

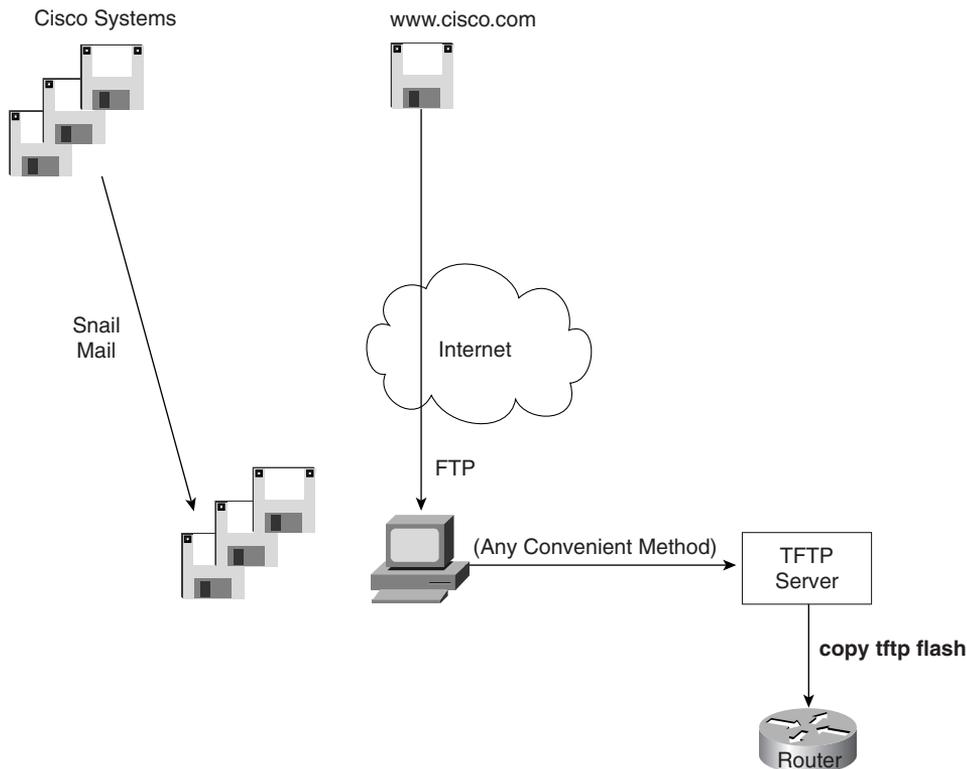
One common task that CCNAs run into is migrating to a new level of IOS. *IOS image* is simply a term referring to the file containing the IOS. Managing image files entails getting new IOS images from Cisco; backing up the currently used, older version from your routers; updating your routers with the new image; and testing. Also included in IOS image management is how to tell a router to use a particular IOS the next time it boots.

IOS files are typically stored in Flash memory. Flash memory is rewritable, permanent storage, which is ideal for storing files that need to be retained when the router loses power. Also, because there are no moving parts, there is a smaller chance of failure as compared with disk drives, which provides better availability.

Upgrading an IOS Image into Flash Memory

As Figure 2-11 illustrates, to upgrade an IOS image into Flash memory, you first must obtain the IOS image from Cisco. Then, you must place the IOS image into the default directory of a TFTP server. Finally, you must issue the **copy** command from the router, copying the file into Flash memory.

Figure 2-11 Complete IOS Upgrade Process



During this process of copying the IOS image into Flash memory, the router will need to discover several important facts:

- 1 What is the IP address or host name of the TFTP server?
- 2 What is the name of the file?
- 3 Is space available for this file in Flash memory?
- 4 If not, will you let the router erase the old files?

The router will prompt you for answers, as necessary. Afterward, the router erases Flash memory as needed, copies the file, and then verifies that the checksum for the file shows that no errors occurred in transmission. The **show flash** command then can be used to verify the contents of Flash memory (see Example 2-6). (The **show flash** output can vary between router families.) Before the new IOS is used, however, the router must be reloaded.

