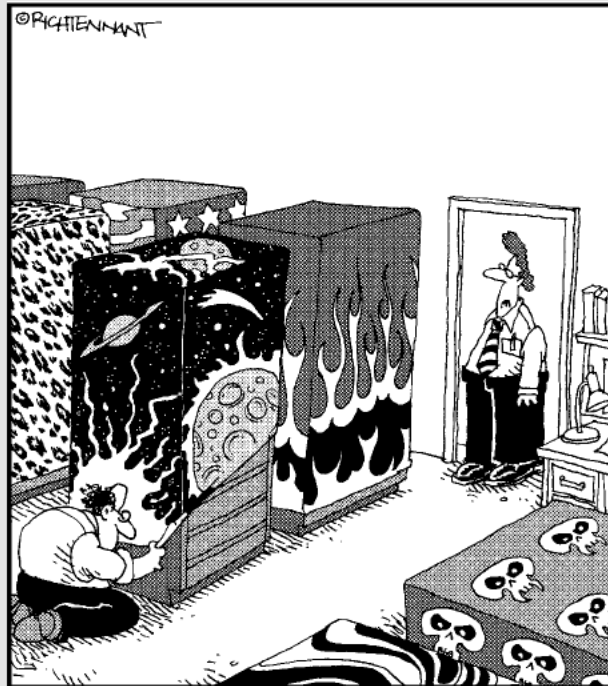


Book IV

Routing with Cisco Routers

The 5th Wave

By Rich Tennant



"I didn't know they made skins for mainframes."

Contents at a Glance

Chapter 1: Introducing Layer 3 Routers	505
Layer 3 — Network Layer Review	505
Purpose of a Layer 3 Router	508
Basic Router Functions	511
Chapter 2: Managing a Router Using Cisco IOS	517
Best Practices for Using Cisco Routers	517
Connecting to a Cisco Router	519
Cisco Router Startup Process	525
Configuring a Cisco Router	528
Managing Cisco Router Authentication	554
Chapter 3: Network Routing	567
Introducing Network Routes	567
Routing Protocols	571
Routed Protocols	572
Routing Decision Criteria	572
Routing Methods	576
Configuring Routing Protocols	582
Chapter 4: Routing Information Protocol (RIP)	587
Introducing Routing Information Protocol (RIP)	588
RIPv1	593
RIPv2	595
RIPng	597
Configuring RIP	598
Verifying RIP	601
Chapter 5: Enhanced Interior Gateway Routing Protocol (EIGRP)	607
IGRP — The Foundation of EIGRP	608
EIGRP Benefits	608
Characteristics of EIGRP	609
EIGRP Operation	610
Configuring EIGRP	615
Verifying and Monitoring EIGRP Operation	617
Troubleshooting EIGRP	620
Chapter 6: Open Shortest Path First (OSPF) Protocol	625
Introducing Open Shortest Path First (OSPF)	625
OSPF Routing Hierarchy	628
Configuring OSPF	634
Verifying and Monitoring OSPF Operation	639
Troubleshooting OSPF	641

Chapter 1: Introducing Layer 3 Routers

Exam Objectives

- ✓ Describing network OSI Layer 3 and how it relates to Layer 3 routers
- ✓ Describing the purpose of a Layer 3 router
- ✓ Differentiating a Layer 3 router from a Layer 2 switch
- ✓ Describing basic Layer 3 router functions

Recall that Layer 3 in the Open Systems Interconnection (OSI) and TCP/IP network models is the network layer. The main function of network layer devices and protocols is to *route data packets* between hosts. Routing means choosing the best route to send packets between two hosts. The hosts can be next to each other or across the globe. Whereas the data link layer (Layer 2) routes data frames locally between two devices in the same LAN, the network layer (Layer 3) routes data packets between two devices in separate LANs. In other words, the data link layer sends data *within* the same LAN, whereas the network layer routes data *between* LANs.

Layer 3 — Network Layer Review

The network layer assigns logical addresses (IP addresses) to all devices in the network to be able to identify each source host, each destination host, as well as each network through which packets need to be routed. Logical addresses are assigned at the network protocol level as opposed to physical addresses, which are assigned on a physical device, such as a network card.

The network layer does the following:

- ◆ Receives each data segment from the transport layer on the sending host
- ◆ Wraps up the segment in a *data packet* along with global routing data (source and destination logical IP addresses)
- ◆ Sends the data packet down to the data link layer to prepare it to be sent over the LAN connection

The data link layer does the following:

- ◆ Receives each packet from the network layer on the sending host
- ◆ Wraps up the packet in a *data frame* along with local routing data (source and destination physical MAC addresses)
- ◆ Sends the data frame down to the physical layer to code an electrical or optical signal

The physical layer transmits the data frame over a wire or over the air in wireless networks.

On the receiving host, the data link layer does the following:

- ◆ Unwraps the data frame received
- ◆ Extracts the packet out of the data frame
- ◆ Sends the packet up to the network layer

On the receiving host, the network layer does the following:

- ◆ Unwraps the data packet received
- ◆ Extracts the data segment from the data packet
- ◆ Sends the data segment up to the transport layer

The Internet Protocol (IP) is the TCP/IP protocol that operates at Layer 3 to handle network functions. Hence, whenever you consider Layer 3 in TCP/IP, you need to think about IP and logical IP addresses. Also, keep in mind that Layer 3, the network layer, is concerned with routing data between LANs interconnected in global networks. The mission of the network layer is to handle the routing of data packets between two devices connected in different local-area networks (LANs) that are interconnected by global wide-area networks (WANs). The network layer does the following:

- ◆ Routes data packets between LANs
- ◆ Uses the Internet Protocol (IP)
- ◆ Identifies hosts using logical IP addresses

Logical addressing at the network layer is *hierarchical*:

- ◆ A limited range of IP addresses identifies a few global networks.
- ◆ Global networks interconnect large- and medium-size networks that use another specific range of IP addresses.
- ◆ Large- and medium-size networks interconnect smaller networks that use yet another specific range of IP addresses.



Hierarchical logical addressing involves assigning a network layer address to each network, network device, and host device.

The hierarchical IP addressing scheme facilitates routing. This is very similar to the hierarchy of real street addresses, which are composed of information such as street number, street name, neighborhood name (for larger cities), city name, state name, and country name.

The advantage of using hierarchical street addresses is that you do not need to know exactly where your destination is. All you need to know is the location of the nearest mailbox. The post office routes your package to the destination from there. Suppose you are in Australia and you need to send something to Japan. The Australian post office employees don't need to know where the destination city and street are located *within* Japan. All they need to know is that they must send your package to Japan. The Japanese post office will route your packet to the Japanese destination when the packet reaches Japan. This is the power of hierarchical addressing: Anyone can send anywhere without knowing exactly where the destination is.



Routing at the network layer in computer networks works similarly to courier services:

- ◆ A few extremely large global networks (think countries) interconnect other large networks.
- ◆ Large-sized networks (think states or provinces) interconnect medium-sized networks (think cities).
- ◆ Medium-sized networks interconnect smaller networks (think neighborhoods).
- ◆ Small-size networks interconnect mini-networks (think streets).
- ◆ Finally, there are computer hosts within each of the mini-networks (think street numbers).

Computer hosts embed the sender and receiver IP address in each data packet they send to another computer:

- ◆ If the receiving computer host is in the same network as the sender (living on the same street), the packet is simply routed locally at the data link layer using the physical address (the MAC address).
- ◆ If the receiving computer host is not in the same network as the sender, the packet is handed off to a *gateway* to be routed outside the network.

A gateway is a *router* that links a network to another network.

- ◆ The gateway looks at the logical address (IP address) of the receiving computer host and determines in which network it is located (on which street):
 - If the gateway knows about the network of the receiving computer host (it knows the street; it's in the same city), it sends the data packet to that network.
 - If the gateway does not know the destination network, it hands the packet to the higher-up gateway.

Layer 3 routers relate to networks like courier services routing and distribution centers. Layer 3 routers inspect the destination IP address of each data packet they receive to determine where to send that packet:

- ◆ If they know the destination network, they send the packet on a port that links to the destination network.
- ◆ Otherwise, they hand off the packet to the next higher-up router.

Routers remember the networks they are connected to. This helps them route data packets to the ports that reach those networks. Whenever a router receives a packet bound for a network it has never “heard about,” the router sends the packet to its own gateway, the outbound router that reaches out to other unknown networks.

Purpose of a Layer 3 Router

A Layer 2 switch is a network device that creates one collision domain per port and forwards data frames only on the outbound port that reaches the destination of the frame.



Considering the post office analogy, a Layer 2 switch is like a postman that delivers the package on a given street or in a given neighborhood. Routers are like the postal routing and distribution centers that group (route) the packets by neighborhood and street and hand the packets off to the postman (the Layer 2 switch) to deliver them to their local destinations.

Layer 2 switches are typically faster than routers because they do not need to look at the network layer (Layer 3) IP packet header. They only inspect the data-link (Layer 2) frame to look at the source and destination MAC address of the frame. This is why they are called Layer 2 switches: They only operate on the data-link (Layer 2) frame.

Figure 1-1 illustrates how data packets are processed by an intermediary node (a router) on their journey between two hosts in different LANs. The router needs to inspect the packet that it extracts from the data-link frame.

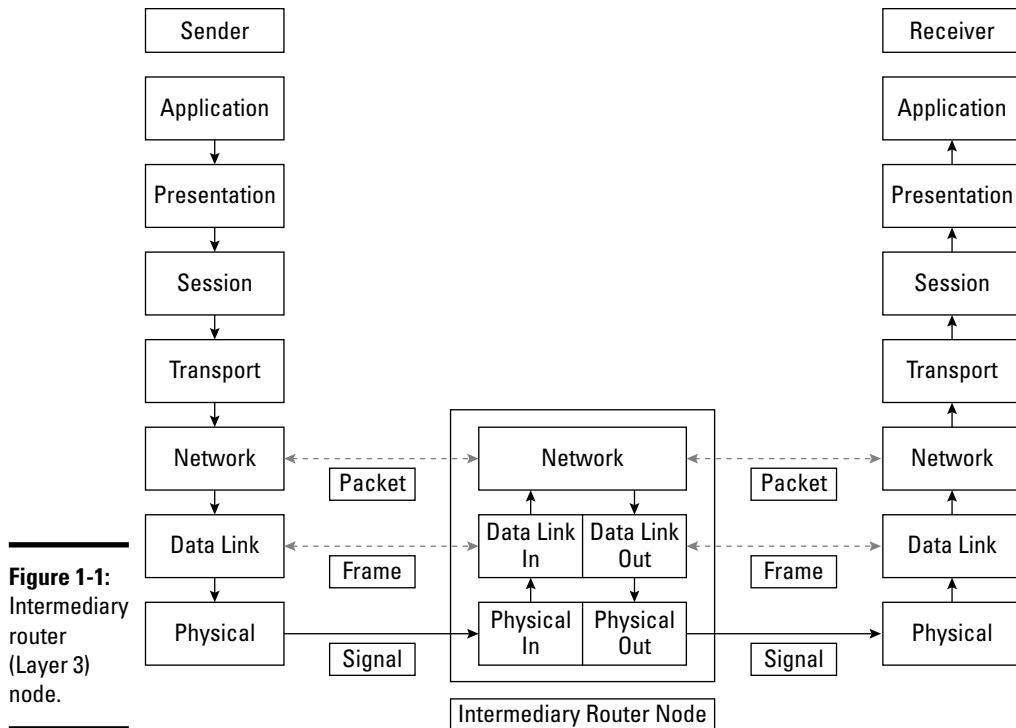
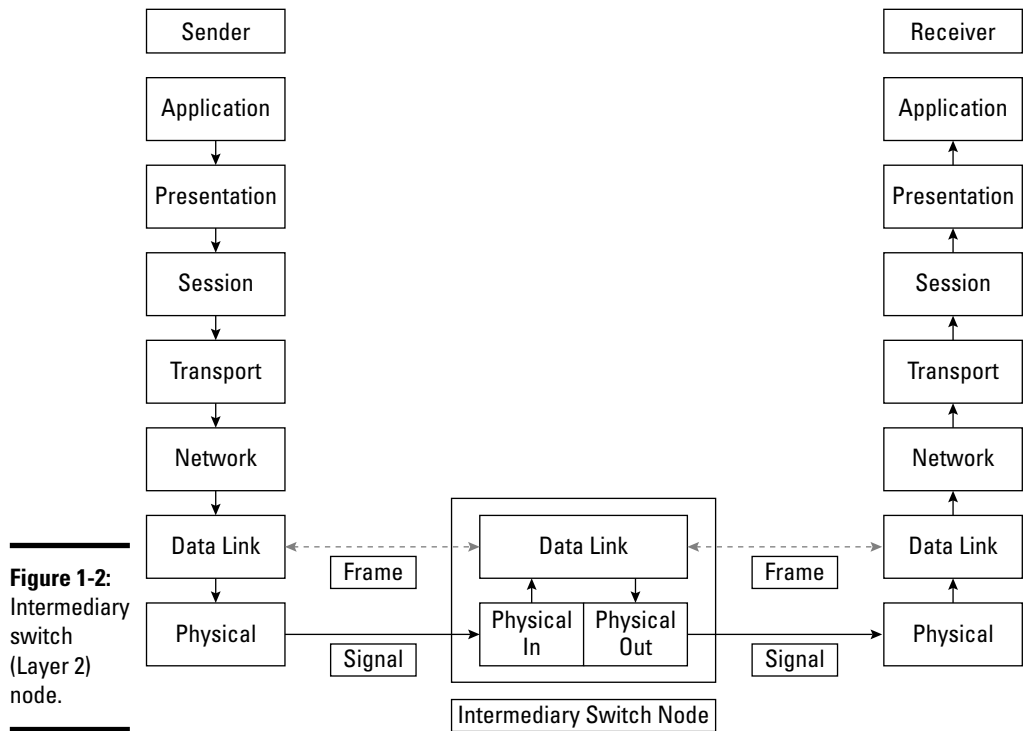


Figure 1-1:
Intermediary
router
(Layer 3)
node.

By contrast, a switch only needs to look at the data frame, as shown in Figure 1-2. Switches do not analyze the IP packet that is encapsulated in the Layer 2 data frame.

The purpose of a router is to route data packets between networks:

- ◆ The router inspects the IP header of each data packet that passes through it.
- ◆ The router extracts the destination IP address and inspects the address to determine the destination network of the data packet.
- ◆ If the router knows the destination network, it sends the data packet to that destination network.



- ◆ If the router does not know the destination network, it sends the packet to the outbound gateway of the router:
 - The outbound gateway is also a router. Hence, when the outbound gateway receives the data packet, it goes through the same process to determine where to send the packet.
 - The outbound gateway extracts the destination IP address and inspects the address to determine the destination network of the data packet.
 - If the outbound gateway knows the destination network, it sends the data packet to that destination network.
 - If the outbound gateway does not know the destination network, it sends the packet to the higher-up outbound gateway.

Eventually, an outbound gateway that is high enough in the network hierarchy knows the destination network.

So, how does a router know about a network? By keeping *routing tables* in memory.

Routing tables keep track of the following:

- ◆ Each network known
- ◆ Router interface through which each network can be reached
- ◆ Metrics associated with each route

Routers keep one routing table for each protocol, because each protocol has its own addressing scheme and metrics.

Routers use routing tables to keep information about the networks they know. Routers build their routing tables by exchanging information about the networks they know about. Over time, as each router finds out about new networks, and new routes to those networks, the collective information about networks and routes gets more accurate.

Two types of protocols operate at the network layer: routed protocols and routing protocols:



- ◆ *Routed protocols* are used to route *data packets*. Routed protocols also identify nodes (hosts) in global networks by assigning a unique logical network address to each node in the network.

For example, IP (IPv4) is a routed protocol that uses IP addresses to identify each node in the global IP network. IPv6, AppleTalk, IPX, and SNA are other routed protocols that operate at the network layer.

- ◆ *Routing protocols* are used to send and receive *route update packets*. Route update packets carry information about new networks and new routes. Routers send each other route update packets whenever a new network is created or a new route is enabled. Some of the most common routing protocols are Routing Information Protocol (RIP), RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). Different routing protocols use different metrics to decide which routes are better than others.

Basic Router Functions

A Layer 3 router must accomplish four basic functions:

- ◆ Manage routing protocols
- ◆ Build routing tables using routing protocols
- ◆ Route packets using routed protocols and routing tables
- ◆ Maintain routing tables

IP addresses are hierarchical. They have

- ◆ A part that identifies the network
- ◆ A part that identifies the host device

For example, a network may be identified by network IP address 192.168.25.0 (subnet mask 255.255.255.0). All hosts in this network have an IP address that starts with 192.168.25.

Another network may be identified by network IP address 192.168.67.0 (subnet mask 255.255.255.0). All hosts in this network have an IP address that starts with 192.168.67.

In these two small networks, the first three numbers (192.168.25 and 192.168.67) identify the network. The last number identifies each host within its network.

Layer 2 switches interconnect hosts locally in networks 192.168.25.0 and 192.168.67.0.

Managing routing protocols

How can hosts on different networks send a data packet to each other? The routers for the two networks need to learn about each other's network. But even before that happens, they need to set up their routing protocols. Think of it in human communication terms: Before you can speak with someone in a foreign language, you need to "set up your language": learn the foreign language.

Setting up a routing protocol on a router typically involves the following:

- ◆ Starting up the routing protocol on each router
- ◆ Enabling the routing protocol on interfaces on each router
- ◆ Configuring routing protocol options

You need to execute these setup steps manually on each router. Some routing protocols can automatically negotiate certain configuration options. You read about some of these options later in this book.



Building routing tables

Routing tables keep track of networks, paths to networks, and *metrics* for each path.



Routing protocols exchange information about the networks in the immediate vicinity of each router, after the protocols are activated on each router.

The following information is exchanged:

- ◆ Each network known by each router
- ◆ The router interface through which each network can be reached
- ◆ Metrics associated with each route

Routing packets

Eventually, each router knows about its own networks (that is, networks in its immediate vicinity) and about networks in the immediate vicinity of its partner router. After RIP packets have been exchanged between routers, the routing tables contain information about the following:

- ◆ All networks known by each router
- ◆ Routes to those networks
- ◆ Metrics for each route

Prep Test

- 1 Which of the following describes the network layer?**
 - A ☐ Routes data frames between devices in the same local-area network (LAN)
 - B ☐ Routes data packets between devices in separate local-area networks (LANs)
 - C ☐ Routes data segments between MAC addresses on the same device
 - D ☐ All of the above
- 2 How does the network layer identify devices?**
 - A ☐ By assigning a physical address, also known as a MAC address, to each device in the LAN
 - B ☐ By assigning a world-wide port name (WWPN) to each node in the LAN
 - C ☐ By assigning a logical address, also known as an IP address, to each device in the network
 - D ☐ All of the above
- 3 IP addresses are organized hierarchically to facilitate which of the following?**
 - A ☐ Video streaming
 - B ☐ Audio streaming
 - C ☐ Routing
 - D ☐ Switching
- 4 What is the purpose of a router?**
 - A ☐ To route data packets between networks
 - B ☐ To switch data frames between nodes in a specific local network
 - C ☐ To segment data into small chunks to facilitate routing
 - D ☐ All of the above
- 5 How does a router know the destination of each data packet?**
 - A ☐ It inspects the data-link frame header of each data packet and extracts the destination MAC address from the header.
 - B ☐ It inspects the IP header of each data packet and extracts the destination IP address from the header.
 - C ☐ It inspects the TCP header of each data packet and extracts the destination TCP port from the header.
 - D ☐ All of the above.

6 Which of the following occurs whenever a router does not know the destination network of a data packet?

- A ☐ It sends the data packet to the default outbound gateway.
- B ☐ It sends the data packet to the nearest Layer 2 switch.
- C ☐ It discards the data packet.
- D ☐ All of the above.

7 How do routers keep track of networks?

- A ☐ By saving the TCP port of each network in the TCP port routing table
- B ☐ By saving the MAC address of each network in the MAC address routing table
- C ☐ By saving data about each network in routing tables
- D ☐ All of the above

8 Name one of the basic functions of a router.

- A ☐ Maintains TCP port tables
- B ☐ Maintains routing tables
- C ☐ Maintains MAC address tables
- D ☐ Manages the STP protocol operation

9 How does a router determine the quality of each network route to reach a certain destination?

- A ☐ By calculating metrics (costs) associated with each route
- B ☐ By sending the first data packet on all routes at the same time and picking the quickest route to send all the following packets
- C ☐ By inspecting the IP address of the destination network
- D ☐ All of the above

10 How are routing protocols used?

- A ☐ To send and receive MAC address updates between routers
- B ☐ To send and receive data frames between routers
- C ☐ To send and receive data packets between routers
- D ☐ To send and receive route update packets between routers

Answers

- 1 B. The network layer routes data packets between devices in separate local-area networks (LANs). See *"Layer 3 — Network Layer Review."*
- 2 C. The network layer identifies devices by assigning a logical address, also known as an IP address, to each device in the network. Refer to *"Layer 3 — Network Layer Review."*
- 3 C. IP addresses are organized hierarchically to facilitate the routing of data packets through networks. Read *"Layer 3 — Network Layer Review."*
- 4 A. The purpose of a router is to route data packets between networks. Look over *"Purpose of a Layer 3 Router."*
- 5 B. A router knows the destination of each data packet by extracting the destination IP address from the IP header of each data packet. Review *"Basic Router Functions."*
- 6 A. A router sends a data packet to the default outbound gateway if the router does not know the destination network of a data packet. Check out *"Basic Router Functions."*
- 7 C. Routers keep track of networks by saving data about each network in routing tables. Refer to *"Basic Router Functions."*
- 8 B. One of the basic functions of a router is to maintain routing tables. Read *"Basic Router Functions."*
- 9 A. A router determines the quality of each network route by calculating the metrics (costs) associated with each route. Look over *"Basic Router Functions."*
- 10 D. Routing protocols send and receive route update packets between routers to help routers keep track of their neighbors and of routes available. Review *"Basic Router Functions."*

Chapter 2: Managing a Router Using Cisco IOS

Exam Objectives

- ✓ **Connecting to a Cisco router**
- ✓ **Understanding the startup process of a Cisco router**
- ✓ **Configuring a Cisco router**
- ✓ **Managing Cisco router configurations**
- ✓ **Managing Cisco router authentication**

Read this chapter to find out how to use the Cisco Internetwork Operating System (IOS) to manage Cisco routers. The following topics are covered:

- ◆ Local and remote router connectivity options
- ◆ How to use the IOS command-line interface (CLI) as well as the graphical user interface (GUI) to manage Cisco routers
- ◆ How to secure access to Cisco routers using passwords
- ◆ How to manage configurations on Cisco routers

Managing a Cisco router is very similar to managing a Cisco switch. Most IOS commands are the same for switches and routers, but the output differs in some cases. Most IOS commands and GUI tools are available for both switches and routers. Some GUI tools are only available for routers, such as the Cisco Router and Security Device Manager (SDM) and SDM Express. Other GUI tools are only available for switches, such as the Cisco Device Manager. You find out about router management IOS commands and GUI tools in this chapter. You can skip over or skim through sections covering tools that you already read about in Book III, Chapter 2.

Best Practices for Using Cisco Routers

You need to understand best practices for using entry-level and top-of-the-line products. For example, top-of-the-line routers are best suited for the

core layer or for the *distribution layer* of the network. Entry-level and mid-range routers are best suited for the *access layer* or for the *distribution layer*. Cisco defines three layers in a network: core layer, distribution layer, and access layer.

Top-of-the-line routers manage the following specialized services in a network:

- ◆ Open Shortest Path First (OSPF) designated router (DR)
- ◆ OSPF backup designated router (BDR)
- ◆ Inter-VLAN routing
- ◆ WAN gateway connectivity

These services are used throughout the network. Hence, they need to run on a highly efficient and highly available router. You find out about these services in this book.

Figures 2-1 and 2-2 show the front and rear panels, respectively, of a Cisco 2621 entry-level router.



Figure 2-1:
Cisco 2621
router and
accessory
items —
Front panel.



Figure 2-2:
Cisco 2621
router and
accessory
items —
Rear panel.

Connecting to a Cisco Router

Unlike a computer host, Cisco routers do not have a keyboard, a monitor, or a mouse device to allow direct user interaction. Cisco routers can be managed by connecting either locally or remotely to the router from a computer host. You basically leverage the computer host user interface to interact with the Cisco router.



Connecting locally

Cisco routers have several ports. Think of router ports as plugs where you either connect computer hosts or other network devices.

Some router ports are reserved for other purposes than network connectivity. These are the *console* port and the *auxiliary* port on a Cisco router.

Console port

The *console port* is used to connect a management computer host to the router using a rollover cable. You use this port whenever you want to connect locally to the console of your router. The console is the default monitoring and configuration input and output facility of the router. All Cisco devices have a *console facility*, where the Cisco operating system (IOS)



displays status messages, error messages, diagnostic messages, and user prompts.

Think of the console facility as a virtual computer monitor and keyboard:

- ◆ Router output messages are going to the virtual computer monitor.
- ◆ Router user input is gathered using the virtual keyboard.

To access the console facility, you need to connect to the console port on your router. You use a rollover cable connected at one end to the console port of your router and connected at the other end to the management computer host.

Figure 2-3 illustrates a Cisco 2621 router with a management computer host connected to the router console port using a rollover cable. This figure illustrates the rear panel of the router.

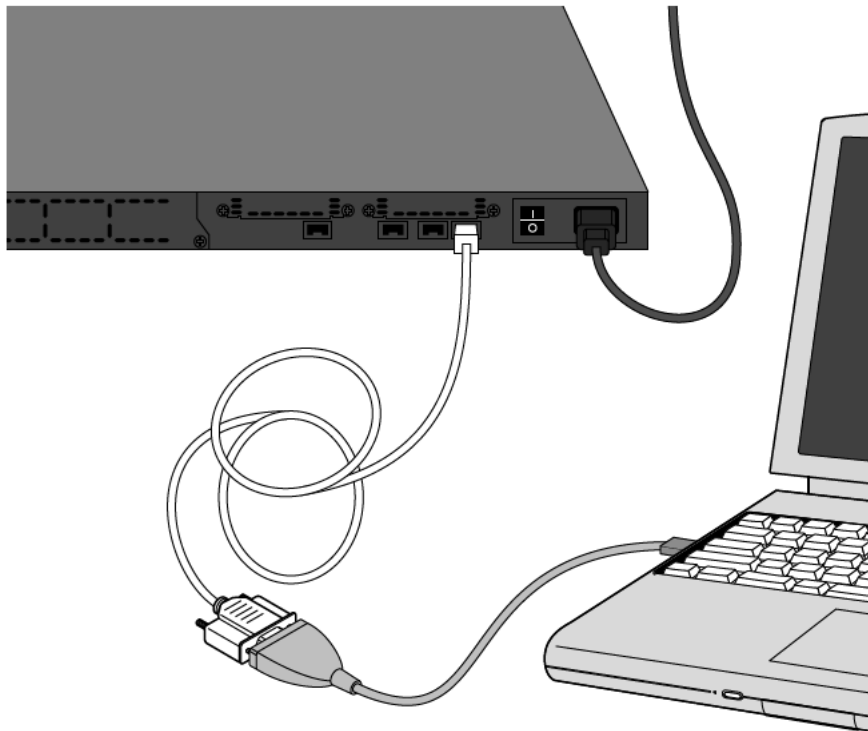


Figure 2-3:
Cisco router
console
connection.

After you physically connect the router to your computer using a rollover cable, you need to use a terminal emulation application on your management computer to open a serial terminal connection to your router. The following Telnet applications support terminal emulation:

- ◆ HyperTerminal
- ◆ TeraTerm
- ◆ SecureCRT

You need to configure a connection profile for your Cisco router using specific RS232 serial communication parameters:

- ◆ Baud rate: 9600
- ◆ Data bits: 8
- ◆ Parity: none
- ◆ Stop bits: 1
- ◆ Flow control: none

Serial communications (RS232) are governed by these parameters. Older computer hosts used to have serial communications ports (RS232) named COM1, COM2, COM3, and so on. Since the invention of USB, serial ports are being phased out. Your laptop probably boasts several USB ports but no serial port. If you do not have a serial port on your computer, you need a RS232 serial/USB port adapter.

Figure 2-4 illustrates a DB9 serial-to-USB converter (on the right in the picture). The router rollover cable (on the left in the picture) plugs in to the converter. The converter plugs in to one of the USB ports on the laptop.

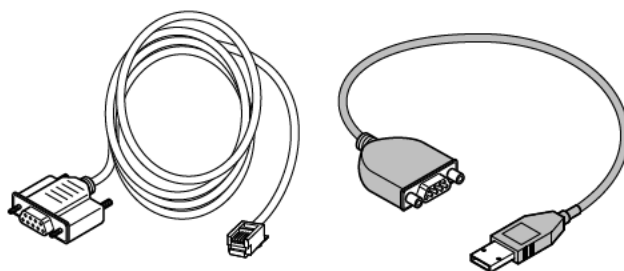


Figure 2-4:
Serial-to-
USB port
adapter.

Auxiliary port

The *auxiliary* port is used to connect a management computer host to the router using a rollover cable, similarly to the *console* port. However, you use this port whenever you want to connect a modem locally to the auxiliary port. Next, you configure the modem to receive calls from a management computer host over a telephone line. After the management computer host establishes a modem connection to the router, you are connected to the *console facility* of the router. This port is really used for remote connections to your router, but you still need to connect an answering modem locally in the auxiliary port of the router.

It is important to configure passwords to challenge console port and auxiliary port connections.

Figure 2-5 illustrates a Cisco router with a management computer host connected to the router auxiliary port using two modems.

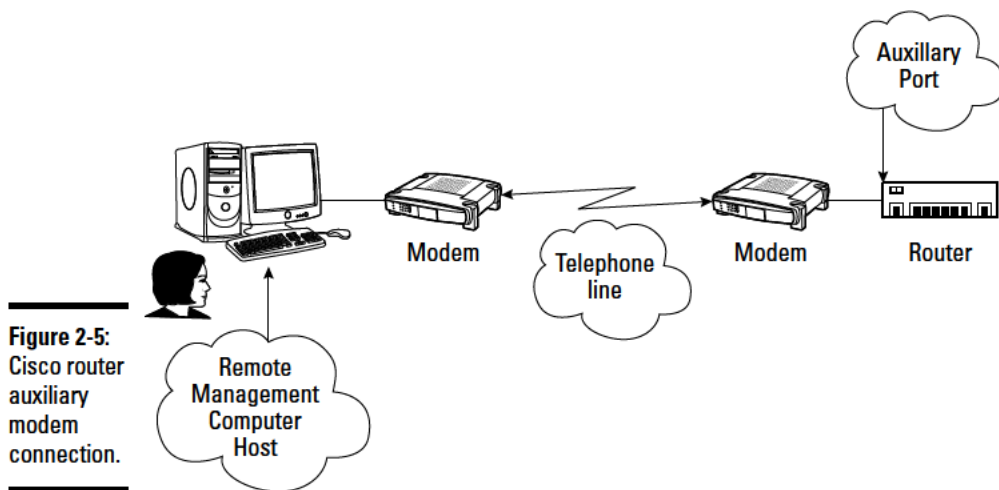


Figure 2-5:
Cisco router
auxiliary
modem
connection.

Connecting remotely

You can connect remotely to a Cisco router. You can connect both to the router console and to its terminal window from a remote management computer host.

You can connect remotely to Cisco routers in several ways:

- ◆ Connect to the auxiliary port of the router using a modem connection. This connects you to the console of the router from a remote location.

- ◆ Connect to the network IP address of the router using a Telnet or secure Telnet application. Each router has a network IP address that identifies the router as an IP node in the network. You can connect to this IP address using any Telnet or secure Telnet application, just as you connect to a computer host using Telnet or secure Telnet.
- ◆ Connect to the console IP address of the router using a Console Terminal Server. You can configure a Console Terminal Server that makes the router console facility available at a specific IP address and at a specific TCP/IP port number in the network. You can connect to this IP:port address using any Telnet application.

It is important to configure passwords to challenge console port, auxiliary port, and Telnet connections. You see how to configure console, auxiliary, and Telnet passwords in the “Configuring a Cisco Router” and the “Managing Cisco Router Authentication” sections, later in this chapter.

Figure 2-6 illustrates a Cisco router with a management computer host connected to the router IP address using Telnet.

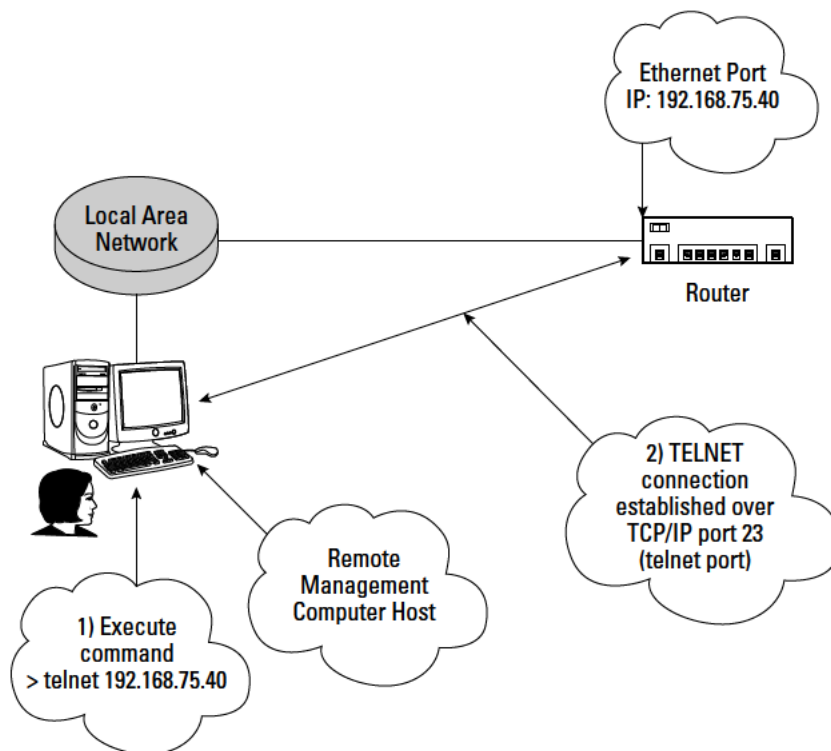


Figure 2-6:
Cisco router
Telnet
connection.

Figure 2-7 illustrates a Cisco router with a management computer host connected to the router console via a Terminal Server.

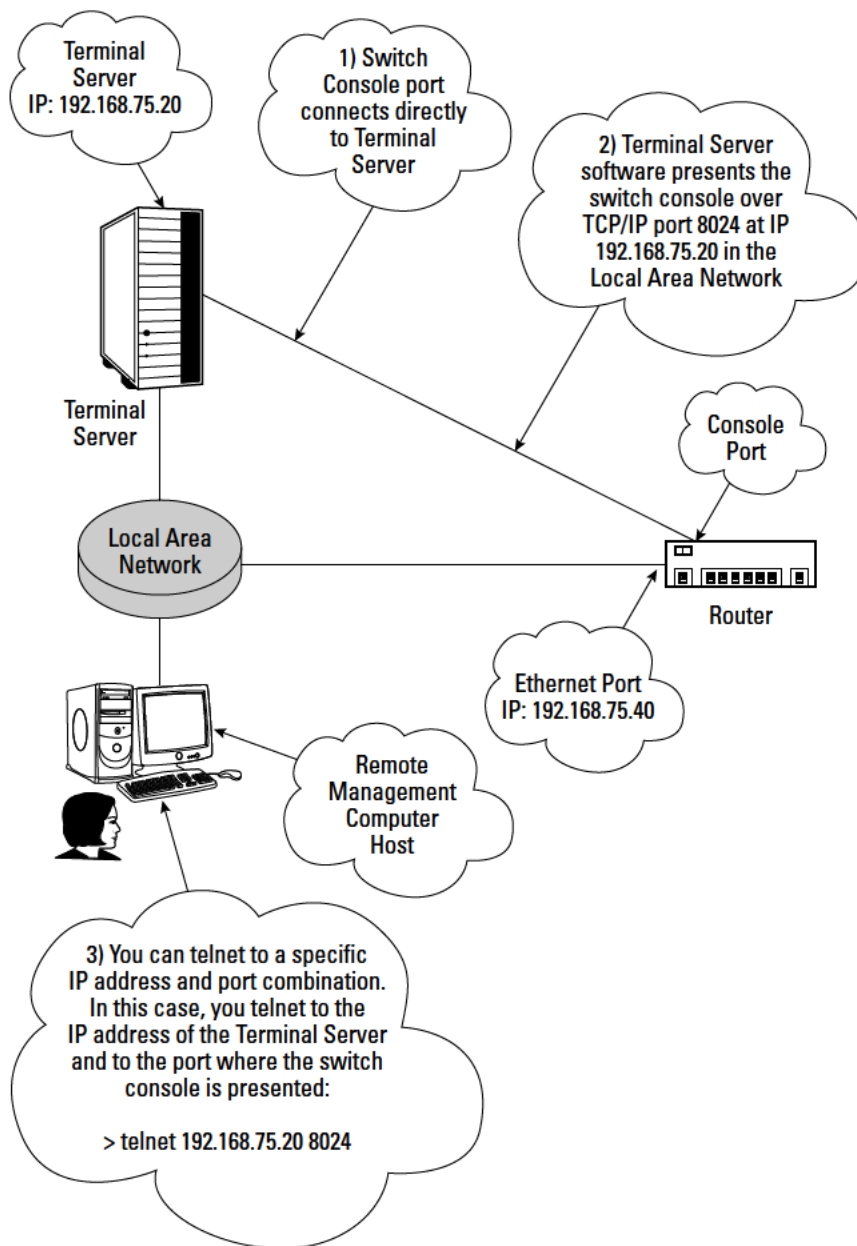


Figure 2-7:
Cisco router
Console
Terminal
Server
connection.

Cisco Router Startup Process

A Cisco router always follows the same process when it is powered up. The steps of this process are:

1. Run the POST: The Cisco router runs the power-on self test.

The POST is a microprogram, stored in ROM, that is used to verify basic functionality of the Cisco router hardware.

2. Boot up: The Cisco router runs the *bootstrap program*, also known as the *boot loader software*.

The boot loader is a microprogram, stored in ROM, that is used to bring up the router and transition it to normal operation mode by loading the Cisco IOS from flash memory. If the boot loader does not find a valid Cisco IOS in flash memory, it tries to load the IOS from a TFTP server or from ROM.

3. Load the IOS: The Cisco IOS loads into RAM.

By default, the Cisco IOS is loaded from flash memory. However, as mentioned earlier, if the bootstrap program does not find a valid IOS in flash memory, it tries to load from a TFTP server, if one is configured. If no TFTP server is configured, or if no valid IOS is on the TFTP server, the bootstrap program loads the Rx-boot image from ROM. Recall that the Rx-boot image is a subset of the Cisco IOS operating system. The Rx-boot image is used to manage the boot process. The Rx-boot image comes up with the (boot)> prompt, where you can run various commands to manage the boot process. For instance, you can manually specify a location from which to load the IOS image.

4. Load the startup configuration: After the Cisco router loads the IOS in RAM, the IOS loads the device `startup-configuration` file from NVRAM.

The *startup configuration* is loaded into RAM and becomes the *running configuration*, the configuration that changes dynamically while the Cisco device is running.

At this point, the Cisco device is in normal operation mode, ready for business.

The following IOS CLI segment shows a Cisco 2621 router starting up for the first time.

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by Cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 65536 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0xed9ee4

Self decompressing the image : #####
[OK]
```

The first part of the preceding example shows the following output from the bootstrap program:

- ◆ The version of the bootstrap program: 11.3(2)XA4
- ◆ The router platform: C2600 platform with 65K of system memory
- ◆ The IOS image size: 0xed9ee4
- ◆ The IOS image loading: Self decompressing the image : ##### ...

The output you see in the preceding example starts at the second step in the process (bootup). You do not see the output from the first step of the process (POST) here. The first part of the POST only displays messages upon test failures.

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(1a), RELEASE SOFTWARE
      (fc1)
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Fri 06-Jun-03 22:08 by dchih
Image text-base: 0x80008098, data-base: 0x819BD990
```

This part loads the Cisco IOS from flash memory and executes it in RAM. The bootstrap program loads the C2600-IK9O3S3-M Cisco IOS image.

```
cisco 2621 (MPC860) processor (revision 0x102) with 60416K/5120K bytes of memory.

Processor board ID JAD04410AGK (901795976)
M860 processor: part number 0, mask 49
Bridging software
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

This part shows some information about the router hardware and software installed:

- ◆ This is a Cisco 2621 router with an MPC860 CPU.
- ◆ It has 65K of system memory.
- ◆ It has bridging software installed.
- ◆ It supports the X.25 WAN protocol.
- ◆ It has two Fast Ethernet interfaces.
- ◆ It has 32K of system memory configured as NVRAM.
- ◆ It has 16K of system memory configured as flash memory.

Next, the IOS prompts you to start the initial configuration dialog:

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK903S3-M), Version 12.3(1a), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Fri 06-Jun-03 22:08 by dchih

Router>
```

This part shows the final stage of the boot process (load startup configuration). Because this is a new router, no startup configuration exists.

The IOS asks whether you would like to enter the initial configuration dialog. This dialog allows you to quickly configure the router:

- ◆ IP address
- ◆ Default gateway (router)
- ◆ Subnet mask
- ◆ Console password
- ◆ Host name
- ◆ Telnet password

If you choose not to run the initial configuration dialog at this time, you can press Enter to access the Router> prompt. When you're at the Router> prompt, you can run IOS commands to monitor and manage the router.

Routers that have Cisco SDM (Router and Security Device Manager) preinstalled, such as the 1800 series, require that you create an administrator user before you are allowed to run the initial configuration dialog. These routers provide a default administrator user named "cisco," identified by password "cisco," that can only be used one time to create your personalized administrator user. Here is the last part of the boot process on a Cisco 1801 router that has SDM preinstalled:

```
-----
Cisco Router and Security Device Manager (SDM) is installed on this device. This
feature requires the one-time use of the username "cisco" with the password
"cisco". The default username and password have a privilege level of 15.
Please change these publicly known initial credentials using SDM or the IOS
CLI.
```

Here are the Cisco IOS commands.

```
username <myuser> privilege 15 secret 0 <mypassword>
```

```
no username cisco
```

Replace <myuser> and <mypassword> with the username and password you want to use.

For more information about SDM please follow the instructions in the QUICK START GUIDE for your router or go to <http://www.cisco.com/go/sdm>

User Access Verification

Username: cisco

Password: cisco

The router informs you about the “cisco” default temporary administrator user and prompts you to create a new personalized administrator user. To create the new personalized administrator user, use the `username` command:

```
Router> configure terminal
```

```
Router(config)# username Admin007 privilege 15 secret 0 Admin007Password
```

This command creates a new user named Admin007, identified by password Admin007Pasword, with level_15_privilege access permission. From now on, you can log in to your router using this new administrator user. You are ready to set up your router at this point.

The next section describes how to configure a Cisco router.

Configuring a Cisco Router

Read this section to find out how to initially set up a Cisco router. You also see how to manage startup and running configurations.

Cisco routers ship with several items, as shown in Figure 2-8:

- ◆ Console rollover cable: This is the cable you need to connect to the console port on the router.
- ◆ AC power cord.
- ◆ 19-inch rack mounting brackets.
- ◆ Getting Started documentation CD.
- ◆ Router and Security Device Manager (SDM) CD.



Figure 2-8:
Cisco 2621
router and
accessory
items.

These items are needed to initially power up and configure the router. First, use the mounting brackets to mount the router into a standard EIA-310-D data center rack. Next, connect the power cord to the power feed of the EIA-310-D data center rack.

Initial router configuration

Cisco routers are not configured when they are new, out of the box. They do not have a startup configuration, so you need to create one.

Cisco routers revert to setup mode anytime that no startup configuration is saved in NVRAM. This happens in two situations:

- ◆ The device is new: No startup configuration exists on new devices.
- ◆ The startup configuration has been deleted: You can delete the startup configuration using IOS commands.

You can create a startup configuration using one of the following methods:

- ◆ Using the initial configuration dialog
- ◆ Using the Cisco IOS setup mode commands

Initializing the router using the initial configuration dialog

The first time you power on a Cisco router, it has no startup configuration in NVRAM. You can connect to the console of the router to get access to the IOS prompt. The router will be in *setup mode* because no startup configuration exists. In setup mode, the IOS asks you to configure the following:

- ◆ IP address
- ◆ Default gateway (router)
- ◆ Subnet mask
- ◆ Enable and enable secret password
- ◆ Host name
- ◆ Telnet password

If choose not to configure the router and use it without a startup configuration, you can avoid or abort setup mode using one the following methods:

- ◆ Exit setup mode by pressing Ctrl+C
- ◆ Answer no when setup mode asks whether you want to configure the router
- ◆ Answer no when setup mode asks whether you want to save the configuration at the end of the series of setup questions

Although you can use a router without creating a startup configuration, it is best practice to verify the router and to create a startup configuration before you start using the router. Using the router without a startup configuration allows you to initially test the basic functionality of the router. However, you should always have a startup configuration and, specifically, console, auxiliary, and privileged mode passwords configured before you start using the router in a production environment.

Here is an example of the initial setup mode dialog on a Cisco 2621 router:

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by Cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 65536 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0xed9ee4

Self decompressing the image : #####
[OK]

[ ... some boot messages cut ... ]
```

The first part of the output shown in the preceding example displays various boot messages. The router is now up and running.

Because no startup configuration exists in NVRAM, the IOS asks whether you want to run the initial configuration dialog. You type **yes** as follows to run the initial configuration dialog:

```

--- 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

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

Enter host name [Router]: RT1

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: my_priv_encrypt_password

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: my_priv_password

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

```

The second part of the output shown in the preceding example prompts you to set a host name and passwords on your router. In this example

- ◆ You name the router RT1.
- ◆ You set the encrypted privileged mode password to `my_priv_encrypt_password`.
- ◆ You set the unencrypted privileged mode password to `my_priv_password`.
- ◆ You set the VTY access lines password to `my_telnet_password`.

The next section of the initial configuration dialog, shown in the following example, displays a summary of the Ethernet interfaces (ports) available on the router:

```
Current interface summary

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

Interface      IP-Address  OK? Method Status  Protocol
FastEthernet0/0 unassigned YES unset  down    down
FastEthernet0/1 unassigned YES unset  down    down

Enter interface name used to connect to the
management network from the above interface summary: fastethernet0/0

Configuring interface Fastethernet0/0:
Use the 100 Base-TX (RJ-45) connector? [yes]:
Operate in full-duplex mode? [no]: yes
Configure IP on this interface? [yes]:
  IP address for this interface: 192.168.75.40
  Subnet mask for this interface [255.255.255.0] :
  Class C network is 192.168.75.0, 24 subnet bits; mask is /24
```

The third part of the output shown in the preceding example prompts you to set up a management interface for the router. You choose the first Fast Ethernet interface: Fast Ethernet 0/0. You set an IP address and subnet mask on the management interface.

The next section of the initial configuration dialog, shown in the following example, displays a summary of the configuration that will be created on the router.



Only the secret password is encrypted by default: the encrypted privileged mode password.

You can also encrypt the other passwords for increased security.

The following configuration command script was created:

```
hostname RT1
enable secret 5 $1$3GJW$pVC5U4qVd1bzy5x8kDkwa.
enable password my_priv_password
line vty 0 4
password my_telnet_password
no snmp-server
!
no ip routing
!
interface FastEthernet0/0
no shutdown
media-type 100BaseTX
full-duplex
ip address 192.168.75.40 255.255.255.0
!
```

```
interface FastEthernet0/1
shutdown
no ip address
!
end
```

The last section of the initial configuration dialog, shown in the following example, prompts you to do one of the following:

- ◆ Save the configuration you just created to NVRAM.
- ◆ Return to the setup without saving the configuration you just created.
- ◆ Go straight to the IOS prompt without saving the configuration you just created.

Choose “2” in the following example to save the configuration you just created to NVRAM. This configuration becomes the startup configuration.