Example 2-6 *Verifying Flash Memory Contents with the **show flash** Command*

```
fred#show flash

System flash directory:
File Length Name/status
  1 6181132 c4500-d-mz.120-5.bin
[4181196 bytes used, 4207412 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

In some cases, Flash memory could be in read-only mode. That is the case when a router loads only part of the IOS into RAM, to conserve RAM. Other parts of the IOS file are kept in Flash memory (Flash memory access time is much slower than RAM). In this case, if Flash memory must be erased to make room for a new image, the IOS could not continue to run. So, if the router is running from a portion of the IOS in Flash memory, the router first must be booted using the IOS in ROM. Then the Flash memory will be in read/write mode, and the erase and copy processes can be accomplished. The **copy tftp flash** command in later releases of the IOS actually performs the entire process for you. In earlier releases, you had to boot the router from ROM and then issue the **copy tftp flash** command.

Choosing Which IOS Image to Load

The CCNA exam requires you to be proficient in configuring a router to load an IOS image from many sources. Two methods are used by a router to determine where it tries to obtain an IOS image to execute. The first is based on the value of the *configuration register*, which is a 16-bit software register in Cisco's more recently developed routers. (Some older routers had a hardware configuration register, with jumpers on the processor card, to set bits to a value of 0 or 1.) The second method used to determine where the router tries to obtain an IOS image is through the use of the **boot system** configuration command. Figure 2-12 shows an example binary breakdown of the default value for the configuration register.

Figure 2-12 Binary Version of Configuration Register, Value Hex 2102

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0

The *boot field* is the name of the low-order 4 bits of the configuration register. This field can be considered a 4-bit value, represented as a single hexadecimal digit. Cisco represents hexadecimal values by preceding the hex digit(s) with *0x*—for example, *0xA* would mean a single hex digit *A*.

The router chooses the IOS image to load based on the boot field and the *boot system* commands in the configuration. Table 2-6 summarizes the use of the configuration register and the **boot system** command at initialization time. (If the files referred to in the boot system commands are not found, then the router will never complete the boot process. The password recovery process must be used to change the config register to *0x2142* so that the NVRAM configuration is ignored and the **boot** commands can be repaired to point to a valid IOS file name. Refer to the section “Password Recovery,” later in this chapter, for more details.)

Table 2-6 *boot system* Command

Value of Boot Field	Boot System Commands	Result
0x0	Ignored if present	ROM monitor mode, a low-level problem determination mode, is entered.
0x1	Ignored if present	IOS from ROM is loaded.
0x2-0xF	No boot command	The first IOS file in flash is loaded; if that fails, the router broadcasts looking for an IOS on a TFTP server. If that fails, IOS from ROM is loaded.
0x2-0xF	boot system ROM	IOS from ROM is loaded.
0x2-0xF	boot system flash	The first file from Flash memory is loaded.
0x2-0xF	boot system flash <i>filename</i>	IOS with name <i>filename</i> is loaded from Flash memory.
0x2-0xF	boot system tftp <i>filename</i> 10.1.1.1	IOS with name <i>filename</i> is loaded from TFTP server.
0x2-0xF	Multiple boot system commands, any variety	An attempt occurs to load IOS based on the first boot command in configuration. If that fails, the second boot command is used, and so on, until one is successful.

Password Recovery

Several additional concepts related to loading the IOS must be understood before password recovery can be performed. First, software called the *ROM monitor* (rommon) is held in ROM on all routers and actually provides the code that is first used to boot each router. rommon has a rudimentary command structure that is used as part of the password recovery process. A limited-function IOS is also held in either ROM or in additional Flash memory called *bootflash*; in either case, the IOS in bootflash or ROM is used mainly in cases where the IOS in flash is not available for some reason. Finally, bit 6 of the configuration register set to binary 1 means that the router should ignore the NVRAM configuration when booting.

Password recovery revolves around the process of getting the router to boot while ignoring the NVRAM configuration file. The router will be up, but with a default configuration; this enables a console user to log in, enter privileged mode, and change any encrypted passwords or view any unencrypted passwords. To cause the router to ignore NVRAM at boot time, the configuration register must be changed. To do that, you must be in privileged mode—and if you were already there, you could reset any encrypted passwords or view any unencrypted ones. It seems to be a vicious circle.

The two keys to password recovery are knowing that rommon enables you to reset the configuration register and that a console user can get into rommon mode by pressing the Break key during the first 60 seconds after power-on of the router. Knowing how to reset the config register enables you to boot the router (ignoring NVRAM), allowing the console user to see or change the unencrypted or encrypted passwords, respectively.