```
[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]:

Building configuration...

[OK]

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

RT1>

Initializing the router using Cisco IOS setup mode commands

You can also configure router settings manually using Cisco IOS setup mode commands at any time.

The following sections show you a few basic Cisco IOS configuration commands that you can use at any time to configure your Cisco device.

Naming the router

You can name your router using the `hostname` Cisco IOS command. You should name all your routers using meaningful names to ease identification and management of each router.

This is particularly important in large networks.

To configure the host name of the router, run the following commands:

```
Router>enable (or en)
Router#configure terminal (or config t)
Router(config)#hostname SW1
```



```
RT1(config)#exit
RT1#disable
RT1>
```

Configuring the management IP address for the router

You can configure an IP address and an IP gateway for your router using the `ip address` and `ip default-gateway` Cisco IOS commands. This allows you to connect to the router from remote locations using either Telnet or HTTP.

To configure the management IP address and default gateway on your router, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#interface fastethernet0/0 (or int fe0/0)
RT1(config-if)#ip address 192.168.75.40 255.255.255.0
RT1(config-if)#no shutdown
RT1(config-if)#exit
RT1(config)#ip default-gateway 192.168.75.1
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `interface fastethernet0/0` command selects an interface to work with. In this example, you select the first Ethernet interface of the router (Fast Ethernet 0/0).

The `ip address 192.168.75.40 255.255.255.0` command sets the IP address and the subnet mask on the interface that you selected previously. Observe that the IOS prompt now shows `RT1(config-if)#`. `Config-if` means that you are configuring an interface (`if`) now.

The `no shutdown` command starts up the Fast Ethernet 0/0 interface. Recall that you enable components and services on a Cisco router using the component or service name. You disable components and services on a Cisco router using the component or service name prefixed with the `no` keyword. Here, `shutdown` is actually a state, not a component or service. An interface is either shut down or not shut down (started up). To summarize:

- ◆ To shut down an interface, select it and execute `shutdown`.
- ◆ To start up an interface, select it and execute `no shutdown`.

The `ip default-gateway 192.168.75.1` command sets the default gateway for the router. Observe that you first exit from interface configuration mode (`RT1(config-if)#exit`) because the default gateway applies to the whole router, not just to an interface. Now, you are back in global configuration mode (`RT1(config)#`).

The Cisco IOS prompt is designed to show you the configuration mode you're in:

- ◆ `(config)`: You are in global configuration mode.
In this mode, you can execute commands that configure global router settings, that is, settings that apply to the whole router.
- ◆ `(config-if)`: You are in interface configuration mode.
In this mode, you can execute commands that configure router interface settings, that is, settings that apply to just one interface of the router. You select the interface to work with using the `interface` command.
- ◆ `(config-if-range)`: You are in interface range configuration mode.
In this mode, you can execute commands that configure a range of router interfaces, that is, settings that apply to a range of interfaces on the router. You select the range of interfaces to work with using the `interface range` command.

Configuring passwords

You can configure authentication passwords for your router using the `password` and `login` Cisco IOS commands. By default, new Cisco devices do not have a password configured.

You can configure several passwords for different types of access:

- ◆ **Console password:** Used for console access through the console port or through a Console Terminal Server.
- ◆ **Auxiliary password:** Used for console access through the auxiliary port using a modem.
- ◆ **VTY lines password:** Virtual type terminal (VTY) lines are used for Telnet and Secure Shell (SSH) access. They are called virtual type terminal lines because no physical terminal is connected to the router. Rather, you connect a computer host to the network and access the router remotely using the router management IP address. A terminal emulation program on the computer host emulates a physical terminal (TTY).
- ◆ **Privileged password:** Used for privileged mode access. Privileged mode is an “expert” management operation mode used to run some Cisco IOS commands.

The console port and the auxiliary port are enabled by default, even if no password is specified for them. This is a security risk. It is best practice to specify at least a console password on new Cisco devices.

The VTY lines (Telnet and Secure Shell) are disabled by default. You need to specify a password for the VTY lines to enable them.

To configure passwords, you need to instruct the Cisco device to prompt for authentication. You use the `login` Cisco IOS command to do this.

Best practice

You should at least set passwords for console and VTY access to secure access through the console port and to enable and secure remote access through Telnet or SSH.

The following sections describe how to configure passwords for console and VTY access using Cisco IOS commands.

Console password

To configure the console password, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#line console 0 (or line con 0)
RT1(config-line)#password my_password
RT1(config-line)#login
RT1(config-line)#exit
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `line console 0` command selects the console line. Cisco devices have only one console line: console 0.

The `password my_password` command sets the `my_password` password on the console access line.

Finally, instruct the Cisco device to prompt for authentication by entering the `login` Cisco IOS command. From now on, anytime you connect to the console line you will be prompted to provide a password. The password you provide must be `my_password`. To disable the authentication prompt, issue `line console 0` again and enter the `no login` command.

You use the `exit` commands to exit the `config-line` mode and to exit the `config` global configuration mode.

Telnet password

To configure a password for the VTY lines, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#line vty 0 ?
    <0-4> last line number
RT1(config-line)#line vty 0-4
RT1(config-line)#password my_telnet_password
RT1(config-line)#login
RT1(config-line)#exit
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `line vty 0 ?` command asks the Cisco IOS how many VTY lines are available. The response (`<0-4> last line number`) shows that five VTY lines exist on this particular router (you can have five simultaneous Telnet sessions opened to this router). Now, you can configure a password either on one of the VTY lines, by selecting that particular line, or on all VTY lines, by selecting the whole 0–4 line range.

The `line vty 0-4` command selects the whole 0–4 VTY line range. Cisco devices have several VTY *access lines*. Older routers have only five VTY lines. Newer routers have as many as 1,180 VTY lines. It is best practice to query the Cisco IOS about how many VTY lines are available.

Two main reasons exist to have several VTY access lines on a Cisco device:

- ◆ **Allowing you to connect to the router and connect to another device from the router:** Two VTY lines are needed in this case: one to connect into the router and another one to connect out of the router to another device.
- ◆ **Allowing several administrators to work on the router:** In large networks, more than one administrator may manage the network. More than one administrator may need to connect from a remote location to the same router using Telnet or SSH. This is typical with large core routers.

The `password my_telnet_password` command sets the `my_telnet_password` password on the VTY access lines. You can set a different password on each line. However, this is not recommended, because you don't

know which VTY line you are on when you log in, so you wouldn't know which password to enter. Best practice is to select the whole range of VTY lines and to set the same password on all of them.

Finally, instruct the Cisco router to prompt for authentication by entering the `login` Cisco IOS command. From now on, anytime you connect to any of the VTY lines, you will be prompted to provide a password. The password you provide must be `my_telnet_password`. To disable the authentication prompt, issue `line vty 0-4` again and enter the `no login` command.

After you run the initial setup IOS commands, the router has a startup configuration saved in NVRAM. The router is reachable on the IP network. You can now connect to the router either locally to its console or auxiliary port, or remotely to its IP address, as explained previously in the section "Connecting to a Cisco Router."

Configuring banners

You can optionally configure a banner for your router using the `banner` Cisco IOS command. The purpose of a banner is to display a brief message about the router when you log in. This is useful when you have many routers spread out across multiple sites. It helps identify the router you log in to and see its configuration and usage guidelines. Banners are also useful for legal reasons: You can add a security warning in the banner message to warn users against unauthorized logins to the router. Although this does not prevent the user from logging in to the router, it does provide ground for legal action in the case of unauthorized logins. Always use passwords to secure your routers.

Four types of banners are available:

- ◆ **Message of the day (MOTD) banner:** This is the first banner to display when a user connects to a router, regardless of the type of connection. This banner is used to display a message for all users that connect to the router, before they log in. This is typically used for an unauthorized access warning.
- ◆ **Login banner:** This banner is displayed on TTY or VTY terminals after the MOTD banner. This banner is typically used to display information about the router and to provide guidelines on how to log in and use the router.
- ◆ **Incoming terminal connection banner:** This banner is displayed on reverse TTY or VTY terminals after the MOTD banner. This banner is used for the same reasons as the login banner. The only difference is the type of terminal connection: You can specify additional information in this banner for users that connect with reverse TTY or VTY terminals.

- ◆ **EXEC process creation banner:** This banner is displayed whenever an EXEC process is created, after the user is logged in. An EXEC process is created for each user EXEC prompt. User EXEC prompts are established for each user connected to the router, after the user logs in successfully. Hence, the EXEC process creation banner is displayed after the login/incoming banners and after the MOTD banner.

To configure an MOTD banner on your router, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (config t)
RT1(config)#banner motd -
Enter TEXT message. End with character '-'.
$This router is property of silange.com networks. Unauthorized access is
  prohibited. Please disconnect if you are not a silange.com employee,
  customer, or business partner.
-
RT1(config)#
```

The `banner motd -` command starts the banner text editor using '-' as the delimiting character. The delimiting character is used by the IOS to determine when you are done typing the banner text. You enter the banner text of your choice and finish by typing the delimiting character ('-' in this case) and pressing Enter. The delimiting character can be any character, but you cannot use that character within the text of the banner. Cisco IOS would interpret that as the end of the banner text.

Resetting a Cisco router

Cisco routers revert to setup mode anytime no startup configuration exists in NVRAM. Normally, this only happens when the router is new and not yet configured.

However, you may want to clear the current configuration in NVRAM and start a new configuration from scratch. This is typically a last-resort troubleshooting method: When problems affect the router and no troubleshooting method fixes the problems, your last resort is to reset the router and reconfigure it.

Resetting the router clears the configuration of the router.

After it is reset, the router is in the state it was when you purchased it:

- ◆ No IP address
- ◆ No host name
- ◆ No default gateway (router)

- ◆ No subnet mask
- ◆ No console password
- ◆ No Telnet password
- ◆ No startup configuration

It is best practice to back up the startup configuration of a router to a backup computer host before resetting the router.

To reset a router, you need to clear its startup configuration from NVRAM:

```
RT1>enable (or en)
RT1#erase startup-config
Erasing the nvram filesystem removes all configuration files!
Continue? [confirm] <press Enter to confirm>
[OK]
Erase of nvram: complete
RT1#
```

Observe that the `erase` command warns you that the NVRAM contents will be reinitialized and prompts you to confirm. The default answer is `confirm`. To confirm, just press Enter.

Managing Cisco router configuration

Ongoing, you can manage your router using the following:

- ◆ Cisco IOS commands
- ◆ The Cisco Network Assistant (CNA) GUI tool
- ◆ The Cisco Router and Security Device Manager (SDM) GUI tool
- ◆ The Cisco Router and Security Device Manager (SDM) Express Web tool

The Cisco Network Assistant (CNA) tool, the Cisco Router and Security Device Manager (SDM) tool, and the Cisco Router and Security Device Manager (SDM) Express tool are graphical user interface (GUI)-based tools that allow you to manage your router and its startup and running configurations from a remote location using a computer host. Their GUI interfaces are much easier to use and more intuitive than Cisco IOS commands.

Recall that although the Cisco Network Assistant (CNA) tool can monitor and manage both switches and routers, it is typically used with Cisco switches, rather than with Cisco routers. The Cisco Router and Security Device Manager (SDM) and the Cisco Router and Security Device Manager (SDM) Express are the preferred router monitoring and management tools.

You read about the Cisco Network Assistant (CNA) tool, the Cisco Router and Security Device Manager (SDM) tool, and the Cisco Router and Security Device Manager (SDM) Express in Book I, Chapter 10. You find out about Cisco IOS router configuration management commands in the following sections.

Managing the router boot process

Cisco routers always follow the same boot process when they are powered up. This process contains four stages:

1. **Run the POST:** The Cisco router runs the power-on self test to verify basic functionality of the Cisco router hardware.
2. **Boot up:** The Cisco router runs the *bootstrap program* to bring up the router and transition it to normal operation mode by loading the first Cisco IOS image from flash memory.
3. **Load the IOS:** The Cisco IOS loads into RAM from flash memory.
4. **Load the startup configuration:** After the Cisco router loads the IOS in RAM, the IOS loads the device *startup configuration* from NVRAM. The startup configuration is loaded into RAM and becomes the *running configuration*, the configuration that changes dynamically while the Cisco router is running. At this point, the Cisco router is in normal operation mode, ready for business.

This process is also called the *automatic boot process*. The router automatically boots up with current options and loads the startup configuration.

Boot command

Recall that the Cisco bootstrap program loads the first Cisco IOS image file from flash memory, by default, when the router is powered up. In some cases, you may need to boot a specific IOS image file from flash memory. For example, suppose that you download a new Cisco IOS image file that contains additional features, but you would like to test it on your router before you remove the original IOS image file. You can configure the router to boot with the new IOS image file using the `boot` command.

The `boot` command allows you to configure the boot process of a Cisco router. You can control the following:

- ◆ Which Cisco IOS image file is loaded
- ◆ Which startup configuration file is loaded

You can use the Cisco IOS contextual help to see the options available with the `boot` command:

```
RT1>enable (or en)
Password: my_priv_encrypt_password
RT1#configure terminal (or config t, or conf t)
RT1(config)#
RT1(config)#boot ?
    bootstrap  Bootstrap image file
    host        Router-specific config file
    network     Network-wide config file
    system      System image file
RT1(config)#exit
RT1#disable
RT1>
```

Observe that you need to be in privileged global configuration mode to execute the `boot` command.

The `bootstrap`, `host`, and `network` options are beyond the scope of the CCNA test.

The `service-config` command enables loading of router startup configuration files from remote servers. If loading of configuration files from remote servers is not enabled with the `service-config` command, the router ignores the `boot host` and `boot network` options and looks for a startup configuration file in its NVRAM instead.

Loading startup configuration files from remote servers is done in two phases:

1. **The IOS loads the `network` configuration file.** The `network` configuration file contains configuration settings that apply to all routers in your network that are loading their startup configuration from a network configuration server. You would typically have only one `network` configuration file for all your routers. The `network` configuration file name is `network-config` by default.
2. **The IOS loads the `host` configuration file.** The `host` configuration file contains configuration settings that apply to a specific router. You may have as many `host` configuration files as you have routers in your network, if each router needs specific settings. The `host` configuration file name is `<router_hostname>-config` by default. It is comprised of the router host name (in lowercase characters) and the `-config` suffix.

The `boot host` option sets the location of the `host` configuration file of the router.

The `boot network` option sets the location of the `network` configuration file of the router.

Using the `host` and `network boot` options in conjunction with the `service-config` command is useful in large environments where you have a lot of routers to manage. It's more efficient to manage the routers' network and host startup configuration files on a central management computer than to keep track of the files on each router. It is best practice to back up the configuration server host to avoid losing the configuration files.

The `system` option allows you to boot a specific Cisco IOS image file. This is useful in cases when, for example, you download a new Cisco IOS image file, containing additional features, and you would like to test it on your router.

The `system` option allows you to boot a specific Cisco IOS image file either from local flash memory on the router or from a remote server.

Here is an example in which you set the router to boot with a specific Cisco IOS image file stored in flash memory:

```
RT1>enable (or en)
Password: my_priv_encrypt_password
RT1#configure terminal (or config t, or conf t)
RT1(config)#
RT1(config)#boot system flash:/c2600-ik9o3s3-mz.123-1a.bin
RT1(config)#exit
RT1#disable
RT1>
```

Observe that you need to be in privileged global configuration mode to execute the `boot` command.

You can use the `show running-configuration` command to verify the current boot options on a router:

```
RT1>enable (or en)
Password:my_priv_encrypt_password
RT1#show running-configuration | include boot
boot-start-marker
boot system flash c2600-ik9o3s3-mz.123-1a.bin
boot-end-marker
RT1#disable
RT1>
```

Observe that you need to be in privileged EXEC mode to execute the `show running-configuration boot` command.

Note also that you filter the output to display only lines that contain the word *boot* using the `| include boot` suffix.

This command shows the current boot options. All options can be changed with the corresponding `boot` command, as explained earlier. After you change a boot option, you need to reboot your router using the `reload` command in privileged EXEC mode.

Managing the router boot process with the configuration register

In Book I, Chapter 10, you read that the configuration register is a 2-byte (16-bit) area of NVRAM that holds a numeric value defining how the Cisco router starts up.

By default, the value stored in the configuration register instructs the bootstrap program to load the Cisco IOS from flash memory and to load the startup configuration from NVRAM.

You can change the value of the configuration register from the ROMMON prompt. To get to the `rommon >` prompt, you need to break out of the bootstrap process by pressing Ctrl+Break while the Cisco router is booting up.

The configuration register can be set to various values, but the following three values are important to remember:

- ◆ **0x2100:** This value instructs the bootstrap program to boot to the ROMMON prompt. This is equivalent to pressing Ctrl+Break while the Cisco router is booting up to break out of the bootstrap process and exit to the `rommon>` prompt.
- ◆ **0x2101:** This value instructs the bootstrap program to boot to the `(boot) > Rx-boot` prompt.
- ◆ **0x2102 to 0x210F:** These values instruct the bootstrap program to boot the Cisco IOS from flash memory. Observe that there are 14 possible values (2 to F). The value that you specify determines which copy of the IOS is loaded. You can have up to 14 different copies (versions) of the Cisco IOS in flash memory. The value that you set in the configuration register determines which copy is loaded. *The configuration register is set to 0x2102 by default.* The bootstrap program loads the first copy of the Cisco IOS from flash memory.

So, what are the other configuration register values that you can set? The configuration register is comprised of 2 bytes or 16 bits, which means 2^{16} (65,536) possible values. This is a lot of possible configuration variations, but in reality, only a small number of these values are used.

Table 2-1 illustrates the default value of the configuration register (0x2102) in binary and hexadecimal values.

Table 2-1		Configuration Register															
	Nibble 1				Nibble 2				Nibble 3				Nibble 4				
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
Bin	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	
Hex	2				1				0				2				

Each binary nibble (each group of 4 bits) is a digit in hexadecimal. You read this table by nibble:

- ◆ The value of nibble 1 is 0010_2 , which is 2_{16} .
- ◆ The value of nibble 2 is 0001_2 , which is 1_{16} .
- ◆ The value of nibble 3 is 0000_2 , which is 0_{16} .
- ◆ The value of nibble 4 is 0010_2 , which is 2_{16} .

Next, you put the value of each nibble side by side to obtain the hexadecimal number: 0x2102.

Now, how would you express 0x2102 in binary? Each digit is a nibble in binary:

- ◆ The value of nibble 1 is 2_{16} , which is 0010_2 .
- ◆ The value of nibble 2 is 1_{16} , which is 0001_2 .
- ◆ The value of nibble 3 is 0_{16} , which is 0_2 .
- ◆ The value of nibble 4 is 2_{16} , which is 0010_2 .

Next, you put the value of each nibble side by side to obtain the binary number: 0010 0001 0000 0010₂.

By turning bits on and off in the configuration register, you configure the behavior of the bootstrap program. Each bit-set combination corresponds to a number in hexadecimal. You set the configuration register to that bit set by initializing the configuration register with the corresponding hexadecimal number.

Table 2-2 lists the purpose of some of the bits of the configuration register.

Table 2-2 Configuration Register Bit Purpose		
<i>Bit</i>	<i>Hexadecimal Value</i>	<i>Purpose</i>
0–3	0x0000–0x000F	Boot option
6	0x0040	Do not load startup configuration from NVRAM
8	0x0100	Disable break
11,12	0x0800, 0x1000	Set console line speed
13	0x2000	Boot from ROM if TFTP boot fails
15	0x8000	Enable diagnostic messages

Bit 0 instructs the bootstrap program to load a specific operating system. The default value of bit 0 (0x0002) instructs the bootstrap program to load the first copy (version) of the Cisco IOS from flash memory. Recall that you can have 14 different copies (versions) of the Cisco IOS in flash memory. Table 2-3 summarizes the values of bit 0 and their purpose.

Table 2-3 Configuration Register: Bit 0 — Boot Option		
<i>Bit 0 Value</i>	<i>Hex</i>	<i>Purpose</i>
0	0x0000	Boot to <code>rommon></code> prompt
1	0x0001	Boot to <code>(boot)></code> prompt
2	0x0002	Boot first copy of Cisco IOS from flash memory
3	0x0003	Boot second copy of Cisco IOS from flash memory
4	0x0004	Boot third copy of Cisco IOS from flash memory
F	0x000F	Boot 14th copy of Cisco IOS from flash memory

Bit 6 is important for recovering lost passwords. Bit 6 instructs the bootstrap program to avoid reading the startup configuration from NVRAM. This allows you to recover lost or forgotten passwords. You find out how to do this in the section “Recovering router passwords,” later in this chapter.

Bit 8 instructs the bootstrap program to disable the break key (Ctrl+Break) during normal operation. Note that you can always break out of the boot process to the `rommon>` prompt if you press Ctrl+Break during the first 60 seconds while the router boots up, regardless of this setting. Setting bit 8 to 1 really means that Ctrl+Break is disabled during normal operation. Bit 8 is set by default.

Bits 11 and 12 instruct the bootstrap program to use a certain speed for the console line. By default, these two bits are not set: Bit 11 is 0 and bit 12 is also 0. Here are the values and meanings for bits 11 and 12:

- ◆ **00:** Speed is 9600 baud
- ◆ **01:** Speed is 4800 baud
- ◆ **10:** Speed is 1200 baud
- ◆ **11:** Speed is 2400 baud

The console line speed is 9600 baud by default; both bits are 0 by default. There is no reason to change the speed unless you use a computer host that cannot connect at 9600 baud to the console line. You can set a lower speed in that case.

Bit 13 instructs the bootstrap program to boot the default Cisco IOS from ROM if booting from flash memory fails and if booting from a TFTP network boot server also fails.

Bit 15 instructs the bootstrap program to enable diagnostic messages and to ignore the contents of NVRAM. This option is useful for troubleshooting the router.

These values can be combined. For example, the configuration register is set by default to 0x2102. Referring to Table 2-2, bits 13 and 8 are set to 1. Referring to Table 2-3, bit 0 is set to 2. This means the following:

- ◆ **Bit 13:** 0x2000 instructs the bootstrap program to boot the default Cisco IOS from ROM if booting from flash memory fails and if booting from a TFTP network boot server also fails.
- ◆ **Bit 8:** 0x0100 instructs the bootstrap program to disable the break key (Ctrl+Break) during normal operation. Note that you can always break out of the boot process to the `rommon>` prompt if you press Ctrl+Break during the first 60 seconds while the router boots up, regardless of this setting. Setting bit 8 to 1 means that Ctrl+Break is disabled during normal operation.
- ◆ **Bit 0:** 0x0002 instructs the bootstrap program to load the first copy (version) of the Cisco IOS from flash memory. Recall that you can have 14 different copies (versions) of the Cisco IOS in flash memory. The value you set in bit 0 in the configuration register determines which copy is loaded. Table 2-3 summarizes the values of bit 0 and their meaning.

You can change the value of the configuration register using the `config-register` Cisco IOS command. You need to reboot the router for the change to take effect.

Here is an example:

```
SW1>enable (or en)
SW1#configure terminal (or config t)
SW1(config)#config-register 0x2100
SW1(config)#exit
SW1#show version (or sh ver)
...
Configuration register is 0x2102 (will be 0x2100 at next reload)
```

Here you set the configuration register to 0x2100 to boot to the ROM Monitor `rommon>` prompt at next reboot. Observe that the `show version` Cisco IOS command shows you the current value of the configuration register and the future value at next reboot, if you change it.

Managing configurations

Two configurations exist on any Cisco router: the startup configuration and the running configuration. The following sections review the characteristics of startup and running configurations and describe how to manage them on a Cisco router.

Startup configuration

The startup configuration is the configuration that the Cisco IOS loads when it boots up. The startup configuration is stored in NVRAM, which keeps its contents even when the Cisco device is powered down.

Recall that whenever no startup configuration exists in NVRAM, the router starts in setup mode to allow you to create a startup configuration. After you complete the setup mode, you are prompted to save the configuration to NVRAM. If you answer yes, the configuration you created is saved to NVRAM; it becomes the startup configuration. You can also manually save the current configuration to NVRAM by using the `copy running-config startup-config` Cisco IOS command.

Cisco devices use the startup configuration data to configure the device before normal operation starts. The Cisco IOS loads the startup configuration from NVRAM into RAM. At that point, the startup configuration becomes the running configuration. The router is up and ready in normal operation mode.

Running configuration

The running configuration is the dynamic data that changes while the Cisco device is in normal operation mode. This includes the following:

- ◆ Routing tables
- ◆ VLAN data
- ◆ Routing protocol configuration data
- ◆ Temporary buffers

The Cisco IOS loads the startup configuration from NVRAM into RAM during the boot process. After it is in RAM, the startup configuration becomes the running configuration and can change dynamically.

You can save the running configuration into NVRAM to replace the startup configuration with updated data. To do this, use the `copy running-config startup-config` Cisco IOS command. You can also save the running configuration to a file on a computer host.

Saving the running configuration to NVRAM

To save the running configuration to NVRAM, run the following command:

```
RT1>enable (or en)
RT1#copy running-config startup-config (or copy run start)
Destination filename [startup-config]? <press Enter>
Building configuration . . .
[OK]
RT1#
```

The second line shows the `copy` command. You can also use the short form of this command (`copy run start`).

The third line asks where you want to copy the running configuration to. You have several possible destinations:

- ◆ `startup-config`: Use this keyword to copy the current running configuration over the startup configuration in NVRAM.
- ◆ `flash`: Use this keyword to copy the current running configuration to a file in flash memory, alongside the Cisco IOS.
- ◆ `ftp`: Use this keyword to copy the current running configuration to an FTP server. This option is useful to back up the router configuration to a remote computer host.
- ◆ `archive`: This is similar to the `ftp` option, except that you archive to a tape- or disk-based backup system directly, instead of passing through a computer host.

The default destination is the `startup-config` file in NVRAM. To keep the default answer, just press Enter. Sometimes, the Cisco IOS prompts you to enter a value, and it shows the default answer in between brackets []. To keep the default answer, just press Enter.

Monitoring the running configuration

To monitor the running configuration, run the following command:

```
RT1#show running-config (or sh run)
```

Monitoring the startup configuration

To monitor the startup configuration, run the following command:

```
RT1#show startup-config (or sh start)
```

Deleting the startup configuration

Upon reboot, a router starts in setup mode if no startup configuration exists in NVRAM. You can manually delete the startup configuration from NVRAM. This allows you to start a new configuration from scratch. This is typically a last-resort troubleshooting method: When problems affect the router and no troubleshooting method fixes the problems, your last resort is to reset the router and reconfigure it.

It is best practice to back up the startup configuration to a backup computer host before deleting it. You find out how to back up the configuration to a backup computer host in the section “Back up the router running configuration to a computer host,” later in this chapter.

To delete the startup configuration, run the following command:

```
RT1>enable (or en)
RT1#erase startup-config
Erasing the nvram filesystem removes all configuration files!
Continue? [confirm] <press Enter to confirm>
[OK]
Erase of nvram: complete
RT1#
```

Observe that the `erase` command warns you that the NVRAM contents will be reinitialized and prompts you to confirm. The default answer is `confirm`. To confirm, simply press Enter.

Router configuration backup and recovery best practice

It is best practice to save the running configuration to both

- ◆ The startup configuration file in NVRAM on the router itself
- ◆ To a computer host

This protects you against a total failure of the router. If the router fails and you need to replace it with a new one, you don't want to have to re-create the startup configuration from scratch. If you have that configuration saved on a computer host, you can load the startup configuration from the computer host and onto the new router, and you're ready to go in production with the new router.

Back up the router running configuration to a computer host

To back up the running configuration to a computer host, run the following command:

```
RT1>enable (or en)
RT1#copy running-config tftp (or copy run tftp)
Address or name of remote host []? 192.168.75.5
Destination filename [RT1-config]? <press Enter>
812 bytes copied in 0.910 secs (892 bytes/sec)
RT1#
```

The `copy running-config tftp` Cisco IOS command on the second line initiates the copy process of the router running configuration to a TFTP server.

The third line prompts you for the IP address or host name of the remote host destination. Observe that the IOS does offer a suggested IP address or host name. You can configure a default TFTP server. The IP address or host name of that default TFTP server then shows up as a suggestion in line 3.

The fourth line prompts you for the filename you want to give to the configuration file saved on the remote host. The router name, followed by the suffix `-config`, is suggested by default. You simply press Enter to accept the suggested filename.

Now your running configuration is saved in a file named `RT1-config` on the remote computer host with IP address 192.168.75.5.

Recover a router configuration from a computer host

Suppose that you need to load a configuration from a remote host to your router. The same `copy` Cisco IOS command allows you to recover a configuration from a remote host:

```
RT1>enable (or en)
RT1#copy tftp running-config (or copy tftp run)
Address or name of remote host []? 192.168.75.5
Source filename []? RT1-config
Destination filename [running-config]? <press Enter>
Accessing tftp://192.168.75.5/RT1-config...
Loading RT1-config from 192.168.75.5
[OK - 812 bytes]
812 bytes copied in 10.120 secs (80 bytes/sec)
RT1#
```

The `copy tftp running-config` Cisco IOS command on the second line initiates the copy process of the router running configuration from a TFTP server.

The third line prompts you for the IP address or host name of the remote host destination. Observe that, in this example, the IOS does not suggest any source IP address or hostname “[]”. You can configure a default TFTP server on your router. The IP address or hostname of that default TFTP server will then show up suggested between the square brackets.

The fourth line prompts you for the source filename of the configuration file that you want to load from the remote host. Enter the name of a configuration file that you saved previously on the TFTP server. In this example, you enter the name of the configuration you just copied to the TFTP server in the previous example (“RT1-config”).

The fifth line prompts you for the destination filename. The `running-config` filename is suggested. This means that the configuration you load from the TFTP server will replace the current running configuration. Press Enter to accept the suggested choice.

Next, the `copy` command displays a few status messages.

At this point, your running configuration has been loaded from a file named `RT1-config` from a remote TFTP server host with IP address 192.168.75.5.

Managing router configurations using the Cisco IOS File System (IFS)

This section shows how to manage the memory of a Cisco router using Cisco IOS File System (IFS) commands.

Know that you can manage the memory of a Cisco router like a file system on a computer host. The Cisco IFS presents the memory of a Cisco router as directories (or folders) and files within those directories, just like Microsoft Windows, Apple Mac OS X, Linux, or any other computer operating system presents the hard drive of a computer host as directories (or folders) and files.

The Cisco IFS commands are only available in privileged mode. So, you need to run the `enable` command first (or `en` in its short form).

First, verify the current directory:

```
RT1>enable (or en)
RT1#pwd
flash:
```

You are currently in the flash main memory directory, as shown by the `pwd` command. Next, run the `dir` Cisco IFS command to see the contents of flash memory on your router:

```
RT1#dir
Directory of flash:/
 1  -rw-  15572992 <no date>  c2600-ik9o3s3-mz.123-1a.bin
16777216 bytes total (1204160 bytes free)
```

This shows that the flash memory on your router contains a single Cisco IOS image named `c2600-ik9o3s3-mz.123-1a.bin`.

You can easily find other directories and files by using the `dir all-filefilesystems` Cisco IFS command:

```
RT1#dir all-filefilesystems
Directory of nvram:/
27  -rw-   0          <no date>  startup-config
28  ----   0          <no date>  private-config

29688 bytes total (29636 bytes free)

Directory of system:/
10  drwx   0          <no date>  its
 2  dr-x   0          <no date>  memory
 1  -rw-  582        <no date>  running-config
 9  dr-x   0          <no date>  vfiles

No space information available
Directory of flash:/
 1  -rw-  15572992  <no date>  c2600-ik9o3s3-mz.123-1a.bin

16777216 bytes total (1204160 bytes free)
```

Observe that you have three main directories (file systems) on your Cisco router:

- ◆ **nvram:** Stores the `startup-config` and the `private-config` files.
- ◆ **system:** This is the RAM, which contains the `running-config` file.
- ◆ **flash:** This is the flash memory, which contains the Cisco IOS operating system image. This is the Cisco IOS image that the bootstrap program loads in RAM when the router boots up.

You can list the contents of any of these main directories (file systems) individually using the `dir` and `cd` Cisco IFS commands. You can change your working directory from `flash:` to any of the main directories using the `cd` Cisco IFS command.

For example, list the contents of NVRAM:

```
RT1#dir nvram:
Directory of nvram:/
 27  -rw-   0          <no date>  startup-config
 28  ----   0          <no date>  private-config

29688 bytes total (29636 bytes free)
```

Now, change to the RAM directory (`system`) and look at the files and directories available there:

```
RT1#cd system:
RT1#dir
Directory of system:/
 10  drwx   0   <no date>   its
   2  dr-x   0   <no date>   memory
   1  -rw-  582 <no date>   running-config
   9  dr-x   0   <no date>   vfiles
```

Observe the `running-config` file. This is the current running configuration. You can copy a configuration file from a computer host to `system:/running-config` to load a configuration on the router from a configuration backup file on a computer host.

To load a configuration on the router from a configuration backup file on a computer host, run the following Cisco IFS commands:

```
RT1#copy tftp://192.168.75.5/RT1-config system:/running-config
Destination filename [running-config]? <press Enter>
Accessing tftp://192.168.75.5/RT1-config...
Loading RT1-config from 192.168.75.5
[OK - 812 bytes]
812 bytes copied in 10.120 secs (80 bytes/sec)
RT1#
```

The `copy tftp://192.168.75.5/RT1-config system:/running-config` command you use here is very similar to the `copy tftp running-config` command that you used in the previous section. The only difference is that you specify the path to the source and the path to the destination when you use the Cisco IFS version of the `copy` command.

You can also use this command to copy a configuration from a configuration backup file on a computer host to the `startup-config` file in NVRAM. Here is an example:

```
RT1#copy tftp://192.168.75.5/RT1-config nvram:/startup-config
Destination filename [startup-config]? <press Enter>
Accessing tftp://192.168.75.5/RT1-config...
Loading RT1-config from 192.168.75.5
[OK - 812 bytes]
812 bytes copied in 10.120 secs (80 bytes/sec)
```

Managing Cisco Router Authentication

You can configure several passwords for different types of access to your router:

- ◆ **Console password:** Used for console access through the console port or through a Console Terminal Server.
- ◆ **Auxiliary password:** Used for console access through the auxiliary port using a modem.
- ◆ **VTY lines password:** Virtual type terminal (VTY) lines are used for Telnet and Secure Shell (SSH) access. They are called virtual type terminal lines because no physical terminal is connected to the router. Instead, you connect a computer host to the network and access the router remotely using the router management IP address. A terminal emulation program on the computer host emulates a physical terminal (TTY).
- ◆ **Privileged password:** Used for privileged mode access. Privileged mode is an “expert” management operation mode used to run some Cisco IOS commands.

The console port and the auxiliary port are enabled by default, even if no password is specified for them. This is a security risk. It is best practice to specify at least a console password on new Cisco devices.

Privileged EXEC mode is *not* secured with a password by default on Cisco routers. By default, you can access privileged mode by executing the `enable` IOS command at the user EXEC prompt. It is best practice to configure a privileged mode password to secure access to advanced IOS commands that can adversely affect the functionality of the router, if misused.

The VTY lines (Telnet and Secure Shell) are disabled by default. You need to specify a password for the VTY lines to enable them.

To configure passwords, you need to instruct the Cisco device to prompt for authentication. You use the `login` Cisco IOS command to do this.

Console password

This section reviews how to configure a console password. To configure the console password, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#line console 0 (or line con 0)
RT1(config-line)#password my_password
RT1(config-line)#login
RT1(config-line)#exit
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `line console 0` command selects the console line. Cisco devices have only one console line: console 0.

The `password my_password` command sets the `my_password` password on the console access line.

Finally, you instruct the Cisco router to prompt for authentication by entering the `login` Cisco IOS command. From now on, anytime you connect to the console line, you will be prompted to provide a password. The password you provide must be `my_password`. To disable the authentication prompt, issue `line console 0` again and enter the `no login` command.

You use the `exit` commands to exit the config-line mode and to exit the config global configuration mode.

Telnet password

This section reviews how to configure a password for the VTY access lines. To configure a password for the VTY lines, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)# line vty 0 ?
    <0-4> last line number
RT1(config-line)#line vty 0-4
RT1(config-line)#password my_telnet_password
RT1(config-line)#login
RT1(config-line)#exit
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `line vty 0 ?` command asks the Cisco IOS how many VTY lines are available. The response (`<0-4> last line number`) shows that five VTY lines are available on this particular router. Now you can configure a password on any one of the VTY lines (by selecting that particular line) or on all VTY lines (by selecting the whole 0–15 line range).

The `line vty 0-4` command selects the whole 0–4 VTY line range. Cisco routers have several VTY *access lines*. Older routers have only five VTY

lines. Newer routers have as many as 1,180 VTY lines. It is best practice to query the Cisco IOS about how many VTY lines are available.

Two main reasons exist to have several VTY access lines on a Cisco router:

- ◆ **Allowing you to connect to the router and connect to another device from the router.** Two VTY lines are needed in this case: one to connect into the router and another one to connect out of the router to another device.
- ◆ **Allowing several administrators to work on the router.** In large networks, more than one administrator may manage the network. More than one administrator may need to connect from a remote location to the same router using Telnet or SSH. This is typical with large core routers.

The password `my_telnet_password` command sets `my_telnet_password` on the VTY access lines. You can set a different password on each line. However, this is not recommended. You don't know which VTY line you are on when you log in, so you wouldn't know which password to enter. Best practice is to select the whole range of VTY lines and to set the same password on all of them.

Finally, instruct the Cisco router to prompt for authentication by entering the `login` Cisco IOS command. From now on, anytime you connect to any of the VTY lines, you will be prompted to provide a password. The password you provide must be `my_telnet_password`. To disable the authentication prompt, issue `line vty 0-15` again and enter the `no login` command.

Auxiliary password

If your router has an auxiliary port, it is best practice to secure access to the auxiliary port using a password. To configure the auxiliary password, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#line auxiliary 0 (or line aux 0)
RT1(config-line)#password my_aux_password
RT1(config-line)#login
RT1(config-line)#exit
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `line console 0` command selects the console line. Cisco routers have only one console line: console 0.

The `password my_password` command sets the `my_password` password on the console access line.

Finally, instruct the Cisco router to prompt for authentication by entering the `login` Cisco IOS command. From now on, anytime you connect to the console line, you will be prompted to provide a password. The password you provide must be `my_password`. To disable the authentication prompt, issue `line console 0` again and enter the `no login` command.

You use the `exit` commands to exit the `config-line` mode and to exit the `config` global configuration mode.

Privileged password

It is best practice to set up a privileged password to secure access to advanced IOS commands that can adversely affect the functionality of the router if misused. You can use two different commands to configure a privileged password:

- ◆ `enable password my_priv_password`: This command sets `my_priv_password` as the privileged password. This password is not encrypted by default. This command is supported in all IOS versions.
- ◆ `enable secret my_priv_encrypt_password`: This command sets `my_priv_encrypt_password` as the privileged password. This password is encrypted. This command is supported in newer IOS versions.

Using the `enable secret` or the `enable password` commands, you configure a privileged password that is stored locally on your router. The only difference between the two commands is that `enable secret` stores the password on the router in encrypted form, which is more secure than `enable password`, which stores the password on the router in unencrypted form.

Always use the Cisco IOS help to determine whether the `enable secret` command is available. If it is, use it to set the privileged password. It is best practice to encrypt the privileged password using the `enable secret` command whenever this command is available.

You can also configure your privileged password to be stored on a *Terminal Access Controller Access Control System (TACACS)* server. This is a good option in larger networks with many routers when it is better to configure

the privileged password once, centrally, on a TACACS server, instead of configuring passwords on each of your routers.

To configure an encrypted privileged mode password, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#enable secret my_priv_encrypt_password
RT1(config)#exit
RT1#disable
RT1>
```

Encrypting passwords

By default, passwords are stored in plain text in the running configuration in RAM and in the startup configuration file in NVRAM. You can view the passwords on your router in plain text, using either the `show running-config` command or the `show startup-config` command. This is a security risk. It is best practice to encrypt all passwords on your router.

The privileged password is encrypted if you use the `enable secret` command. It is best practice to set a privileged password using the `enable secret` command to make sure that it is encrypted. So, if you use `enable secret` instead of `enable password` to set a privileged password, your privileged password is encrypted.

How about other passwords? Console, auxiliary, and Telnet (VTY) passwords are *not* encrypted, even if you use the `enable secret` command for the privileged password. You need to encrypt them using the `service password-encryption` command.

To encrypt passwords on your router, run the following commands:

```
RT1>enable (or en)
RT1#configure terminal (or config t)
RT1(config)#service password-encryption
RT1(config)#exit
RT1#disable
RT1>
```

The first two commands (`enable` and `configure terminal`) set the IOS in privileged global configuration mode. You can now run commands that configure global router settings, that is, settings that apply to the whole router.

The `service password-encryption` command asks the Cisco IOS to encrypt all passwords except the privileged password that is already encrypted if the `enable secret` command was used.

Enabling Secure Shell (SSH)

Secure Shell (SSH) is similar to Telnet: It allows remote users to connect to the router by using the router IP address. SSH is more secure than Telnet, because it encrypts data exchanged between the remote management computer and the router.

It is best practice to encrypt data exchanged between the remote management computer and the router.

Consider this example: You need to change the passwords on a router located in a remote data center. The data center is too far to walk to, so you need to connect to the router remotely from your computer. While changing the passwords, you enter the passwords on the keyboard of your computer. If you are connected to the router using Telnet, the data exchanged between your computer and the router is in clear text. That data includes the new passwords that you type at your computer keyboard. Hence, passwords are sent over the Internet in clear text. This is a security risk. SSH avoids this security risk by encrypting data exchanged between your computer and the router.

SSH uses encryption keys to encrypt the data exchanged in an SSH session. Cisco supports both SSH version 1.0 (also known as SSH v1 or SSH.1) and SSH version 2.0 (also known as SSH v2 or SSH.2). Cisco started to support SSH v2 with IOS Release 12.1(19)E on some router models.

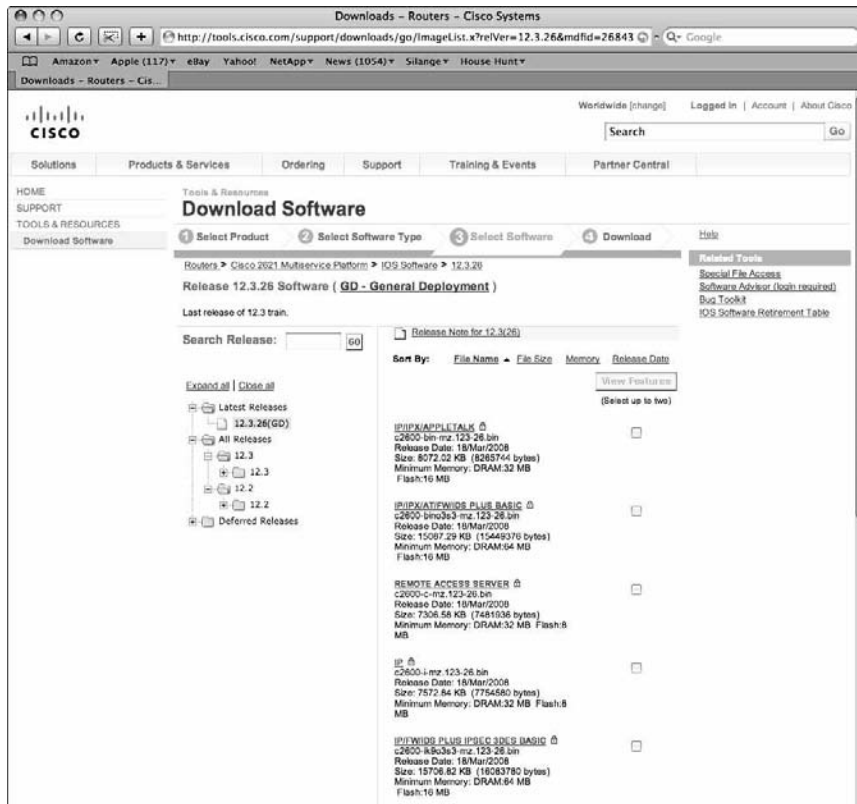
If you get a `%Invalid input` error when you execute the `crypto key generate rsa` command, the Cisco IOS version on your router does not support SSH. You may need to download the cryptographic software image from Cisco. To download the cryptographic IOS software image for your router, log in to www.cisco.com/public/sw-center/index.shtml. Note that you need to register at Cisco.com before downloading. Some software export limitations may apply.

Figure 2-9 shows the Cisco 2621 series router software download section at Cisco.com.

Observe that various packages are available for each release. Each package enables certain features for typical usages of the router. You choose the IOS image that corresponds to your needs. For example:

- ◆ **IP/IPX/APPLETALK:** You choose this Cisco IOS image if you use your 2621 router to route data for IP, IPX, or AppleTalk network protocols. If you do not have any computer hosts using the NetWare IPX protocol and if you do not have any hosts using the AppleTalk protocol, it wouldn't make sense to use this image, because enabling support for more protocols than necessary slows your router.

Figure 2-9:
Down-
loading
Cisco 2621
router IOS
images.



- ◆ **IP:** You choose this Cisco IOS image if all computer hosts in your network are using the Internet Protocol. Contrary to the previous IOS image, which enabled support for IP, IPX, and AppleTalk, this image only enables IP. If all your hosts are using IP, this is the image you want.

Scrolling down the list, you find images that enable encryption. You need to download and install one of those encryption-enabled IOS images.

To enable SSH, you need to

- ◆ Ensure that the Cisco IOS image on your router supports SSH.
- ◆ Ensure that you assigned a host name to your router: SSH needs the host name to generate the encryption keys.
- ◆ Ensure that you assigned an IP domain name to your router: SSH needs the IP domain name to generate the encryption keys.
- ◆ Create a local or TACACS administrator user and assign it a password: SSH cannot use the Telnet password that you assigned to the VTY

access lines. You need to create a specific user that will be used to authenticate SSH sessions.

- ◆ Create the encryption keys.
- ◆ Configure SSH options such as session timeout and number of login retries.
- ◆ Enable SSH on the VTY lines of your router.

Recovering router passwords

The Cisco IOS provides a mechanism to recover passwords, in case you lost them or you do not remember them.

You need to have physical access to the router to connect to its console port. This is a good thing, because you don't want anyone else connecting from a remote location through Telnet to be able to reset the passwords on your routers.

The key point of the password recovery process is to boot up the Cisco router ignoring its current startup configuration, which contains the current passwords. To boot up the Cisco router ignoring its current startup configuration you need to change the value in the configuration register. You can set bit 6 in the configuration register to instruct the bootstrap program to avoid reading the startup configuration from NVRAM. By doing this, you boot up the router as if it had no startup configuration — as if the router were new, coming out of the box.

Password recovery process

Follow these steps to recover passwords on a Cisco router:

- 1. Change the configuration register to 0x2142.**
- 2. Reboot the router.**
- 3. Upon reboot, exit from setup mode.**

The router ignores the startup configuration in NVRAM, so it automatically starts in setup mode. You need to exit setup mode because your router is already set up. You just want to reset the passwords in the current startup configuration, not to reset the whole configuration.

- 4. Enable privileged EXEC mode.**
- 5. Load the startup configuration manually from NVRAM to RAM.**
- 6. Enable global configuration mode.**
- 7. Change the passwords.**
- 8. Save the running configuration over the startup configuration in NVRAM.**
- 9. Change the configuration register back to the default value of 0x2102.**
- 10. Reboot the router.**

Prep Test

- 1 What is the Cisco IOS (Internetwork Operating System)?**
 - A ☐ Cisco's proprietary router graphical user interface
 - B ☐ Cisco's proprietary router operating system
 - C ☐ Cisco's proprietary router console facility
 - D ☐ All of the above
- 2 Name some of the graphical user interface(s) that you can use to manage a Cisco router.**
 - A ☐ Cisco Network Assistant (CNA)
 - B ☐ Cisco Router and Security Device Manager (SDM)
 - C ☐ Cisco Router and Security Device Manager (SDM) Express
 - D ☐ All of the above
- 3 What is the main purpose of the ROM Monitor microprogram, also known as ROMMON?**
 - A ☐ To maintain, test, and troubleshoot the power consumption of a Cisco device
 - B ☐ To maintain, test, and troubleshoot the console port of a Cisco device
 - C ☐ To maintain, test, and troubleshoot the configuration stored in ROM and in the flash memory of a Cisco device
 - D ☐ To maintain, test, and troubleshoot the ROM port of a Cisco device
- 4 When does the power-on self test (POST) run?**
 - A ☐ Immediately after the Cisco IOS loads on a router
 - B ☐ Immediately after the startup configuration loads on a router
 - C ☐ Immediately after the startup configuration loads on a router
 - D ☐ Immediately after a Cisco router is powered up
- 5 What is the main purpose of the bootstrap program, also known as the boot loader?**
 - A ☐ To bring up a Cisco router by loading the startup configuration from flash memory to RAM
 - B ☐ To bring up a Cisco router by loading the Cisco IOS from flash memory to RAM
 - C ☐ To bring up a Cisco router by loading the running configuration from flash memory to RAM
 - D ☐ To bring up a Cisco router by loading the Cisco Device Manager from flash memory to RAM

- 6** It is best practice to use entry-level routers, such as the Cisco 2600 series or the Cisco 2800 series, at what layer(s)?
- A ☐ Access and distribution layer
 - B ☐ Distribution and core layer
 - C ☐ Core layer
 - D ☐ Access and core layer
- 7** What does the flash memory on a Cisco router store?
- A ☐ The startup configuration of a Cisco router
 - B ☐ The image file of the Cisco IOS operating system
 - C ☐ The Cisco Device Manager software application
 - D ☐ All of the above
- 8** On Cisco routers, where is the running configuration loaded from?
- A ☐ The running configuration file during startup
 - B ☐ Cisco's Web site during startup
 - C ☐ The startup configuration file during startup
 - D ☐ All of the above
- 9** The Cisco IOS command-line interface operates in setup mode to do which of the following?
- A ☐ Initially configure the ROM Monitor (ROMMON) microprogram
 - B ☐ Initially configure the Device Manager software application
 - C ☐ Initially configure the IOS
 - D ☐ Initially configure the router
- 10** The Cisco IOS command-line interface operates in privileged configuration mode to do which of the following?
- A ☐ Configure the ROM Monitor (ROMMON) microprogram
 - B ☐ Configure the Device Manager software application
 - C ☐ Configure the IOS
 - D ☐ Configure the router
- 11** You can connect locally to your router to manage it using the _____ port.
- A ☐ Fast Ethernet 24 (fa0/24)
 - B ☐ console
 - C ☐ auxiliary
 - D ☐ Fast Ethernet 0 (fa0/0)

Answers

- 1** B. Cisco's proprietary router operating system. The Cisco IOS (Internetworking Operating System) is Cisco's proprietary switch and router operating system. Review the chapter introduction.
- 2** D. All of the above. Some of the Graphical User Interfaces that you can use to manage a Cisco router are the Cisco Network Assistant (CNA), the Cisco Router and Security Device Manager (SDM), and the Cisco Router and Security Device Manager (SDM) Express edition. Review the chapter introduction.
- 3** C. Maintain, test, and troubleshoot the configuration stored in ROM and in the flash memory of a Cisco device. The ROM monitor micro-program, also known as ROMMON, is used to maintain, test and troubleshoot the configuration stored in ROM and in the Flash memory of a Cisco device. Check *"Cisco router startup process"* and *"Managing Cisco Router Configuration."*
- 4** D. Immediately after a Cisco router is powered up. The Power-On-Self-Test runs immediately after a Cisco router is powered up. Review *"Cisco router startup process."*
- 5** B. Bring up a Cisco router by loading the Cisco IOS from flash memory to RAM. The main purpose of the bootstrap program, also known as the boot loader, is to bring up a Cisco router by loading the Cisco IOS from Flash memory to RAM. See *"Cisco router startup process."*
- 6** A. Access and distribution layer. It is best practice to use entry-level routers, such as the Cisco 2600 series or the Cisco 2800 series at the access and distribution layers. Review *"Best Practice For Using Cisco Routers."*
- 7** D. All of the above. The flash memory on a Cisco router stores the startup configuration of the router, the image file of the Cisco IOS operating system, and the Cisco Device Manager software application program. See *"Cisco router startup process."*
- 8** C. Is loaded from the startup configuration file during startup. The running configuration of a Cisco router is loaded from the startup configuration file during startup. Review *"Cisco router startup process."*
- 9** D. Initially configure the router. The Cisco IOS command line interface operates in setup mode to initially configure the router. Review *"Initial router configuration."*
- 10** D. Configure the router. The Cisco IOS command line interface operates in privileged configuration mode to configure the router. Review *"Managing Cisco Router Authentication."*
- 11** B. Console. You can connect locally to your router to manage it using the console port. Check *"Connecting to a Cisco Router."*

Chapter 3: Network Routing

Exam Objectives

- ✓ Describing the types of network routes and knowing when to use them
- ✓ Describing routing and routed protocols, their characteristics, and purpose
- ✓ Describing routing decision criteria
- ✓ Distinguishing distance vector routing from link-state routing
- ✓ Describing route updates and convergence
- ✓ Describing routing administrative distance
- ✓ Describing common routing protocol metrics
- ✓ Describing the general process to enable and configure a routing protocol

Read this chapter to find out about Layer 3 routing. Routers route data packets between networks. Routers do the following:

- ◆ Manage routing protocols
- ◆ Build routing tables using routing protocols
- ◆ Route packets using routed protocols and routing tables
- ◆ Maintain routing tables

Introducing Network Routes

A *network route* is a data transmission path through one or more networks between two end nodes. The end nodes can be any computer device that supports IP connectivity, such as computer hosts, IP phones, digital video consoles, and smartphones.

More than one route can exist between two end nodes. The main purpose of a router is to find the best route to reach a destination node. The best route is calculated according to *route metrics*: the cost in time and resources to send a data packet over that route.

More than one router can exist in the data transmission path between the sending and the receiving nodes. For example, when you connect to an

Internet Web site from your home computer, your computer sends data packets to your home router. Your home router routes those packets to the default outbound gateway of your Internet service provider. The default outbound gateway of your Internet service provider, also a router, sends your data packets to the network of the Internet Web site. In this example, at least three routers are involved:

- ◆ Your home router
- ◆ Your Internet service provider's router
- ◆ The inbound router of the Internet Web site

You find three types of network routes:

- ◆ Static routes
- ◆ Default routes
- ◆ Dynamic routes

Static routes

You define static routes manually on a router. Static routes are best suited for small networks, such as LANs, where routes rarely change. If routes change, you need to update your routes to reflect the new data transmission paths.

Advantages

Some of the advantages of using static routes are as follows:

- ◆ **Routing efficiency:** By defining static routes, you can leave the routing protocols disabled on your router. This saves some bandwidth. Dynamic routing requires routing protocols to be enabled. Routing protocols consume some bandwidth because they constantly send route update packets between routers.
- ◆ **Security:** In some cases, you may want to define static routes to control the data transmission paths used by your data. This may be useful in highly secure environments. Keep the following in mind though:
 - You can filter routing data using firewalls at the network perimeter.
 - You can use Virtual Private Networking (VPN) to secure your data transmissions, no matter which data path they travel on.

Hence, you can mitigate security risks involving dynamic routes using either firewalls or VPN or both. You read about firewalls and VPN in Book VI.

Disadvantages

Some of the disadvantages of using static routes are as follows:

- ◆ **Maintenance:** If routes change, you need to update your routes to reflect the new data transmission paths. This adds some management overhead.
- ◆ **Accuracy:** If your network changes and you do not update the static routes, your router does not have an accurate knowledge of your network. This can result in lost or delayed data transmissions.
- ◆ **Scalability:** Large networks have hundreds, even thousands, of alternate routes to reach other networks. It is practically impossible to define all these routes statically. Even if you define all alternate routes statically, as soon as a change occurs in the overall network topology, you would need to update the static routes. This is a maintenance nightmare. Hence, static routes are best suited for small networks.

Configuring static routes

You can configure static routes using the `ip route` Cisco IOS command in global configuration mode. The syntax of this command is as follows:

```
ip route dest-ip subnet {next-hop-ip | interface}
```

- ◆ `dest_ip`: This is the IP address of the destination network. You are registering a static route to the destination network.
- ◆ `subnet`: This is the IP subnet mask of the destination network that defines which part of the IP address identifies the network and which part identifies the hosts in that network.
- ◆ `{next-hop | interface}`: This is the IP gateway (router) through which you reach out to the destination network. You have to specify either the IP address of the next hop on the route to the destination network, or the outbound interface on your router through which the router can reach the destination network.



The `{}` notation means that you must specify something. The `|` (pipe) sign means that you need to choose either one of those options. Think of the `|` (pipe) sign as an “or.” Think of the `{}` notation as a “must.”

To remove a static route, you can use the usual `no` prefix with the `ip route` command: `no ip route dest-ip [subnet] {next-hop-ip | interface}`

Here is an example:

```
RT6751>enable (or en)
RT6751#configure terminal (or config t)
RT6751 (config)#ip route 192.168.25.0 255.255.255.0 serial 0/1
RT6751 (config)#exit
RT6751#disable
RT6751>
```

In this example, you define a static route on router RT6751 to network 192.168.25.0 through serial interface 0/1.

Default routes

Default routes are static routes that you define for packets bound to a destination network that is not found in any of the routing tables on the router. Whenever the router receives packets bound to a network the router doesn't know, it sends the packet out on the default route.

It is best practice to define a default route to ensure that data packets bound for networks unknown to your router are forwarded to a default gateway.

Default routes are related to default gateways: A default route is a data transmission path to the default outbound gateway in a network. For example, in a LAN with network IP address 192.168.25.0, the default gateway is typically 192.168.25.1. The default route is the data transmission path that reaches 192.168.25.1, the default gateway.

Configuring default routes

You configure default routes using the same `ip route` Cisco IOS command in global configuration mode. However, the IP address and the subnet mask of the destination network are 0.0.0.0. Here is an example:

```
RT6751>enable (or en)
RT6751#configure terminal (or config t)
RT6751 (config)#ip route 0.0.0.0 0.0.0.0 serial 0/0
RT6751 (config)#exit
RT6751#disable
RT6751>
```

In this example, you define a default route on router RT6751 to outbound serial interface 0/0. Router RT6751 now sends data packets bound for unknown networks out on serial interface 0/0.

You can also use the IP address of the default gateway to configure a default route, as shown here:

```
RT6751>enable (or en)
RT6751#configure terminal (or config t)
RT6751 (config)#ip route 0.0.0.0 0.0.0.0 192.168.67.1
RT6751 (config)#exit
RT6751#disable
RT6751>
```

In this example, you define a default route on router RT6751 to outbound IP address 192.168.67.1. Router RT6751 now sends data packets bound for unknown networks out to the default gateway of network 192.168.67.0.

Dynamic routes

Dynamic routes are routes that change over time. Routing protocols define and maintain dynamic routes. Routes change due to the following:

- ◆ Network topology updates
- ◆ Network traffic updates
- ◆ Available bandwidth
- ◆ Link state

Some of the advantages of using dynamic routes are as follows:

- ◆ **Low maintenance:** You do not need to update your routes whenever data transmission paths change when using dynamic routing. Routes are automatically updated by routing protocols that exchange route update packets. All you need to do is to configure routing protocols on your router.
- ◆ **Accuracy:** Routing protocols keep track of network changes. This improves routing accuracy because routers send packets over the best routes available at any time.
- ◆ **Scalability:** Large networks have hundreds, even thousands, of alternate routes to reach other networks. It is practically impossible to define all these routes statically. Even if you define all alternate routes statically, as soon as a change occurs in the overall network topology, you would need to update the static routes. This is a maintenance nightmare. Dynamic routing avoids this problem by using routing protocols to allow routers to communicate about routes they know, new routes they discover, and routes that became unavailable or overloaded. Thus, networks using dynamic routing can scale out much better than networks that solely use static routes.

Disadvantages

Overhead is a disadvantage of using static routes. Dynamic routing protocols consume some bandwidth because they constantly send route update packets between routers.

Configuring dynamic routes

You configure dynamic routes using routing protocols.

Routing Protocols

Routing protocols exchange network, routes, and metric information between routers to help find optimal routes as fast as possible. Routers use the information provided by routing protocols to build their *routing tables* for each

routed protocol to keep track of networks, paths to networks, and *metrics* associated with each route.

Several routing protocols exist. Most routers support more than one routing protocol. Several routing protocols can be simultaneously enabled on a router. Routing protocols do not interfere and do not communicate with each other.

The most widely used routing protocols, and the ones you need to know for the test, are as follows:

- ◆ Routing Information Protocol (RIP); see Chapter 4
- ◆ Enhanced Interior Gateway Routing Protocol (EIGRP); see Chapter 5
- ◆ Open Shortest Path First (OSPF); see Chapter 6

Routed Protocols

Routed protocols tag each data packet with source and destination hierarchical addresses to allow the routing of data packets through networks as needed. Routed protocols also assign a unique logical address to each node in the network to identify each source and each destination in the network.

Here are some routed protocols that you may encounter in the field:

- ◆ Internet Protocol version 4 (IPv4, commonly referred to as just IP)
- ◆ Internet Protocol version 6 (IPv6)
- ◆ AppleTalk
- ◆ Novell Netware Internetwork Packet Exchange (IPX)

Routing Decision Criteria

Routers may pick different network routes to a destination for a given packet depending on various decision criteria. Some routes may be deemed faster than by others by different routing protocols. Routers keep separate routing tables for each protocol. A route that is best now may not be best in a few minutes, depending on various criteria such as traffic, available bandwidth, and link state. Routers adapt to changes in traffic, available bandwidth, and link state by constantly monitoring the state of each route they know.

Routing tables keep track of networks, paths to networks, and metrics associated with each route.

Routers consider two aspects when deciding which network routes are best at a given moment:

- ◆ **Administrative distance:** How reliable is the information source that provided the data about the network route?
- ◆ **Routing protocol metrics:** What are the costs associated with each network route?

Administrative distance

The administrative distance determines the reliability of the information source that provided the data about the network route. Routers learn about network routes using various methods:

- ◆ **Router connects directly to a network.** The router learns about the network firsthand, because it connects to it.
- ◆ **Router does not connect to the network, but a static route exists to that network.** The router does not “see” the network, but it’s been informed about its existence by a fairly reliable source (the static route).
- ◆ **Router is connected indirectly, through other router(s), to a network.** The router does not “see” the network, but it “heard” about it from another router.

Routers trust routes according to how reliable the source of information is. A router always prefers routes learned from reliable information sources. Cisco defined the concept of administrative distance to measure this trust. Various sources get different administrative distance values, as shown in Table 3-1.

Table 3-1 Administrative Distances	
<i>Routing Information Source</i>	<i>Administrative Distance</i>
Directly connected	0
Static route	1
EIGRP (internal)	90
OSPF	110
RIP (v1 and v2)	120
EIGRP (external)	170

Routers prefer sources with lower administrative distances. In other words, a router trusts a static route more than a route learned from OSPF. On the other hand, a router trusts a route learned from OSPF more than it trusts a route learned from RIP.

If the same routing protocol finds two different routes to the same destination, the administrative distance is the same. In this case, other *metrics* are considered to decide on which route to use.

Routing protocol metrics

You read that routers may pick different network routes to a destination for a given packet depending on various decision criteria, such as traffic, available bandwidth, and link state.

Each routing protocol calculates the efficiency (the cost) of a route differently. Hence, decision differences may exist. For example, considering two different routes to the same destination, route A and route B, OSPF may find that route A is better than route B. However, RIP may find that route B is better than route A. So which route does the router choose? Route A or route B? If you answered route A, you are right: Whenever routing protocols contradict each other, the one with the lowest administrative distance is preferred. However, what if the same routing protocol finds two (or more) routes to the same destination? How would the routing protocol choose one of the routes? By using specific decision criteria to evaluate the quality of each route.

Routing decision criteria are quantified by measurements, or metrics. Each routing protocol uses some metrics to determine the quality, or efficiency, or cost of a certain network route.

I now look at the various metrics that routing protocols consider when calculating the cost of a given route.

Hop count

The hop count is the number of routers that need to be traversed to get to the destination network. Routing protocols prefer routes with fewer hops because a certain delay is always involved at every hop to route the packet between network segments.



Think of flying: For the same cost, most people prefer flights with fewer stops, because time is wasted at every stop.

RIP uses the hop-count metric to choose network routes. RIP prefers routes with fewer hops.

Bandwidth

Bandwidth is the throughput of the network route to the destination. Bandwidth is typically measured in bits per second (bps). Routing protocols prefer routes with larger bandwidth because it is very likely that packets reach the destination faster. This is not a guarantee though. For example, if a large-bandwidth route suddenly becomes congested, routers start sending on alternate routes.



Think of driving: For a comparable distance, most people prefer driving on a freeway because it has more lanes and higher speed limits than a normal road, and no street crossings. However, freeways are not always faster — just ask anyone stuck in rush-hour traffic.

EIGRP uses the bandwidth metric to pick network routes. EIGRP prefers routes with larger bandwidth.

Delay

Delay is the time it takes a data packet to reach the destination. Total delay is calculated based on the following:

- ◆ **Processing delay:** The time routers need to inspect the destination of the data packet
- ◆ **Queuing delay:** The time a packet sits in the inbound or outbound queue of the router before being processed or before being sent to the next hop
- ◆ **Transmission delay:** The time it takes to send the packet onto the link to the next hop
- ◆ **Propagation delay:** The time the signal takes to propagate through the transmission media

EIGRP uses the delay metric to pick network routes. EIGRP prefers routes with shorter delay.

Reliability

Reliability is the percentage of time the route is available.

EIGRP considers the reliability metric to pick network routes. EIGRP prefers routes with higher reliability.

Load

Load measures the bandwidth consumed by current traffic on a given route. Load is the difference between the total bandwidth and the available bandwidth of the route.

EIGRP considers the load metric to pick network routes. EIGRP prefers routes with lower load.

Maximum transmission unit (MTU)

MTU is the size, in bytes, of each data packet. Each network route has a certain MTU value. The higher the MTU, the more data can be transferred at once.

EIGRP considers the MTU metric to pick network routes. EIGRP prefers routes with higher MTU.

Cost

Cost is calculated based on the bandwidth of a network route. Cost is $10^8/\text{bandwidth}$.

The OSPF protocol considers the cost metric to pick network routes. OSPF prefers routes with lower cost.

Routing Methods

Routing protocols exchange network, route, and metric information between routers to help routers build their routing tables. Earlier you saw that routing protocols use different metrics to evaluate the quality of a route. Routing protocols also use different methods to exchange information about network routes.

Distance vector routing

Some routing protocols use the distance to a network to evaluate the quality of a network route. Shorter routes (routes with fewer hops) are considered better than longer routes.

Routers using these protocols build their routing tables based on route distance, and they exchange and combine their routing table with their neighbors. Neighbor routers trust each other's route information, and they relay the combined information farther. These protocols are using *distance vector routing*.

Distance vector routing is also known as *rumor routing*, because routers "hear" about routes from their neighbors and they relay this information to other neighbor routers. Routing tables are combined and relayed to all routers in the network.

Convergence

The initial routing information exchange between routers is called *convergence*. When routers finish exchanging data about networks and routes they know, the routers have *converged*. Because distance vector routing protocols combine the routing tables of all routers and propagate them to all neighbors, the convergence process can be fairly long in larger networks. That is one reason why it is not best practice to enable distance vector routing protocols on core layer routers. Distance vector routing is best suited for access or distribution layer routers.

Route updates

After they have converged, routers continue to update each other about network routes they know. These route updates keep track of route changes. Distance vector routing protocols send updates that contain the whole routing table.

Because this is the combined routing table of all routers in the network, the same combined routing table ends up being sent to all routers at predefined time intervals. This consumes more resources on routers and more bandwidth than link-state routing protocols, which do not send the whole routing table to neighbor routers at predefined time intervals.

Although each router sends a route update at predefined time intervals, you must understand that routers do not necessarily send their route updates at the same time. Hence, variations may exist in the knowledge about routes among the routers in the network.

Distance vector routing protocols

The following protocols use distance vector routing:

- ◆ Routing Information Protocol (RIP)
- ◆ Interior Gateway Routing Protocol (IGRP)

IGRP is no longer supported by Cisco. It has been replaced by EIGRP (Enhanced IGRP). EIGRP is considered a hybrid protocol: It has both distance vector and link-state characteristics.



Routing loops

Distance vector routing can cause routing loops. Routing loops route data packets, in loop, continuously, between neighbor routers. This occurs when routers do not all have the same knowledge of the network.

Route updates send the combined routing table to all routers at predefined intervals. However, routers do not send their route updates at the same time. Hence, variations may exist in the knowledge about routes among the routers in the network.

For example, if a network route becomes unreachable, the router that links to that route knows about it. However, a router that is farther from the failed route still thinks that the route is up. It takes some time before all routers in the network know about the failed route.

Distance vector routing protocols use some tricks to avoid these routing loops:

- ◆ Maximum hop count
- ◆ Split horizon
- ◆ Route poisoning
- ◆ Poison reverse
- ◆ Hold-down timer
- ◆ Triggered update

Maximum hop count

The *maximum hop count* feature ensures that a data packet never takes a route that counts more than a predefined maximum number of hops.

In the example shown previously, the packet will loop indefinitely, which means that it will traverse an infinite number of hops. The maximum number of hops feature attempts to stop this infinite loop. Each protocol has a predefined maximum number of hops. Routers consider a destination network to be unreachable if the number of hops associated with the route to that network exceeds the maximum number of hops allowed by the routing protocol. Table 3-2 lists the predefined maximum hop count for each routing protocol.

Table 3-2 Maximum Hop Count	
<i>Routing Protocol</i>	<i>Maximum Number of Hops</i>
RIP	15
EIGRP	255 (can be configured between 1 and 255; default is 100)
OSPF	Unlimited, because this is a link-state protocol

Split horizon

The *split horizon* feature prevents a route from being advertised back to its advertiser. Here is how this works: Consider two routers, 67<>51 and 51-2. Router 67<>51 advertises the existence of network 67 to router 51-2. Next, router 51-2 advertises network 67 to other routers: router 51-1 and router 25<>51. Without the split horizon feature, router 51-2 would also advertise network 67 back to router 67<>51. This would confuse router 67<>51 because it would think that there is an alternate route back to network 67 through router 51-2. If you assume that the split horizon feature does not exist, this can cause a routing loop:

- ◆ This would cause router 67<>51 to think that an alternate route exists back to network 67 through router 51-2.
- ◆ Router 51-2 knows about network 67 from router 67<>51.
- ◆ Assume that router 67<>51 lost its connection to network 67.
- ◆ Router 67<>51 thinks that an alternate route exists back to network 67 through router 51-2, because router 51-2 advertised network 67 back to router 67<>51 (no split horizon feature).
- ◆ Now, router 67<>51 sends packets bound for network 67 to the alternate route to network 67 through router 51-2.
- ◆ Router 51-2 knows about network 67 from router 67<>51, so it sends packets bound for network 67 back to router 67<>51.
- ◆ And so on. The data packets bound for network 67 bounce infinitely between routers 67<>51 and 51-2.