The process is slightly different for different models of routers, although the concepts are identical. Table 2-7 outlines the process for each type of router.

Table 2-7 *Password Recovery*

Step	Function	How to Do This for 1600, 2600, 3600, 4500, 7200, 7500	How to Do This for 2000, 2500, 3000, 4000, 7000
1	Turn router off and then back on again.	Use the power switch.	Same as other routers.
2	Press the Break key within the first 60 seconds.	Find the Break key on your console devices keyboard.	Same as other routers.
3	Change the configuration register so that bit 6 is 1.	Use the rommon command confreg , and answer the prompts.	Use the rommon command o/r 0x2142 .
4	Cause the router to load an IOS.	Use the rommon reload command or, if unavailable, power off and on.	Use rommon command initialize .
5	Avoid using setup mode, which will be prompted for at console.	Just say no.	Same as other routers.

Table 2-7 Password Recovery (Continued)

Step	Function	How to Do This for 1600, 2600, 3600, 4500, 7200, 7500	How to Do This for 2000, 2500, 3000, 4000, 7000
6	Enter privileged mode at console.	Press Enter and use enable command (no password required).	Same as other routers.
7	View startup config to see unencrypted passwords.	Use exec command show startup-config .	Same as other routers.
8	Use appropriate config commands to reset encrypted commands.	For example, use enable secret xyz123 command to set enable secret password.	Same as other routers.
9	Change config register back to original value.	Use config command Config-reg 0x2102 .	Same as other routers.
10	Reload the router after saving the configuration.	Use the copy running-config startup-config and reload commands.	Same as other routers.

A few nuances need further explanation. First, the **confreg** rommon command prompts you with questions that correspond to the functions of the bits in the configuration register. When the prompt asks, “Ignore system config info[y/n]?”, it is asking you about bit 6. Entering **yes** sets the bit to 1. The rest of the questions can be defaulted. The last **confreg** question asks, “Change boot characteristics[y/n]?”, which asks whether you want to change the boot field of the config register. You don’t really need to change it, but the published password recovery algorithm lists that step, which is the only reason that it is mentioned here. Just changing bit 6 to 1 is enough to get the router booted and you into privileged mode to find or change the passwords.

The original configuration is lost through this process, but you can overcome that. When you save the configuration in Step 10, you are overwriting the config in NVRAM. There was no configuration in the running config except default and the few things you configured. So, before Step 8, you might want to perform a **copy startup-config running-config** command and then proceed with the process.

Foundation Summary

The Foundation Summary is a collection of tables and figures that provide a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final preparation before the exam, these tables and figures will be a convenient way to review the day before the exam.

Table 2-8 reviews the different types of passwords and the configuration for each type.

Table 2-8 *CLI Password Configuration*

Access from . . .	Password Type	Configuration
Console	Console password	line console 0 login password faith
Auxiliary	Auxiliary password	line aux 0 login password hope
Telnet	vty password	line vty 0 4 login password love

Table 2-9 lists the commands used to manipulate previously typed commands.

Table 2-9 *Key Sequences for Command Edit and Recall*

Keyboard Command	What the User Gets
Up-arrow or Ctrl+p	This calls up the most recently used command. If pressed again, the next most recent command appears, until the history buffer is exhausted. (The p stands for <i>previous</i> .)
Down-arrow or Ctrl+n	If you have gone too far back into the history buffer, these keys will go forward, in order, to the more recently typed commands. (The n stands for <i>next</i> .)
Left-arrow or Ctrl+b	This moves the cursor backward in the currently displayed command without deleting characters. (The b stands for <i>back</i> .)
Right-arrow or Ctrl+f	This moves the cursor forward in the currently displayed command without deleting characters. (The f stands for <i>forward</i> .)

Table 2-9 *Key Sequences for Command Edit and Recall (Continued)*

Keyboard Command	What the User Gets
Backspace	This moves the cursor backward in the currently displayed command, deleting characters.
Ctrl+a	This moves the cursor directly to the first character of the currently displayed command.
Ctrl+e	This moves the cursor directly to the end of the currently displayed command.
Esc+b	This moves the cursor back one word in the currently displayed command.
Esc+f	This moves the cursor forward one word in the currently displayed command.
Ctrl+r	This creates a new command prompt, followed by all the characters typed since the previous command prompt. This is particularly useful if system messages confuse the screen and it is unclear what the user has typed so far.

Table 2-10 summarizes the use of the configuration register and the **boot system** command at initialization.

Table 2-10 *boot system Command*

Value of Boot Field	Boot System Commands	Result
0x0	Ignored if present	ROM monitor mode, a low-level problem determination mode, is entered.