You see now how the split horizon feature allows routers to avoid this situation by preventing router 51-2 from advertising “network 67 reachable through router 51-2” back to router 67<>51.

Route poisoning

The *route poisoning* feature changes the hop count associated with a route that becomes unreachable: It sets the hop count to the maximum hop count plus 1. This effectively tells all routers in the network that the route is unreachable because the hop count exceeds the maximum hop count allowed by the routing protocol. It is a method of disabling an unavailable route in the routing tables as quickly as possible.

In the preceding example, when network 67 becomes unreachable, router 67<>51 sends a packet to router 51-2 advertising network 67 with a hop count of MaxHopCount+1. Right away, router 51-2 considers network 67 unreachable. This prevents router 51-2 from getting confused by router 25<>51 when it advertises “network 67 up” right after router 67<>51 advertises “network 67

down”: Even if router 51-2 thinks that network 67 is up and reachable through router 25<>51 now, the hop count is larger than the maximum hop count allowed by the routing protocol, so 51-2 would never send to network 67.

Poison reverse

The *poison reverse* feature is similar to router poisoning but in the reverse direction. In the preceding example, when router 67<>51 sends a packet to router 51-2 advertising network 67 with a hop count of MaxHopCount+1, router 51-2 sends back a packet to router 67<>51 advertising network 67 with a hop count of MaxHopCount+1. This basically breaks the split horizon rule, but that’s okay, because the whole purpose of all of these rules is to prevent routing loops from happening. By using poison reverse, the routers ensure that all neighbors know as quickly as possible that network 67 is down.

Hold-down timer

The *hold-down timer* prevents a router from accepting updates about a route for a certain time if that route was advertised as unavailable. This prevents routing loops by ensuring that when a route has been advertised as being unreachable, it is not readvertised as being back up by a router that did not receive the “route down” message yet.

For example, router 51-2 is confused by router 25<>51 when 25<>51 advertises “network 67 up” right after router 67<>51 advertises “network 67 down.” The hold-down timer feature avoids this confusion by preventing router 51-2 from accepting the “network 67 up” update sent by router 25<>51, right after router 67<>51 sent a “network 67 down” update.

Triggered update

The *triggered update* feature allows routers to update each other as soon as a change occurs in the network, as opposed to waiting until the scheduled route updates to be exchanged.

By default, distance vector routing protocols combine and exchange the routing tables of all routers at predefined time intervals. If a network fails right after the router sent its scheduled route update, the other routers won’t know about the failed network until the next route update sent by the router that connects to the failed network. This opens a large window of time when routers in the network think that a route is up when in fact it is down. Triggered updates fix this by causing the router to send its update to neighbors as soon as it detects that the route is down.

Link-state routing

Link-state routing protocols build their routing tables independently based on route updates they receive from their neighbors. Link-state protocols do not merge the routing tables of neighbor routers. Rather, they enable routers

to have a clear image of their neighbors, network topology, and routes to their neighbors and beyond.

Here are the main characteristics of link-state protocols:

- ◆ Route updates are only sent when routes change, as opposed to distance vector protocols, which send route updates periodically.
- ◆ Route updates contain information about the route that changed only, as opposed to distance vector protocols, which send route updates that contain the whole combined routing table.
- ◆ Routers first exchange “Hello” messages to get acquainted with their neighbors, as opposed to distance vector protocols, which exchange and combine their routing tables from the get-go.
- ◆ Routers maintain neighbor and topology tables in addition to routing tables to help routers keep track not only of routes but also of the topology of the network and of their neighbor routers.

Convergence

Routers execute an initial exchange of routing information when they power up and join the network. This initial exchange is called the *convergence* process. When routers finish exchanging data about networks and routes they know, the routers have *converged*.

Because link-state routing protocols only exchange “Hello” messages initially and because link-state protocols do not merge their routing tables, they converge faster than distance vector protocols.

It is best practice to use link-state routing protocols or hybrid protocols on core layer routers. Distance vector routing is best suited for access or distribution layer routers.

Route updates

Similar to distance vector protocols, link-state routing protocols continue to update routers about available routes after they have converged. These route updates keep track of route changes. Contrary to distance vector routing protocols, link-state protocols do not send regular updates that contain the whole routing table. Link-state routing protocols send route updates that contain only information about the route that changed.

Because link-state route updates are relatively infrequent and contain only a small advertisement about the route that changed, they consume fewer resources on routers and less bandwidth than distance vector routing protocols, which send the whole routing table to neighbor routers regularly, at predefined time intervals.

Link-state routing protocols

The Open Shortest Path First (OSPF) protocol uses link state routing.

Hybrid routing

Hybrid protocols have both distance vector and link-state characteristics:

- ◆ Like distance vector protocols, hybrid protocols use distance to evaluate the quality of routes.
- ◆ Like link-state protocols, hybrid protocols use other metrics in addition to distance to evaluate the quality of routes, such as available bandwidth, delay, reliability, load, and MTU.

Convergence

Similar to link-state routing protocols, hybrid protocols only exchange “Hello” messages initially. Hence, they converge faster than distance vector protocols.

Hybrid protocols are well suited for core layer, distribution layer, and even access layer routers.

Route updates

Similar to distance vector protocols, hybrid routing protocols send route updates that contain the whole routing table. However, unlike distance vector protocols, hybrid protocols do not send route updates regularly at predefined time intervals. They only send updates when routes change, like link-state protocols.

Hybrid routing protocols

Enhanced IGRP (EIGRP) is considered a hybrid routing protocol.

Configuring Routing Protocols

The procedure to configure routing protocols on Cisco routers is the same for all protocols. Follow these steps to enable any given routing protocol on a Cisco router:

1. Start up the routing protocol on each router.
2. Enable the routing protocol on interfaces on each router.
3. Configure routing protocol options.

You need to execute these setup steps manually on each router. Some routing protocols can automatically negotiate certain configuration options.

Prep Test

- 1 Describe a network route.**
 - A ☐ A set of metrics that routers use to evaluate distance to a network
 - B ☐ A data transmission path through one or more networks between two end nodes
 - C ☐ A Layer 3 protocol
 - D ☐ All of the above
- 2 Describe a static route.**
 - A ☐ It is predefined on your router.
 - B ☐ You create it manually on your switch.
 - C ☐ You create manually on your router.
 - D ☐ All of the above.
- 3 What is the main advantage of static routes?**
 - A ☐ Routing efficiency: fewer resources consumed on your router and less bandwidth spent for routing
 - B ☐ Maintenance: easier to maintain than dynamic routes
 - C ☐ Scalability: static routes scale out very well, even in large networks
 - D ☐ All of the above
- 4 Describe a dynamic route.**
 - A ☐ It is predefined on your router.
 - B ☐ Routing protocols are created and maintained on your router.
 - C ☐ It is manually created on your router.
 - D ☐ All of the above.
- 5 Dynamic routes are necessary for network environments that need which of the following?**
 - A ☐ Adaptive routing accuracy: routes are updated as they change by routing protocols
 - B ☐ Low maintenance: easier to maintain than static routes
 - C ☐ High scalability: dynamic routes scale out very well, even in large networks
 - D ☐ All of the above

6 Define a default route.

- A ☐ It is a predefined route on your router.
- B ☐ Routing protocols are created and maintained on your router.
- C ☐ It is a static route that defines the destination of any packets whose destination network is unknown
- D ☐ All of the above

7 Routing protocols have which of the following features?

- A ☐ Exchange network, routes, and metric information between routers
- B ☐ Help routers build their routing tables
- C ☐ Do not route data packets
- D ☐ All of the above

8 Describe routed protocols.

- A ☐ They tag each data packet with the source and destination hierarchical addresses.
- B ☐ They assign a unique logical address to each node in the network.
- C ☐ They route data packets.
- D ☐ All of the above.

9 The administrative distance defines which of the following?

- A ☐ How reliable is the information source that provided the data about the network route
- B ☐ How far is the next router on a given route
- C ☐ How far is the next administration service point on a given route
- D ☐ All of the above

10 When the administrative distance of two routes to the same network is the same, routing protocols use _____ to evaluate the quality of each route

- A ☐ Helper agents
- B ☐ Metrics
- C ☐ Switch modules
- D ☐ All of the above

11 Describe the hop-count metric.

- A ☐ It is the number of routers and networks that need to be traversed to get to the destination network.
- B ☐ It is the number of ports on a router.
- C ☐ It is the number of links between two networks.
- D ☐ All of the above.

Answers

- 1** B. A network route is a data transmission path through one or more networks between two end nodes. Read *"Introducing Network Routes."*
- 2** C. You create manually on your router. A static route is a route that you manually create on your router. See the *"Introducing Network Routes"* section.
- 3** A. Routing efficiency: fewer resources consumed on your router and less bandwidth spent for routing. The main advantage of static routes is their efficiency. Static routes consume very few resources on the router since you don't need to run routing protocols to maintain static routes the way you do for dynamic routes. See the *"Introducing Network Routes"* section.
- 4** B. Routing protocols create and maintain on your router. A dynamic route is a route that routing protocols create and maintain on your router. See the *"Introducing Network Routes"* section.
- 5** D. All of the above. Dynamic routes are well suited for network environments that need adaptive routing accuracy, low maintenance, and high scalability. See the *"Introducing Network Routes"* section.
- 6** C. Is a static route that defines the destination of any packets whose destination network is unknown. A default route is a static route that defines where packets are sent when the router cannot find any route for them. See the *"Introducing Network Routes"* section.
- 7** D. All of the above. Routing protocols exchange network, routes and metric information between routers to help routers build their routing tables. Routing protocols do not route packets. Routed protocols route packets. Review the *"Routing Protocols"* section.
- 8** D. All of the above. Routed protocols tag each data packet with the source and destination hierarchical addresses. They assign a unique logical address to each node in the network and they route data packets. Review the *"Routing Protocols"* section.
- 9** A. How reliable is the information source that provided the data about the network route. The administrative distance defines how reliable is the information source that provided the data about the network route. Review the *"Routing Decision Criteria"* section.
- 10** B. Metrics. When the administrative distance of two routes to the same network is the same, routing protocols use metrics to evaluate the quality of each route. Review the *"Routing protocol metrics"* section.
- 11** A. The number of routers and networks that need to be traversed to get to the destination network. The hop count metric measures the number of routers and networks that need to be traversed to get to the destination network. Review the *"Routing protocol metrics"* section.

Chapter 4: Routing Information Protocol (RIP)

Exam Objectives

- ✓ Defining distance vector and interior gateway protocols
- ✓ Examining routing updates and convergence
- ✓ Understanding hop-count metrics, routing loops, and split horizon
- ✓ Comparing RIPv1 and RIPv2
- ✓ Detailing RIP packet structures
- ✓ Defining autonomous systems
- ✓ Configuring RIP
- ✓ Verifying RIP installations

The Routing Information Protocol, or RIP for short, is a dynamic local- and wide-area network distance vector, interior gateway protocol. The distance vector routing algorithm on which RIP is based has been in use since the mid-1950s. Known originally as the Bellman-Ford algorithm, it was first used for the ARPANET computer networks in 1968. This distance vector algorithm is used in packet-switched networks to calculate paths and distances to target networks by mathematically comparing multiple routes to the same destination. RIP uses these calculations to determine the best path to the target network.

Distance vector protocols such as RIP are required to periodically announce any known network topology changes to other neighboring routing devices. Because distance vector protocols do not have knowledge of the entire network topology, these updates are repeated at regular intervals on User Datagram Protocol (UDP) port 520. Also, during network topology configuration changes, these updates are recorded in the routing table of each connected network router. Routing updates continue between network routers with the goal of having all routing tables in complete agreement with one another, or matching. This is known as *convergence*. Without convergence, it is impossible for distance vector protocols to function properly.

Introducing Routing Information Protocol (RIP)

Because routers initially have only information pertaining to directly attached interfaces, neighboring routes must be discovered. Routers use distance vector algorithms (such as RIP) and routing tables to discover, analyze, and record distances between possible destinations.

Each router periodically sends a list of all known routes and announces these routes to all other neighboring routers (on directly attached segments). Distance vector protocols do not maintain a map of the entire network, just neighboring next-hop addresses. This differs from link-state protocols, which contain the entire network map and include updates to remote router segments. So, a general overview of RIP may be consolidated as follows:

- ◆ Each router on an internetwork has an individual identity and advertises directly attached links using a zero metric.
- ◆ During the router bootup process, the complete routing table is forwarded to all neighboring routers.
- ◆ Routing updates are propagated (sent to other neighboring routers) every 30 seconds, or they may be forwarded automatically when topology changes are detected.
- ◆ Each router calculates which neighbor may be used to reach a destination network using the shortest available path.



Due to protocol limitations, RIP is known to have slow convergence times and is considered a poor choice for large-scale WANs. RIP is best suited for smaller-scale deployments isolated within a single autonomous system (AS).

An interior gateway protocol

RIP is also defined as an interior gateway protocol and was originally designed for smaller networks, with similar network topology and specifications. This means that the routing protocol is contained within the same routing domain, or autonomous system. Autonomous systems are considered to be a single network or multiple groups of networks under the control of the same administrative structure. For example, the IT department of a single university tasked with the administration of multiple campus networks is considered a single autonomous system. The routers inside these interior networks use interior gateway protocols such as RIP to communicate and share routing information between subnets.

Communication outside or between autonomous systems is handled by a Border Gateway Protocol (BGP), formerly known as an Exterior Gateway Protocol. To separately distinguish and uniquely identify each AS on the

Internet, autonomous systems are assigned an Autonomous System Number (ASN) by the Internet Assigned Numbers Authority (IANA) or individual Regional Internet Registries (RIRs).

Cisco routers use a number of different protocols to transfer data. Multiple protocols may be activated simultaneously and run independently of one another. To decide which methods of communications to use, protocols are weighted by administrative distance (AD). The higher the AD value, the less likely that the protocol will be chosen by the IOS. For example, RIP carries an AD value of 120, with Open Shortest Path First (OSPF) assigned a value of 110. If two routes exist on a router (using RIP and OSPF in this example) to a particular destination network, the lowest AD, OSPF, is selected. The default assigned values for administrative distance are listed in Figure 4-1. The `distance` command may be used to change these default values.

Administrative Distance	Routing Method
0	Direct Connection
1	Static Route
5	Enhanced IGRP Summary Route
20	External BGP
90	Internal Enhanced IGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
160	On Demand Routing
170	External Enhanced IGRP
200	Internal BGP
255	Unknown

Figure 4-1:
Cisco
default
admini-
strative
distances.

Routing tables, updates, and hop count

RIP relies heavily on a metric hop count to determine the path and distance to the destination network. The optimal route to a destination is decided by RIP's calculated number of hops it must make to deliver data to the target network. To RIP, less hops means less stops and shorter distances to the destination. The lowest metric value is considered by RIP to be the best route available. For example, a route with five hops to a target network will be preferred over a different six-hop route leading to the same destination.

This method of route determination by RIP may also prove dramatically inefficient. For example, the speed of both links has not been taken into consideration. RIP considers the five-hop route closer in distance than the six-hop route and chooses the shortest metric for delivery. This would prove to be a poor choice if the six-hop route were established over high-speed connections while the five-hop route used much slower WAN links.

RIP limits the hop count to eliminate the condition known as "counting to infinity." By assigning each IP packet a starting default Time-To-Live (TTL) value of 15, a packet "life span" is established. Every packet must reach its final destination in 15 hops or less. As a packet progresses through a gateway, a hop is recorded, and the TTL value is reduced by 1. Each router along the path to the destination is considered a hop and decreases the TTL value inside the IP packet by 1. If the packet's TTL value equals 0 and still has not reached its final destination, it is discarded. This eliminates routing loops and prevents undeliverable packets from remaining on the internetwork indefinitely.

When a routing table update is received, the router checks for changes by comparing the update to the currently existing routing table. If a new route is announced in an update, it is added to the existing routing table. This increases the metric value by a factor of 1, and the sender's IP address is assigned as the next-hop address. To ensure proper convergence, the router then sends this new update to all neighboring routers right away and separately from any other regularly scheduled routing updates. If an identical route exists in both the update and current routing table (but includes a lower metric for the route), the lower metric is used by replacing the existing routing table entry with the updated route (smaller metric value).

Routing error mitigation methods

RIP depends on neighboring routing devices and gateways to announce routing table updates (every 30 seconds) and uses the best route to a destination. Problems arise when a gateway or router along the destination path fails. In such cases, these newly unreachable gateways are unable to announce their "downed" status:

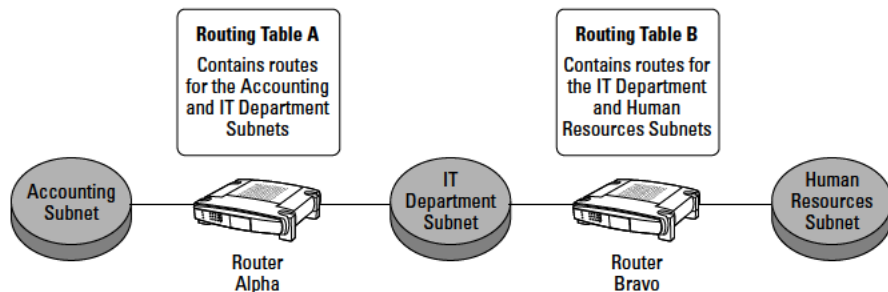
- ◆ If communication to a router is not made after 90 seconds, the route is considered invalid.
- ◆ After 180 seconds, the hold-down timer is reached, and RIP determines that the route is no longer available.

Neighboring gateways are contacted with an update regarding the unavailable route.

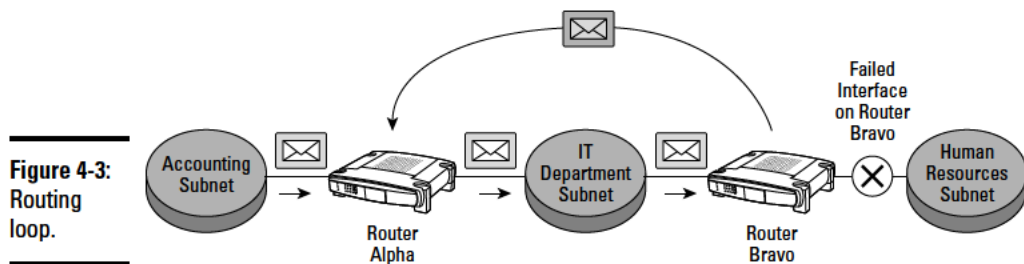
- ◆ After 270 seconds, if no other information is received regarding the failed route, the flush timer removes the route from the routing table.

RIP also prevents the possibility of routing loops by limiting the hop count value to 15. A routing loop is an error occurring in the routing algorithm, causing an endless, infinite loop that designates a remote destination network as unreachable. To examine the RIP routing table update process and looping problem, refer to Figure 4-2. Three subnets are connected using two routers. The routing table on the Alpha router contains information on how to reach the accounting and IT department, while the Bravo router knows routes for the IT department as well as the human resources subnet. After routing table updates are exchanged between routers, each router will have a defined map to reach all three subnets.

Figure 4-2:
Exchange
of routing
updates
between
networks.



Now, a user on the accounting subnet wants to communicate with a user on the human resources subnet. Complications begin in this scenario when an interface on a router fails. The user's packet reaches the Bravo router, but the Bravo router's interface to the human resources subnet goes down and has no possibility of delivering the packet. If the Alpha router is advertising an alternate route to the human resources department, the Bravo router will forward the packet back to the Alpha router, figuring that the packet will be deliverable through the Alpha route. The Alpha router will then do a routing table lookup and determine that the next-hop path to the human resources department is through router Bravo. As shown in Figure 4-3, without the hop-count limitation, this loop would continue to infinity.



Split horizon

RIP provides other preventive measures to eliminate routing loops. Split horizon is a method that prevents a router from advertising a route back out of the same interface on which the route was received, or learned on.

This would eliminate the problem from the previous example. Router Alpha knows the path to the human resources department only because of router Bravo's routing table announcements, and therefore does not send routing information to router Bravo regarding the human resources network. Likewise, Router Bravo has discovered the accounting subnet only because of the broadcasted announcements of router Alpha and — using the split horizon rules of communication — does not send its routing table information regarding the accounting department to router Alpha. Split horizon is thus enabled by default on interfaces running RIP, Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP).

Split horizon with poison reverse is a slightly modified version of the split horizon loop-mitigation method previously mentioned. In standard split horizon, router Alpha's path to the human resources subnet is not advertised to router Bravo. Likewise, router Bravo's known route to the accounting subnet is not advertised to router Alpha. Instead of not advertising the path to prevent the loop as with standard split horizon, poison reverse inexplicably denies the path. This is done by assigning the route with a TTL metric of 16. When the router reads this in its routing table, the route is ignored.

Convergence and timers

RIP relies on convergence and timers to keep routing tables between interconnected routing devices on a WAN current and accurate.

Convergence allows all routing devices to be in complete synchronization with one another. Convergence may prove to be more difficult to achieve in larger-scale network deployments. As an internetwork grows, more

routing tables must be updated and kept in agreement with all other gateways. When a change inside the internetwork topology is detected, a new routing table update is triggered. This “triggered update” occurs independently from the repetitive, regularly scheduled 30-second automatic routing table updates and improves convergence times. For example, when a router detects a link failure to a neighboring router of a gateway, a routing update is triggered, notifying all other neighboring routing devices of the failed link. Each contacted router then informs its own neighbors regarding the link failure until all devices converge (are in agreement).

Problems may arise if all routers do not converge in a timely fashion. If a neighboring router has not yet been informed and is unaware of the link failure, and its own (outdated) routing table update is sent to a router that has already been notified of the link failure, a reactivation of the failed link by means of an unwanted routing table update (reinserting the route to the bad link) could happen. Timers, such as the hold-down timer, are used in preventing the reactivation of failed links. Hold-down timers deny propagation of dead routes via updates for specific periods of time, allowing proper network convergence to occur.



Keep the following points in mind regarding the Routing Information Protocol:

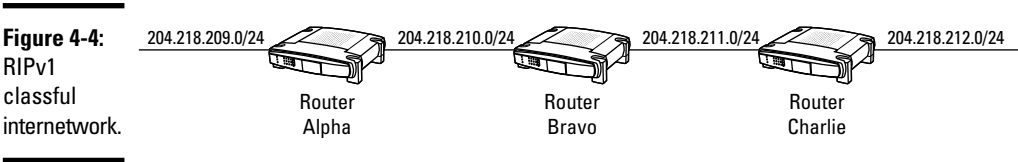
- ◆ Hop count limit of 15.
- ◆ RIP broadcasts routing updates every 30 seconds.
- ◆ Sends routing table updates on UDP port 520.
- ◆ Inefficient routing decisions. Best path determined by smaller metric.
- ◆ Slow convergence in large-scale networks.
- ◆ Uses minimal CPU and memory resources.
- ◆ Efficient in single autonomous systems or small-scale networks.
- ◆ Universal interoperability protocol support between hardware manufacturers and software developers allows interconnecting legacy and newer hardware.

RIPv1

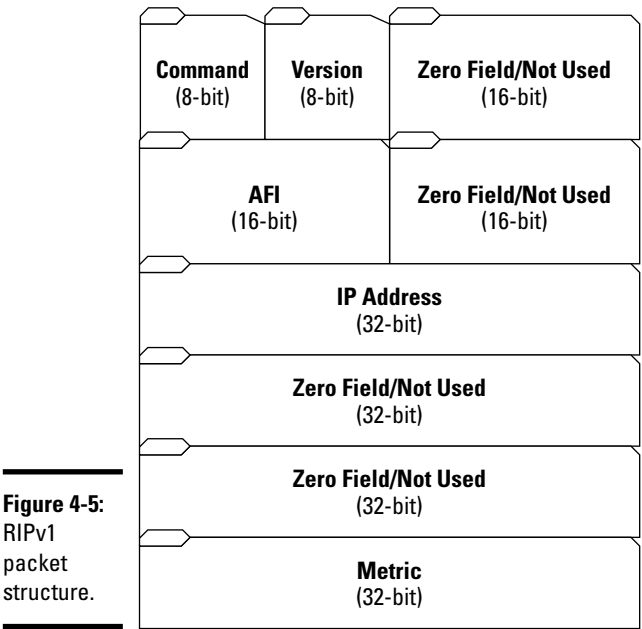
The original RIP specification, created by Xerox Corporation, is known as RIP version 1.