0x1	Ignored if present	IOS from ROM is loaded.
0x2-0xF	No boot command	The first IOS file in flash is loaded; if that fails, IOS from ROM is loaded. If that fails, the router broadcasts looking for an IOS on a TFTP server. If that fails, the IOS in ROM is loaded.
0x2-0xF	boot system ROM	IOS from ROM is loaded.
0x2-0xF	boot system flash	The first file from Flash memory is loaded.
0x2-0xF	boot system flash <i>filename</i>	IOS with name <i>filename</i> is loaded from Flash memory.
0x2-0xF	boot system tftp 10.1.1.1 <i>filename</i>	IOS with name <i>filename</i> is loaded from the TFTP server.
0x2-0xF	Multiple boot system commands, any variety	An attempt occurs to load IOS based on the first boot command in configuration. If that fails, the second boot command is used, and so on, until one is successful.

Figure 2-13 summarizes the use of memory in Cisco routers.

Figure 2-13 *Cisco Router Memory Types*

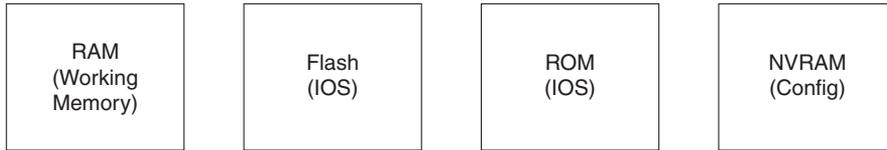
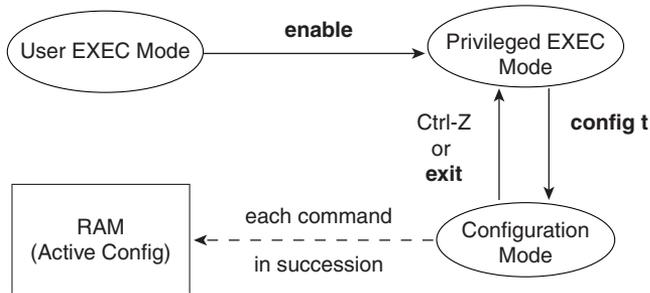


Figure 2-14 illustrates the relationships among configuration mode, user EXEC mode, and privileged EXEC mode.

Figure 2-14 *CLI Configuration Mode Versus EXEC Modes*



The **copy** command is used to move configuration files among RAM, NVRAM, and a TFTP server. The files can be copied between any pair, as Figure 2-15 illustrates.

Figure 2-15 *Locations for Copying and Results from Copy Operations*

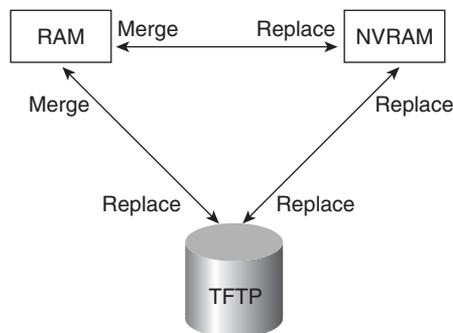


Figure 2-16 shows both the old and new commands used to view configurations.

Figure 2-16 Configuration *show* Commands

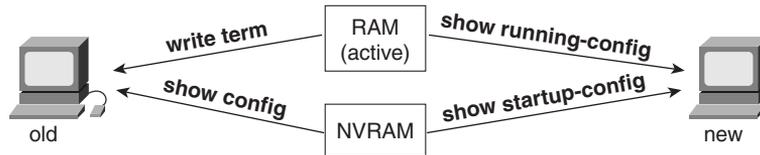
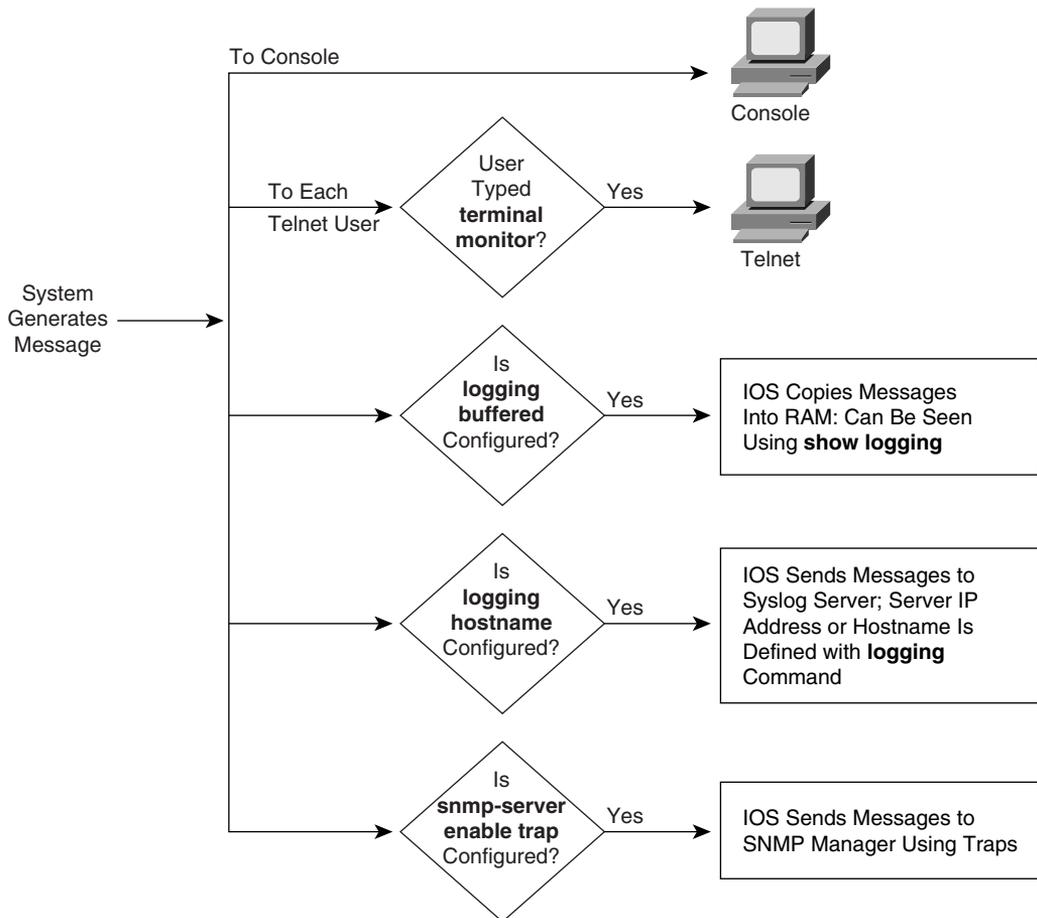


Figure 2-17 summarizes the flow of syslog messages, including debug messages.

Figure 2-17 Syslog Message Flows



Q&A

As mentioned in Chapter 1, the questions and scenarios in this book are more difficult than what you should experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam; however, they are designed to make sure that you know the answer. Rather than allowing you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject. Questions from the “Do I Know This Already?” quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter’s topic areas. Hopefully, these questions will help limit the number of exam questions on which you narrow your choices to two options and then guess. Make sure to use the CD and take the simulated exams.

The answers to these questions can be found in Appendix A, on page 703.

- 1 What are the two names for the router’s mode of operation that, when accessed, enables you to issue commands that could be disruptive to router operations?
- 2 What are three methods of logging on to a router?
- 3 What is the name of the user interface mode of operation used when you cannot issue disruptive commands?
- 4 Can the auxiliary port be used for anything besides remote modem user access to a router? If so, what other purpose can it serve?
- 5 How many console ports can be installed on a Cisco 7500 router?
- 6 What command would you use to receive command help if you knew that a **show** command option begins with a **c**, but you cannot recall the option?
- 7 While you are logged in to a router, you issue the command **copy ?** and get a response of “Unknown command, computer name, or host.” Offer an explanation as to why this error message appears.
- 8 Is the number of retrievable commands based on the number of characters in each command, or is it simply a number of commands, regardless of their size?
- 9 How can you retrieve a previously used command? (Name two ways.)
- 10 After typing **show ip route**, which is the only command you typed since logging in to the router, you now want to issue the **show ip arp** command. What steps would you take to execute this command by using command recall keystrokes?
- 11 After typing **show ip route 128.1.1.0**, you now want to issue the command **show ip route 128.1.4.0**. What steps would you take to do so, using command recall and command editing keystrokes?

-
- 12 What configuration command causes the router to require a password from a user at the console? What configuration mode context must you be in—that is, what command(s) must be typed before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.
 - 13 What configuration command is used to tell the router the password that is required at the console? What configuration mode context must you be in—that is, what command(s) must you type before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.
 - 14 What are the primary purposes of Flash memory in a Cisco router?
 - 15 What is the intended purpose of NVRAM memory in a Cisco router?
 - 16 What does the NV stand for in NVRAM?
 - 17 What is the intended purpose of RAM in a Cisco router?
 - 18 What is the main purpose of ROM in a Cisco router?
 - 19 What configuration command would be needed to cause a router to use an IOS image named `c2500-j-1.112-14.bin` on TFTP server `128.1.1.1` when the router is reloaded? If you forgot the first parameter of this command, what steps must you take to learn the correct parameters and add the command to the configuration? (Assume that you are not logged in to the router when you start.)
 - 20 What command sets the password that would be required after typing the **enable** command? Is that password encrypted by default?
 - 21 To have the correct syntax, what must you add to the following configuration command:

```
banner This is Ivan Denisovich's Gorno Router - Do Not Use
```
 - 22 Name two commands that affect the text used as the command prompt.
 - 23 When using setup mode, you are prompted at the end of the process as to whether you want to use the configuration parameters you just typed in. Which type of memory is this configuration stored into if you type yes?
 - 24 What two methods could a router administrator use to cause a router to load the IOS stored in ROM?
 - 25 What could a router administrator do to cause a router to load file `xyz123.bin` from TFTP server `128.1.1.1` upon the next reload? Is there more than one way to accomplish this?
 - 26 What is the process used to update the contents of Flash memory so that a new IOS in a file called `c4500-d-mz.120-5.bin` on TFTP server `128.1.1.1` is copied into Flash memory?
 - 27 Name three possible problems that could prevent the command **boot system tftp c2500-j-1.112-14.bin 128.1.1.1** from succeeding.

- 28 Two different IOS files are in a router's Flash memory: one called c2500-j-1.111-3.bin and one called c2500-j-1.112-14.bin. Which one does the router use when it boots up? How could you force the other IOS file to be used? Without looking at the router configuration, what command could be used to discover which file was used for the latest boot of the router?
- 29 What does CDP stand for?
- 30 On what type of interfaces is CDP enabled by default? (Assume IOS versions 11.0 and later.)
- 31 What command can be used to provide as much detailed information as possible with CDP?
- 32 Is the password required at the console the same one that is required when Telnet is used to access a router?
- 33 How could a router administrator disable CDP?
- 34 Which IP routing protocols could be enabled using setup?
- 35 Name two commands used to view the configuration to be used at the next reload of the router. Which one is a more recent addition to the IOS?
- 36 Name two commands used to view the configuration that is currently used in a router. Which one is a more recent addition to the IOS?
- 37 True or False: The **copy startup-config running-config** command always changes the currently used configuration for this router to exactly match what is in the startup configuration file. Explain.

Scenarios

Scenario 2-1

Compare the following output in Example 2-7 and Example 2-8. Example 2-7 was gathered at 11:00 a.m., 30 minutes earlier than Example 2-8. What can you definitively say happened to this router during the intervening half hour?

Example 2-7 *11:00 a.m. show running-config*

```
hostname Gorno
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.1 255.255.255.0
!
interface Serial1
 ip address 134.141.13.1 255.255.255.0
!
interface Ethernet0
 ip address 134.141.1.1 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
```

Example 2-8 *11:30 a.m. show running-config*

```
hostname SouthernSiberia
prompt Gorno
!
enable secret $8df003j56ske92
enable password cisco
!
interface Serial0
 ip address 134.141.12.1 255.255.255.0
!
interface Serial1
 ip address 134.141.13.1 255.255.255.0
!
interface Ethernet0
 ip address 134.141.1.1 255.255.255.0
 no cdp enable
```

continues

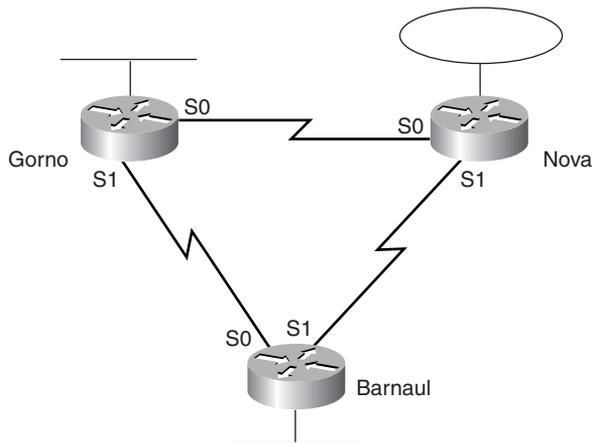
Example 2-8 11:30 a.m. *show running-config* (Continued)