The major difference between RIPv1 and RIPv2 is that routing updates in RIP version 1 cannot contain subnet information.

As shown in Figure 4-4, RIPv1 is known as a classful routing protocol. You cannot use RIPv1 in a classless routing environment. Because all subnets must be of the same size, creating unequal-sized subnets with variable-length subnet masking (VLSM) is not possible using RIPv1. RIPv1 also supports no method to authenticate router updates, which leaves the network vulnerable to malicious attacks.



RIPv1 transports routing table updates in IP packets reaching 512K in size. The structure of these individual packets is shown in Figure 4-5. Following are the descriptions of the various fields that comprise a RIPv1 packet:



- ◆ **Command:** Field distinguishing the type of packet being transmitted. Request packets are used to poll other routers for routing table updates. Response packets are either generated due to a request packet or as a normally scheduled routing table update.

- ◆ **Version Number:** Field displaying the RIP version number currently in use. For RIPv1, this value is set to 1. A value of 2 indicates RIPv2.

The version number field may be used in troubleshooting scenarios, allowing administrators to pinpoint potential incompatibility problems between RIP versions.

- ◆ **Zero/Unused:** Unused field holding a default value of 0.
- ◆ **Address-Family Identifier (AFI):** Because RIP is able to transport routing information for multiple protocols, this field is used to designate the address family, or advertised protocol, used by RIP.

Each AFI number identifies the address being used by its value, with 2 representing IP addressing.

- ◆ **Address:** Field holding the IP address.
- ◆ **Metric:** The number of hops encountered along the way to a particular destination. A reachable route always uses a metric of 15 hops or less. Any destination requiring more than 15 hops is considered unreachable.

RIPv2

RIPv2 builds on the existing structure of RIPv1 by adding the following features:

- ◆ **Enhanced security measures:** Provides support for message digest algorithm 5 (MD5) and plain-text password authentication.
- ◆ **Support for classless addressing schemes:** Classless interdomain routing (CIDR) and VLSM are supported by adding a subnet mask field to the RIPv2 packet structure.
- ◆ **Route Tag field:** Separator for internal and external RIP routes.
- ◆ **Next Hop field:** Allows packet forwarding to the immediate next-hop address.
- ◆ **Multitasking:** RIPv2 supports multitasking using IP address 224.0.0.9.

The RIPv2 packet structure is similar in size to the RIPv1 packet but replaces the zero fields with router tag, subnet mask, and next-hop addressing information.

The changes to the packet structure allow RIPv2 to provide authentication security and VLSM/CIDR support, which are not available in RIPv1. The RIPv2 packet structure is shown in Figure 4-6, and the following descriptions explain the various fields that comprise a RIPv2 packet:

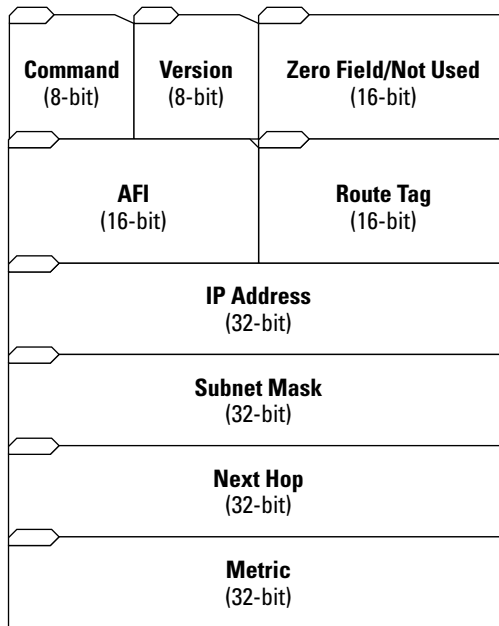


Figure 4-6:
RIPv2
packet
structure.

- ◆ **Command:** As with RIPv1, this field is used to distinguish the type of packet being transmitted. Request packets are used to poll other routers for routing table updates. Response packets are either generated due to a request packet or as a normally scheduled routing table update.
- ◆ **Version:** Denotes the RIP version used. For RIPv2, this value is set to 2.
- ◆ **Zero/Unused:** Unused field holding a default value of 0 and implemented only for backward compatibility with nonstandard (outdated) RIP versions.
- ◆ **Address-Family Identifier (AFI):** Shows the address family used by RIP. The AFI field of RIPv2 functions similarly to RIPv1.

One difference between RIPv1 and RIPv2 is the use of authentication. If the AFI hex message entry in the first message equals 0xFFFF, the remaining entries will contain authentication information consisting of a simple password.

- ◆ **Route Tag:** Field used to show whether the route is an internal or external route. Internal routes are discovered by RIP alone, whereas external routes are discovered via non-RIP protocols.
- ◆ **IP Address:** Field used for IP address information.
- ◆ **Subnet Mask:** Field used for subnet mask information.

A subnet mask field value of 0 means that no subnet mask addressing information has been given. This field is not available in RIPv1.

- ◆ **Next Hop:** IP address of the next-hop address.
- ◆ **Metric:** The number of hops encountered along the way to a particular destination. A reachable route always uses a metric of 15 hops or less. Any destination requiring more than 15 hops is considered unreachable.



The maximum number of router table entries in a RIPv1 or RIPv2 packet is 25. Using RIPng (see the next section), there is no longer a limit for routing table entries and is only limited by the maximum transmission unit (MTU).

RIPng

Routing Information Protocol Next Generation, or RIPng, is intended for IPv6 networks. Based on the RIP IPv4 algorithm, RIPng is designed for medium-sized autonomous systems using interior gateway protocols.

The following are key differences in implementation between IPv4 and IPv6:

- ◆ RIPng does not need to implement authentication on packets.
If authentication is required, it is performed by IP Security (IPsec), increasing efficiency.
- ◆ Packets use the Prefix Length field instead of a subnet mask.
- ◆ Next-hop addresses are contained in a separate routing entry to conserve space.
- ◆ Uses multicasts for transmissions using FF02::9.
- ◆ Uses UDP port 521 instead of 520.

The packet structure of IPv6 compared to IPv4 is shown in Figure 4-7. An explanation of the RIPng packet fields follows:

- ◆ **Command:** Distinguishes between request and response messages. Request messages seek information for the router's routing table and contain the value of 1. A value of 2 indicates response messages, sent periodically or when a request message is received.
- ◆ **Version Number:** Specifies the version of RIPng that the originating router is running. This will be set to 1 because this is the first version of the RIPng protocol.
- ◆ **Zero/Unused:** An unused, reserved field set with a default value of 0.

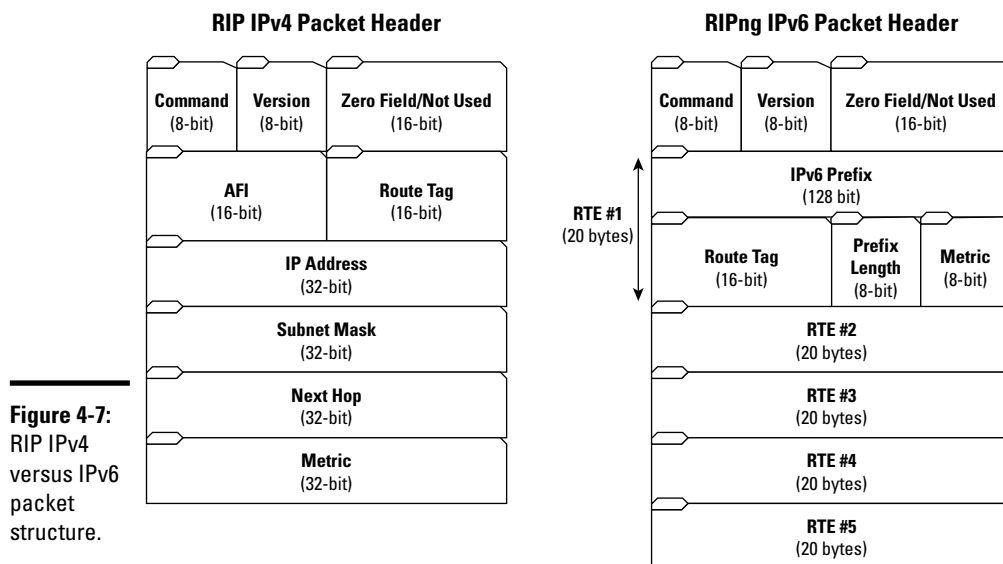


Figure 4-7:
RIP IPv4
versus IPv6
packet
structure.

♦ **Route Table Entries:** A 20-byte routing table entry field containing information regarding reachable routes. Each RIPng packet contains a variable amount of routing table entries (RTEs). RTE subfields include the following:

- *IPv6 prefix:* The 128-bit network address.
- *Route Tag:* Distinguishes between internal and external routes.
- *Prefix Length:* An 8-bit prefix length field analogous to an IPv4 subnet mask. The prefix length is used to separate the network and host portion of the address.
- *Metric:* A value of 15 or less, designating a valid route. Invalid routes are marked with an unreachable value of 16, or infinity.

Configuring RIP

Matching the simplistic characteristics of the protocol, RIP configuration is also simple and easy to implement. There are two main requirements when configuring RIP on a Cisco router:

- ♦ The `router rip` command is used to enable RIP on the router.
- ♦ The `network` command is issued to designate the networks that allow RIP traffic.

Execute the following IOS commands to enable RIP on a Cisco router:

1. In global configuration mode, assign IP addresses to the router interfaces (if not already configured):

```
Router>enable
Router#config t
Router(config)#interface ethernet 0
Router(config-if)#ip address 192.168.10.1
Router(config-if)#interface ethernet 0
Router(config-if)#ip address 192.168.11.1
Router(config-if)#no shutdown
Router(config-if)#exit
```

2. Enable RIP:

```
Router(config)#router rip
```

3. Specify a network to associate with RIP routing (from Step 1):

```
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.11.0
Router(config-router)#exit
```

Although not mandatory, quite a few additional configuration options are available for RIP.

The following options may be used after RIP has been enabled on the Cisco router:

- ◆ **Permit unicast updates:** RIP is considered a broadcast protocol. To allow the exchange of routing updates between broadcast and nonbroadcast networks, issue the following command in router configuration mode:

```
Router(config-router)#neighbor 192.168.10.1
```

RIP router table updates will now be sent to the nonbroadcast neighboring router (192.168.10.1).

- ◆ **Prevent updates on a specified interface:** In certain cases, limiting router updates from reaching certain interfaces may be warranted. For example, preventing the advertisement of local routes from Ethernet (LAN) interfaces to be sent to serial (WAN) interfaces may be required, thus regulating advertised routes. To disable RIP updates to a specified interface, use the following command in router configuration mode:

```
Router(config-router)#passive interface s1
```

- ◆ **Routing metric offsets:** Allows increasing incoming and outgoing metric values learned by RIP. In the following example, an incoming offset of 10 is established to any routes learned from the Ethernet 0 interface (using access-list number 50):

```
Router(config-router)#offset-list 50 in 10 ethernet 0
```

- ◆ **Timer adjustments:** Interval settings may be adjusted for the frequency of outgoing routing updates, specified time period until a route becomes invalid, and the elapsed time until a dead route is removed from the routing table. To adjust timers, use the `timers basic` command in router configuration mode:

```
Router(config-router)#timers basic 30 90 180 270 0
```

Listed here are the default timer interval settings:

- *Update (30 seconds):* Time interval between routing table updates
 - *Invalid (90 seconds):* Time interval during which a route is considered invalid
 - *Holddown (180 seconds):* Time interval during which routing information regarding better paths is ignored, or suppressed
 - *Flush (270 seconds):* Amount of time elapsed before a route is removed from the routing table
 - *Sleeptime (0 milliseconds):* Amount of time in which routing updates will be postponed
- ◆ **RIP version:** Specifies the sending and receiving of RIPv1 or RIPv2 updates. By default, Cisco routers receive incoming RIPv1 and RIPv2 router table updates, but send outgoing RIPv1 updates only.

To specify the required RIP version, use the `ip rip send version` and `ip rip receive version` IOS commands in interface configuration mode:

- To send and receive RIPv1 packets only:

```
Router(config-if)#ip rip send version 1
Router(config-if)#ip rip receive version 1
```

- To send and receive RIPv2 packets only:

```
Router(config-if)#ip rip send version 2
Router(config-if)#ip rip receive version 2
```

- To send and receive both RIPv1 and RIPv2 packets:

```
Router(config-if)#ip rip send version 1 2
Router(config-if)#ip rip receive version 1 2
```

- ◆ **Enable RIP authentication:** Because RIP authentication is not possible in version 1, sending and receiving of RIPv2 packets must be enabled to use this option. RIP authentication only applies to RIPv2. Plain text (used by default and is a security risk) and message digest algorithm 5 (MD5) are the two types of authentication methods.

MD5 authentication is enabled in interface configuration mode as follows:

```
Router(config-if)#ip rip authentication mode md5
keychain NAMEOFCHAIN
```

- ◆ **Disable route summarization:** When disabled, subnet and host routing information is transmitted across classful network boundaries. RIPv2 supports route summarization by default.

To disable this feature, use the `no auto-summary` command in router configuration mode:

```
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

- ◆ **Disable source IP address validation:** By default on Cisco routers, incoming RIP routing updates are validated by source IP address. This allows verification of the sender's address. If the IP address is determined to be from an unauthorized source (mismatching IP), the update is discarded.

To disable this feature (not recommended), enter the following in router configuration mode:

```
Router(config-router)#no validate-update-source
```

- ◆ **Split horizon:** Used to prevent routing loops. The rule of split horizon specifies that no received inbound routing updates may be sent back outbound on the same interface. This feature improves network communications and is enabled by default for all encapsulation types other than nonbroadcast networks such as Frame Relay.

In the case of nonbroadcast network types, it may be advantageous to disable split horizon in interface configuration mode as follows:

```
Router(config-router)#no ip split horizon
```

To enable split horizon, enter the following:

```
Router(config-router)#ip split horizon
```

Verifying RIP

A few methods exist to verify the functionality of RIP on Cisco devices. Basic IOS commands such as `ping` and `traceroute` are invaluable troubleshooting aids regarding connectivity issues and the routes packets take to reach a destination. Many additional and helpful clues may be learned from various `show` and `debug` commands. Listed here are the most helpful IOS commands when troubleshooting RIP:

- ◆ **show ip protocols:** Used in EXEC mode to display the state and parameters of the active routing protocols.

This allows a network administrator to verify that RIP (or other IP protocols) is actively running on a router and to view the configured timers and networks, as shown here:

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 5 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface        Send  Recv  Key-chain
    Ethernet0         2     2     trees
    Fddi0             2     2
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.2.1         120           00:00:13
    10.1.5.2         120           00:00:07
  Distance: (default is 120)
```

Quite a bit of information is given from the sample output shown here regarding RIP (because RIP is the only configured protocol in the example). The first line states that the routing protocol is RIP. Routing updates are being sent every 30 seconds (default), with the next update arriving in 5 seconds. The intervals for invalid, hold-down, and flush timers are 180, 180, and 240 (nondefault), respectively. Incoming and outgoing filter lists specify whether filters have been set, and the default version control displays that sending and receiving of RIPv2 packets are active. Routing for networks displays the IP addresses of networks into which the routing process is currently injecting routes. Routing information sources shows any address, distance, and last update of routing sources used in compiling the routing table.

- ◆ **show ip route:** Displays the routing table. A sample output is shown here:

```
Router#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

    172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Ethernet0
C       172.16.2.0 is directly connected, Ethernet1
```

As shown in this code, both Ethernet networks are directly attached to the router

- ◆ **show ip rip database:** Displays summary address entries in the RIP routing database, as shown here:

```
Router#show ip rip database
172.18.0.0/16    auto-summary
172.18.0.0/16
  [1] via 172.16.1.2, 00:02:44 (permanent), Serial1/0
    * Triggered Routes:
      - [1] via 172.16.1.2, Serial1/0
172.19.0.0/16    auto-summary
172.19.0.0/16
  [1] via 172.16.1.2, 00:02:45 (permanent),Serial1/0
    * Triggered Routes:
      - [1] via 172.16.1.2, Serial1/0
```

- ◆ **debug ip rip:** Used to display information on RIP events and issues a log message for each RIP update:

```
R1#debug ip rip
RIP protocol debugging is on

RIP: received v1 update from 192.168.1.2 on Ethernet0
  192.168.2.0 in 1 hops
  192.169.2.0 in 1 hops

RIP: sending v1 update to 255.255.255.255 via Ethernet0 (192.168.1.1)
  network 192.169.1.0, metric 1

RIP: sending v1 update to 255.255.255.255 via Loopback0 (192.169.1.1)
  network 192.168.1.0, metric 1
  network 192.168.2.0, metric 2
  network 192.169.2.0, metric 2
```

The first section displays routing updates received from the source network, and the next two RIP updates are sent to destination addresses.

To disable debugging, enter the following:

```
Router#undebug all
All possible debugging has been turned off
```

Additionally, the `debug ip rip` command contains many keywords to specify certain criteria. A few of these are listed here:

- **debug ip rip events:** Displays information regarding RIP routing transactions
- **debug ip rip trigger:** Provides information on RIP triggered packet events
- **debug ip rip database:** Displays information regarding RIP database events



Disable debugging output with the `undebug all`, `no debug all`, and `no debug ip rip` commands.

Prep Test

- 1 Which types of protocol is RIP? (Choose two.)**
 - A ☐ Interior gateway protocol
 - B ☐ External gateway protocol
 - C ☐ Distance vector protocol
 - D ☐ Link-state protocol
- 2 Which statement is true regarding RIPv1?**
 - A ☐ RIP does not use subnet masks.
 - B ☐ All subnets must use the same subnet mask.
 - C ☐ Subnets may use variable subnet masks.
 - D ☐ VLSM support is built into all versions of RIP.
- 3 Which features allow RIP to prevent routing loops? (Choose two.)**
 - A ☐ VLSM
 - B ☐ Authentication
 - C ☐ Split horizon
 - D ☐ CIDR
 - E ☐ Hold-down timers
- 4 Which method best describes RIP's best-path route determination?**
 - A ☐ Fastest link
 - B ☐ Administrative distance (AD)
 - C ☐ Bandwidth allocation
 - D ☐ Hop count
- 5 Which of the following are disadvantages of RIPv1? (Choose three.)**
 - A ☐ Slow convergence
 - B ☐ Classless routing
 - C ☐ Poor performance in large-scale networks
 - D ☐ No security features

- 6** Which commands are used to configure RIP? (Choose two.)
- A ☐ `configure rip`
 - B ☐ `network`
 - C ☐ `rip enable`
 - D ☐ `route rip`
 - E ☐ `router rip`
- 7** What is the administrative distance for RIP?
- A ☐ 110
 - B ☐ 120
 - C ☐ 140
 - D ☐ 130
- 8** By default, at what intervals are RIP routing updates broadcast?
- A ☐ Every 30 seconds
 - B ☐ Every 45 seconds
 - C ☐ Every 60 seconds
 - D ☐ Every 90 seconds
 - E ☐ Every 180 seconds
- 9** What is the difference between split horizon and split horizon with poison reverse?
- A ☐ Poison reverse ignores routes learned from the destination router.
 - B ☐ Poison reverse inexplicably denies the path using a 16 metric.
 - C ☐ Poison reverse allows advertisements back out the same interface it was learned on.
 - D ☐ Poison reverse inexplicably denies the path using a 1 metric.
- 10** Which command is best used to display whether RIP is running on the router?
- A ☐ `show ip route`
 - B ☐ `debug ip rip`
 - C ☐ `show ip running config`
 - D ☐ `show ip protocols`
- 11** Which command is used to prevent updates on certain interfaces?
- A ☐ `passive interface`
 - B ☐ `no auto-summary`
 - C ☐ `rip authentication`
 - D ☐ `router rip no update`

Answers

- 1 A, C. Distance vector and interior gateway protocol. RIP is designed for containment within an autonomous system and is used in packet-switched networks to calculate paths and distances to target networks. Review *"Introducing Routing Information Protocol (RIP)."*
- 2 B. RIPv1 is a classful routing protocol, and all subnets using RIPv1 must be configured with identical subnet masks. See *"RIPv1"* and *"RIPv2."*
- 3 C, E. Split horizon and hold-down timers are used to prevent routing loops. Split horizon prevents advertisements back out the same interface in which the route was originally learned on. Hold-down timers prevent the reactivation of a dead link. Refer to *"Split horizon"* and *"Convergence and timers."*
- 4 D. RIP uses a hop-count metric to determine the shortest path to the destination. Read *"Routing tables, updates, and hop count."*
- 5 A, C, D. Slow convergence and poor performance in large-scale networks, along with lack of authentication methods, are all disadvantages of RIPv1. RIP was designed for deployment in small-scale, single autonomous systems. See *"Convergence and timers"* and *"RIPv1."*
- 6 B, E. `router rip` and `network` are the IOS commands used to enable RIP. Examine *"Configuring RIP."*
- 7 B. 120 is the administrative distance for RIP. Review *"An interior gateway protocol."*
- 8 A. RIP routing table updates are sent every 30 seconds. Read *"Routing error mitigation methods."*
- 9 B. Instead of not advertising the path to prevent the loop as with standard split horizon, poison reverse inexplicably denies the path. Review *"Split horizon."*
- 10 D. The `show ip protocols` command is used to determine whether RIP is enabled and running on a Cisco Interface. Read *"Verifying RIP."*
- 11 A. To disable RIP updates to a specified interface, use the `passive interface` command. Check out *"Configuring RIP."*

Chapter 5: Enhanced Interior Gateway Routing Protocol (EIGRP)

Exam Objectives

- ✓ Describing the features and characteristics of EIGRP
- ✓ Distinguishing EIGRP from IGRP
- ✓ Describing EIGRP routing decision criteria
- ✓ Describing EIGRP route updates and convergence
- ✓ Describing EIGRP routing tables and operation
- ✓ Understanding the Diffusing Update Algorithm (DUAL)
- ✓ Deploying EIGRP
- ✓ Verifying and troubleshooting EIGRP on a Cisco router

As the name implies, the Cisco-proprietary Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol that contains many advantages over Routing Information Protocol (RIP) and its superseded predecessor, the Interior Gateway Routing Protocol (IGRP). EIGRP is the enhanced version of IGRP. Like RIP, IGRP is known as a distance vector protocol, but it uses a dramatically improved distance vector algorithm to determine the best path to a particular destination. IGRP relies more heavily on the bandwidth and delay metrics of a route as opposed to RIP, which relies on the distance of a route.

EIGRP includes features commonly found in more advanced link-state protocols. EIGRP also uses a more advanced method of loop mitigation than both RIP and IGRP, providing a 100-percent loop-free environment.

Other benefits of EIGRP include high scalability with minimal network overhead and very fast convergence speeds. To fully understand the capabilities of EIGRP, it is beneficial to first take a look at the protocol on which it is based, namely IGRP.

IGRP — The Foundation of EIGRP

The Interior Gateway Routing Protocol was originally developed in the mid-1980s by Cisco Systems to exchange routing information between IP-based networks. A major reason for the development of IGRP was to overcome the limitations of RIP. A protocol was needed that would support larger-scale networks not limited by the 15-hop-count metric of RIP. By introducing a complex formula for route calculations, IGRP replaced the single routing metric employed by RIP, and combined multiple metrics (such as bandwidth, delay, load, MTU, and reliability) into a single unit.

IGRP uses the following metrics:

- ◆ **Default metrics:** Bandwidth, delay
- ◆ **Optional metrics:** Load, reliability, MTU

IGRP still imposed limitations on network topologies by limiting routing to classful networks. Because IGRP did not contain a field for the subnet mask inside the packet, support for variable-length subnet masks (VLSMs) and classless networking was not available. These classful protocols, such as IGRP and RIP, assume that all networks are using the same subnet mask. This imposes a huge waste of IP addresses and proves highly inefficient, considering the constant depletion of IPv4 address space.