```
!
router rip
 network 134.141.0.0
!
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 Login
```

Questions on Scenario 2-1

- 1 During the process of changing the configuration in Scenario 2-1, the command prompt temporarily was **SouthernSiberia(config)#**. What configuration commands, and in what order, could have changed the configuration as shown and allowed the prompt to temporarily be **SouthernSiberia(config)#**?
- 2 Assuming that Figure 2-18 is complete, what effect does the **no cdp enable** command have?

Figure 2-18 Siberian Enterprises' Sample Network



- 3 What effect would the **no enable password cisco** command have at this point?

Scenario 2-2

Example 2-9 shows that the **running-config** command was executed on the Nova router.

Example 2-9 Configuration of Router Nova

```

hostname Nova
banner # This is the router in Nova Sibiersk; Dress warmly before entering! #
!
boot system tftp c2500-js-113.bin 134.141.88.3
boot system flash c2500-j-1.111-9.bin
boot system rom
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.2 255.255.255.0
!
interface Serial1
 ip address 134.141.23.2 255.255.255.0
!
interface TokenRing0
 ip address 134.141.2.2 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login

```

Questions on Scenario 2-2

- 1 If this is all the information that you have, what IOS do you expect will be loaded when the user reloads Nova?
- 2 Examine the following command output in Example 2-10, taken immediately before the user is going to type the **reload** command. What IOS do you expect will be loaded?

Example 2-10 *show ip route* on Nova

```

Nova#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

```

continues

Example 2-10 *show ip route on Nova (Continued)*

```

134.141.0.0/24 is subnetted, 6 subnets
C    134.141.2.0 is directly connected, TokenRing0
R    134.141.3.0 [120/1] via 134.141.23.3, 00:00:15, Serial1
R    134.141.1.0 [120/1] via 134.141.12.1, 00:00:20, Serial0
C    134.141.12.0 is directly connected, Serial0
R    134.141.13.0 [120/1] via 134.141.12.1, 00:00:20, Serial0
      [120/1] via 134.141.23.3, 00:00:15, Serial1
C    134.141.23.0 is directly connected, Serial1

```

- 3 Now examine the following **show flash** command in Example 2-11, which was issued immediately after the **show ip route** command in Example 2-10, but before the user issued the **reload** command. What IOS do you think would be loaded in this case?

Example 2-11 *show flash on Router Nova*

```

Nova#show flash
4096K bytes of flash memory sized on embedded flash.
File name/status
 0 c2500-j-1.111-3.bin
[682680/4194304 bytes free/total]

```

- 4 Now examine the configuration in Example 2-12. Assume that there is now a route to 134.141.88.0 and that the file c2500-j-1.111-9.bin is an IOS image in Flash memory. What IOS do you expect will be loaded now?

Example 2-12 *show running-config on Router Nova*

```

hostname Nova
banner # This is the router in Nova Sibiersk; Dress warmly before entering! #
!
boot system tftp c2500-js-113.bin 134.141.88.3
boot system flash c2500-j-1.111-9.bin
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.2 255.255.255.0
!
interface Serial1
 ip address 134.141.23.2 255.255.255.0
!
interface Ethernet0
 ip address 134.141.2.2 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login

```

Example 2-12 *show running-config* on Router Nova (Continued)

```
line aux 0
line vty 0 4
  password cisco
  login
!
config-register 0x2101
```

Answers to Scenarios

Scenario 2-1 Answers

In Scenario 2-1, the following commands were added to the configuration:

- **enable secret** as a global command.
- **prompt** as a global command.
- **no cdp enable** as an Ethernet0 subcommand.
- The **hostname** command also was changed.

The scenario questions' answers are as follows:

- 1 If the host name was changed to *SouthSiberia* first and the **prompt** command was added next, the prompt would have temporarily been *SouthSiberia*. Configuration commands are added to the RAM configuration file immediately and are used. In this case, when the **prompt** command was added, it caused the router to use “Gorno,” not the then-current host name “SouthernSiberia,” as the prompt.
- 2 No practical effect takes place. Because no other Cisco CDP-enabled devices are on that Ethernet, CDP messages from Gorno are useless. So, the only effect is to lessen the overhead on that Ethernet in a very small way.
- 3 No effect takes place other than cleaning up the configuration file. The **enable password** is not used if an **enable secret** is configured.

Scenario 2-2 Answers

The answers to the questions in Scenario 2-2 are as follows:

- 1 The first boot system statement would be used: **boot system tftp c2500-js-113.bin 134.141.88.3**.
- 2 The **boot system flash** command would be used. The TFTP boot would presumably fail because there is not currently a route to the subnet of which the TFTP server is a part. It is reasonable to assume that a route would not be learned 2 minutes later when the router had reloaded. So, the next **boot system** command (**flash**) would be used.
- 3 The **boot system ROM** command would be used. Because there is no file in Flash called *c2500-j-1.111-9.bin*, the boot from Flash memory would fail as well, leaving only one **boot** command.
- 4 The IOS from ROM would be loaded due to the configuration register. If the configuration register boot field is set to 0x1, **boot system** commands are ignored. So, having a route to the 134.141.88.0/24 subnet and having *c2500-j-1.111-9.bin* in Flash memory does not help.