Enhanced IGRP replaced IGRP. IGRP is no longer supported by Cisco Systems. RIP also has many disadvantages compared to the more powerful EIGRP. Here are some of the limitations of both RIP and IGRP:

- ◆ Slow convergence
- ◆ No CIDR/VLSM support
- ◆ Hop-count limitation of 15 (RIP)
- ◆ Not 100-percent loop-free
- ◆ Broadcasts complete routing table during updates

EIGRP Benefits

Cisco developed EIGRP to overcome IGRP limitations, so EIGRP:

- ◆ Converges quickly
- ◆ Supports CIDR and VLSM
- ◆ Hop count can be configured between 1 and 255, with a default of 100

- ◆ Uses the more advanced DUAL (Diffusing Update Algorithm) to evaluate the quality of each route
- ◆ Can leverage routes maintained by other routing protocols
- ◆ Is compatible with existing IGRP and can route Internet Protocol (IP), Novell Netware Internetwork Packet Exchange (IPX), and Apple AppleTalk routed protocols

Characteristics of EIGRP

Although EIGRP evolved out of IGRP, which is a *distance vector protocol*, EIGRP is considered to be a *hybrid routing protocol* because it provides many advanced features that are typically found in *link-state protocols*.



Whenever you are asked about EIGRP on the CCNA test, always think of it as a *hybrid routing protocol*. In fact, EIGRP performs as well, and sometimes better than, Open Shortest Path First (OSPF), which is a link-state protocol. So, EIGRP is in the OSPF and other link-state protocols' league, not in the distance vector protocols' league.

Here are the main characteristics of EIGRP:

- ◆ EIGRP uses many metrics to evaluate the quality of a route, in addition to the distance of the route:
 - Bandwidth and delay (these are EIGRP default metrics)
 - Reliability, load, MTU (these are EIGRP optional metrics)
 - Evaluates quality of routes using DUAL (Diffusing Update Algorithm)
- ◆ EIGRP, like OSPF and other link-state routing protocols, sends route updates only when changes occur in the network.

RIP and IGRP broadcast the routing table periodically to all routers in the network.
- ◆ EIGRP, like OSPF and other link-state routing protocols, exchanges only "Hello" messages between routers during the convergence process.
- ◆ EIGRP is not supported on non-Cisco routers, because it is a Cisco-proprietary routing protocol.
- ◆ EIGRP uses two administrative distance values:
 - 90 for routes learned with EIGRP
 - 170 for routes learned from other routing protocols

EIGRP Operation

To understand EIGRP operation, you need to understand its components.

Basic components

EIGRP consists of four basic components:

- ◆ **Neighbor discovery/recovery:** Technology used by Cisco routers to discover the presence of neighboring routers on direct-attached networks. The discovery process allows Cisco routers to use small-sized, low-overhead hello packets to contact other routers. The sending and receiving of these efficient hello packets determine whether a neighbor is functioning properly or whether a routing device has become unreachable. Routers acknowledge their presence to other networks with these packets, and after they are exchanged, communications may begin. If no hello packet is received from a neighboring router, it is considered unreachable.
- ◆ **Reliable Transport Protocol (RTP):** Provides reliable and guaranteed delivery of EIGRP multicast or unicast packets to all neighboring routers. To maintain protocol efficiency, RTP only transmits packets reliably when required. Certain multicast-capable networks such as Ethernet do not require guaranteed delivery or acknowledgment of hello packets to and from neighbors, and is indicated as such inside the packet header. Packets that contain routing table updates do require acknowledgment.
- ◆ **DUAL finite-state machine:** Routing algorithm used by EIGRP to compute, select, and track loop-free routes. DUAL uses a metric to determine least-cost routes based on feasible successors. Feasible successors are considered guaranteed, loop-free routing neighbors that will be used to forward packets reliably to the end destination.
- ◆ **Protocol-dependent modules:** Independent modules used by a particular protocol at the OSI network layer for sending and receiving packets.

The IP protocol-dependent module for EIGRP is called IP-EIGRP and is tasked with delivering and receiving EIGRP packets encapsulated using IP. IP-EIGRP communicates with DUAL to compute routes that are then stored in the routing table.

Routing tables

Information regarding neighboring routers and the topology of the network is collected by EIGRP and is stored in a series of tables. Three main types of tables are used by EIGRP:

- ◆ **Neighbor table:** Contains information regarding neighboring routers that are accessible through directly connected interfaces. All collected information is added to the neighbor table, to include interface and addressing values. Each router running EIGRP maintains its own neighbor table. Thus:
 - Each router has a clear picture of its peer routers.
 - Each router has a clear picture of the network topology in its immediate vicinity.
- ◆ **Topology table:** A collection of EIGRP routing tables received from routing neighbors. The topology table lists EIGRP-routable destination networks and their metric calculations. If available, a successor and feasible successor are also listed for each destination in the topology table. Each destination is marked either in an active or passive state. A passive state means that the router knows the route to the destination, while an active state denotes a topology change in which the router is currently updating its routing information for a particular route. Each router running OSPF maintains its own link-state table. Thus:
 - Each router has a clear picture of the topology in the immediate vicinity of its neighbors.
 - Using the neighbor table and the link state, each router has a two-level knowledge of the network topology: the topology in its immediate vicinity and the topology in the vicinity of its neighbors.

For each destination network, the topology table keeps track of the following:

 - *The successor route:* This is the best route to the destination as evaluated by DUAL.
 - *The feasible successor route:* This is the next best route to the destination as evaluated by DUAL.
- ◆ **Routing table:** A map of all known destination routes. The routing table is built using information collected from the topology table. Whereas the neighbor and link-state tables are used to quantify routes, the routing table is used to qualify each route:
 - Only the *successor route* is copied from the topology table to the routing table, and this route is used as long as it's available.
 - Whenever the *successor route* is down, the *feasible successor route* is copied from the topology table to the routing table and is used as the alternate route.

Neighboring successors

There are two main types of neighboring devices (next-hop routers) are used in EIGRP-based networks. Both types guarantee that they will not be part of a routing loop:

- ◆ **Successor:** A next-hop router that provides the shortest distance to a destination network. In other words, this neighbor provides the best route to the destination network.
- ◆ **Feasible successor:** A next-hop router that provides the next shortest distance to a destination network. In other words, this neighbor provides the next best route to the destination network.

EIGRP packet types

EIGRP uses five types of packets:

- ◆ **Hello/ACKs:** Unacknowledged, multicast hello packets used in the process of neighbor discovery and recovery. Any hello packet empty of data is considered an acknowledgment, or ACK. ACKs are unicast addressed packets specified by a nonzero acknowledgment number.
- ◆ **Updates:** Reliable unicast packets that contain routing advertisements that are received by neighboring devices to build and maintain a map (routing table) of the network topology. If an update contains a cost change for a particular link, the update will be included in a multicast packet.
- ◆ **Queries:** Multicast packet queries transmitted when the destination node enters an active state. If the query is sent in response to a received query, it is formatted as a unicast packet.
- ◆ **Replies:** Reliable unicast packets transmitted in response to queries. Replies indicate to the originator that feasible successors are available and should not enter an active state.
- ◆ **Requests:** Unreliable multicast or unicast packets used to gather information from neighboring devices.

Convergence

EIGRP converges much faster than RIP and IGRP because neighbor routers only exchange “Hello” messages initially as opposed to typical distance vector routing protocols, which need to merge and distribute their routing tables among them during the convergence process.



Using EIGRP, the routers get to know each other during the convergence process, exchanging communication parameters and setting up their *neighbor table*. This is similar to OSPF and other link-state routing protocols' convergence process.

Two routers can only become neighbors if the following things occur:

- ◆ They successfully exchanged “Hello” messages.
- ◆ They have interfaces in the same routing domain (that is, in the same autonomous system).
- ◆ They use the same metrics: EIGRP uses bandwidth and delay metrics by default. If you decide to also use the optional metrics, such as load, reliability, and MTU, you need to do this on both routers.
- ◆ They have their hello timers set to same values for
 - The frequency at which routers send “Hello” messages to each other.
 - How long neighbors wait before they consider a router out of network.

Hello messages are not only sent during the convergence process but also afterward to keep track of which routers are still there in the network. If a router becomes unavailable and stops sending “Hello” messages, one of the hello timers defines how long neighbor routers wait for a “Hello” message before they consider the unavailable router out of the network.

Route updates

EIGRP continues to update routers about available routes after they have converged. This allows routers to maintain their *link-state tables*.

After they have built their neighbor and link-state tables, routers know their neighbors, the network topology in their immediate vicinity, and the network topology in the vicinity of their neighbors.

Next, each router evaluates the quality of each route registered in the link-state table. EIGRP uses DUAL (Diffusing Update Algorithm) to evaluate the quality of each route in the link-state table.

DUAL — Diffusing Update Algorithm

Cisco leverages the *Diffusing Update Algorithm*, shortly known as *DUAL*, to evaluate the quality of network routes maintained by EIGRP.

DUAL improves the efficiency of EIGRP over IGRP, most notably avoiding routing loops altogether. Here are some of the characteristics of DUAL:

- ◆ For each destination network, it calculates a *successor route* (the best route to the destination as evaluated by DUAL) and a *feasible successor route* (the next best route to the destination as evaluated by DUAL).
- ◆ DUAL supports variable-length subnet masking (VLSM), allowing EIGRP to route across networks with different subnets.
- ◆ DUAL provides alternate routes very quickly in case the best route to a destination is down. DUAL provides two features that enable a very quick alternate route calculation:
 - The successor and feasible successor routes: For each route, an alternate route is already available and ready to kick in.
 - If both the successor and the feasible successor routes are down, DUAL enables routers to communicate with their neighbors to find an alternate route.

Because neighbors also have a successor and a feasible successor route to each destination, an alternate route borrowed from a neighbor can be readily used to reach the destination network.

Classful and classless routing

EIGRP supports both classful and classless routing. By default, like RIPv1 and IGRP, EIGRP is a *classful routing protocol*:

- ◆ It does not send subnet information in the route updates.
- ◆ It automatically summarizes routes on boundary routers based on the IP address class that each network belongs to. For example, if a router sends an update for network 172.16.50.0, EIGRP summarizes this route to 172.16.0.0. This works if the router that receives the update is also in the 172.16.0.0 IP address class. Intermediary routers also need to be in the same IP address class.

EIGRP can be configured to run in classless mode by executing the `no auto-summary` Cisco IOS command in router configuration mode. *Classless routing protocols* have the following features:

- ◆ Send subnet information in the route updates.
- ◆ Do not automatically summarize routes on boundary routers based on the IP address class each network belongs to. For example, if a router sends an update for network 172.16.50.0, EIGRP does not summarize the route in classless mode; it really sends 172.16.50.0. This works even if

the router that receives the update, or the intermediary routers, are not in the 172.16.0.0 IP address class.

Networks that contain multiple subnets in different IP address classes are called *discontiguous networks*. Discontiguous networks require classless routing (that is, with RIPv2 and with EIGRP, you need to execute the `no auto-summary` command). You can still summarize routes manually.

You find out about manual route summarization in Book IV, Chapter 6. The OSPF protocol does not automatically summarize routes: OSPF is a classless routing protocol.

Configuring EIGRP

You configure EIGRP on a Cisco router similarly to RIP:

- ◆ Start up EIGRP on each router
- ◆ Enable EIGRP on interfaces on each router
- ◆ Configure EIGRP options

Figure 5-1 shows an example of a network that you will configure with EIGRP. This network spans three subnets:

- ◆ 192.168.25.0/24
- ◆ 192.168.67.0/24
- ◆ 51.10.1.0/24

Observe that these networks are in different IP address classes. Hence, this is a *discontiguous network*. You need to disable autosummarization of routes in this setup to set EIGRP in classless routing mode.

Start up EIGRP

To start EIGRP, you run the `router eigrp as_id` Cisco IOS command in global configuration mode.

The `as_id` is the autonomous system (AS) number, also known as the routing domain ID. You need to set a common autonomous system number on all routers that will exchange EIGRP routing data. EIGRP routing data can only be exchanged between routers with the same autonomous system number. The EIGRP AS is a number between 1 and 65535.

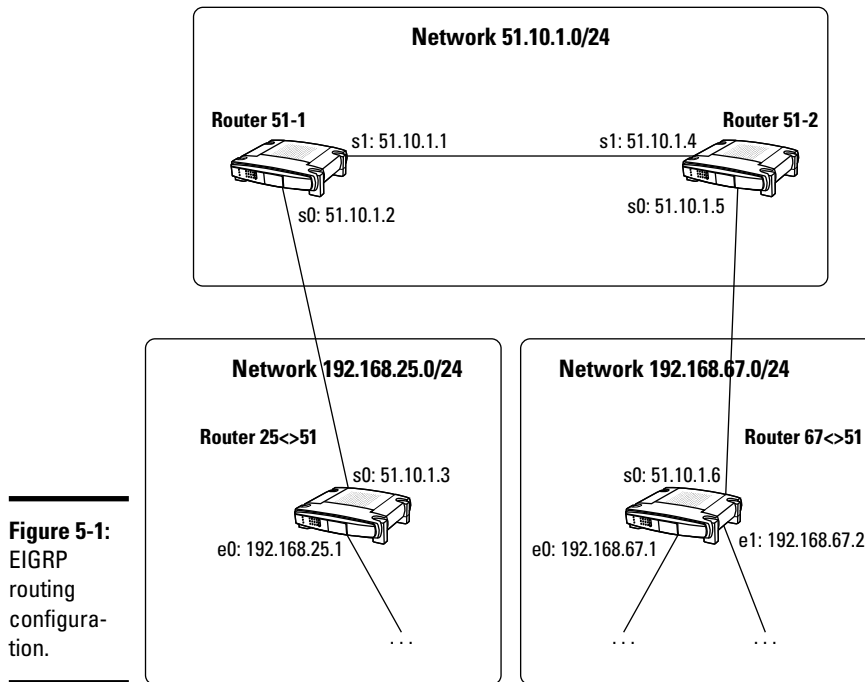


Figure 5-1:
EIGRP
routing
configura-
tion.

Enable EIGRP on router interfaces

To enable EIGRP on interfaces on your router, you run the `network int_IP` Cisco IOS command in global configuration mode.

The `int_IP` is the IP address that identifies the interface on which you enable OSPF.

Configuring EIGRP on Router 2551

```
R251>enable (or en)
R2551#configure terminal (or config t)
R2551(config)#router eigrp 1
R2551(config-router)#network 192.168.25.0
R2551(config-router)#network 51.0.0.0
R2551(config-router)#no auto-summary
R2551(config-router)#exit
R2551(config)#exit
R2551#disable
R2551>
```

Configuring EIGRP on Router 6751

```
R6751>enable (or en)
R6751#configure terminal (or config t)
R6751(config)#router eigrp 1
R6751(config-router)#network 192.168.67.0
R6751(config-router)#network 51.0.0.0
R6751(config-router)#no auto-summary
R6751(config-router)#exit
R6751(config)#exit
R6751#disable
R6751>
```

Configuring EIGRP on Router 51-1

```
R51-1>enable (or en)
R51-1#configure terminal (or config t)
R51-1(config)#router eigrp 1
R51-1(config-router)#network 51.0.0.0
R51-1(config-router)#no auto-summary
R51-1(config-router)#exit
R51-1(config)#exit
R51-1#disable
R51-1>
```

Configuring EIGRP on Router 51-2

```
R51-2>enable (or en)
R51-2#configure terminal (or config t)
R51-2(config)#router eigrp 1
R51-2(config-router)#network 51.0.0.0
R51-2(config-router)#no auto-summary
R51-2(config-router)#exit
R51-2(config)#exit
R51-2#disable
R51-2>
```

Verifying and Monitoring EIGRP Operation

You can verify a few elements to monitor EIGRP operation and ensure optimum routing.

Inspect the routing table

You look at the routing tables on a Cisco router using the `show ip route` Cisco IOS command in privileged EXEC mode. The output includes the following:

- ◆ Network IP information
- ◆ Available subnets

- ◆ Routes currently stored in the routing table. For each route, the command displays the following:
 - The IP address of the destination network reached by that route
 - The word *connected*, if the router you run the command on is directly connected to the destination network of that route
 - The IP address of the gateway (router) to the destination network of that route if the router you run the command on is not directly connected to the destination network of that route
 - The router interface that connects either to the destination network or to the gateway that reaches the destination network

Inspect EIGRP protocol configuration

You use the `show ip protocols` Cisco IOS command in privileged EXEC mode to look at the IP routing protocol configuration on a Cisco router.

The output displays one section for each IP routing protocol enabled on your router. For EIGRP, it shows the following:

- ◆ EIGRP process ID
- ◆ Whether an outgoing update filter is set
- ◆ Whether an incoming update filter is set
- ◆ Whether automatic network summarization is active
- ◆ Destination networks
- ◆ Information sources about destination networks
- ◆ Current administrative distances: internal and external

Inspect EIGRP topology table configuration

You use the `show ip eigrp topology` Cisco IOS command in privileged EXEC mode to look at the EIGRP topology table. The command displays the following:

- ◆ Destination networks and for each destination network:
 - *The successor route*: Shows the interface name and its IP address to reach that route
 - *The feasible successor route*: Shows the interface name and its IP address to reach that route
- ◆ Whether the destination network is A (active) or P (passive)

Passive destination networks are networks that converged. In other words, the successor and the feasible successor routes to that network have

converged. All routers know those routes; they are not exchanging route updates about them. After the routers have converged, destination networks show up as passive.

Active destination networks are networks that have not converged yet (the successor and the feasible successor routes to that network have not converged). Routers are still exchanging route updates about them. A destination network would show up as active, after routers have converged, if either the successor or the feasible successor route becomes unavailable and the router needs to exchange data with its neighbors about alternate routes to the destination network.

Inspect EIGRP neighbor information

You use the `show ip eigrp neighbors` Cisco IOS command in privileged EXEC mode to look at information about the EIGRP neighbors of your router. The command shows the following information:

- ◆ EIGRP process ID.
- ◆ Order of discovery of each neighbor.
- ◆ IP address of each neighbor.
- ◆ Interface reaching each neighbor.
- ◆ Hold time, also known as the Hello timer: This determines how long the router waits for a Hello message from its neighbor.
- ◆ SRTT — Smooth Round-Trip Timer: This is the time it takes for a packet to make a round trip from the router to the neighbor and back to the router.

This used to determine how long the router should wait for replies from its neighbor: It should wait at least as long as it takes a packet to do a round trip.

- ◆ RTO — Retransmission Timeout: This timeout value determines how long the router waits before retransmitting a packet for which it received no acknowledgment from its neighbor.
- ◆ Q Cnt — Queue Count: This shows how many packets are waiting to be sent in the router's queue.

If the queue count is consistently high, it shows that some communication problems exist between the router and its neighbor. One of the following is occurring:

- The router is sending too much to its neighbor.
- Its neighbor is not fast enough.
- Something is wrong with the link between the router and its neighbor.

Troubleshooting EIGRP

Whenever you notice EIGRP routing malfunctions, you use the `debug eigrp` Cisco IOS command in privileged EXEC mode to look at information about EIGRP operation on your router.

The `debug` command enables *debug mode* on specific components and protocols. In this case, you enable debug mode on EIGRP to capture detailed troubleshooting data about EIGRP. You execute the `debug eigrp` command in privileged EXEC mode.

To disable debugging, execute the `no debug eigrp` command in privileged EXEC mode.

Prep Test

- 1** EIGRP is which of the following?
 - A ☐ A distance vector protocol
 - B ☐ A proprietary protocol that was developed by Cisco
 - C ☐ An interior gateway protocol (IGP)
 - D ☐ All of the above
- 2** What does the EIGRP neighbor table keep track of?
 - A ☐ Routers in the vicinity of a router
 - B ☐ Neighboring cables in an unshielded twisted-pair (UTP)
 - C ☐ Patch panels in the vicinity of a router
 - D ☐ All of the above
- 3** What does the EIGRP topology table keep track of?
 - A ☐ The routes on neighbor patch panels
 - B ☐ Destination networks and best and next-best routes to them
 - C ☐ The cable links to the default gateway
 - D ☐ All of the above
- 4** How does EIGRP converge?
 - A ☐ Slowly, because it needs to merge routing tables from all routers and exchange them between all routers
 - B ☐ Quickly, because it only exchanges hello packets to allow routers to build their neighbor tables
 - C ☐ Never, because routers running EIGRP do not need to exchange information about their routes
 - D ☐ All of the above
- 5** To evaluate the quality of each route in the topology and routing tables, EIGRP uses which of the following?
 - A ☐ The Diffusing Update Algorithm (DUAL)
 - B ☐ The distance of the route
 - C ☐ Both the bandwidth and the distance of a route
 - D ☐ All of the above

- 6** EIGRP uses the _____ and the _____ metrics by default to calculate the quality of each route.
- A ☐ load, MTU
 - B ☐ reliability, load
 - C ☐ bandwidth, delay
 - D ☐ All of the above
- 7** Which of the following is an EIGRP feature?
- A ☐ Does not support route summarization
 - B ☐ Automatically summarizes routes by default, but can be configured for manual summarization as well
 - C ☐ Only summarizes feasible successor routes
 - D ☐ All of the above
- 8** EIGRP does which of the following?
- A ☐ Can leverage routes found by other routing protocols
 - B ☐ Communicates with RIP and IGRP on neighbor routers
 - C ☐ Shares its routing tables with RIP and IGRP
 - D ☐ All of the above
- 9** EIGRP can route packets for which of the following protocols?
- A ☐ IP (Internet Protocol)
 - B ☐ IPX (Novell Network Internetwork Packet Exchange) protocol
 - C ☐ AppleTalk protocol
 - D ☐ All of the above
- 10** You need to do which of the following to configure EIGRP in your network?
- A ☐ Start up EIGRP on each router in your network
 - B ☐ Enable EIGRP on interfaces on each router in your network
 - C ☐ Configure optional routing protocol parameters
 - D ☐ All of the above

Answers

- 1** B. EIGRP is a proprietary protocol that was developed by Cisco. Check out *"Characteristics of EIGRP."*
- 2** A. The EIGRP neighbor table keeps track of the routers in the vicinity of the router that owns the EIGRP neighbor table. Review *"Routing tables."*
- 3** B. The EIGRP topology table keeps track of the destination networks and best and next-best routes to them from the router that owns the EIGRP topology table. Look over *"Routing tables."*
- 4** B. EIGRP converges quickly because it only exchanges hello packets to allow routers to build their neighbor tables. See *"Convergence."*
- 5** A. EIGRP uses the Diffusing Update Algorithm (DUAL) to evaluate the quality of each route in the topology and routing tables. Check out *"DUAL — Diffusing Update Algorithm."*
- 6** C. EIGRP uses the bandwidth and the delay metrics by default to calculate the quality of each route. Read *"Characteristics of EIGRP."*
- 7** B. EIGRP automatically summarizes routes by default, but can be configured for manual summarization as well. Review *"Classful and classless routing."*
- 8** A. EIGRP can leverage routes found by other routing protocols. Refer to *"EIGRP Benefits."*
- 9** D. All of the above. EIGRP can route packets for IP, IPX, and AppleTalk. Check out *"EIGRP Benefits."*
- 10** D. All of the above. To configure EIGRP in your network, you need to start up EIGRP on each router in your network, enable EIGRP on interfaces on each router in your network, and configure optional routing protocol parameters. Look over *"Configuring EIGRP."*

Chapter 6: Open Shortest Path First (OSPF) Protocol

Exam Objectives

- ✓ Describing the features and characteristics of OSPF
- ✓ Describing OSPF routing decision criteria
- ✓ Describing OSPF route updates and convergence
- ✓ Distinguishing OSPF designated and backup designated routers
- ✓ Understanding the Dijkstra shortest path first (SPF) routing algorithm
- ✓ Describing OSPF route summarization
- ✓ Configuring OSPF on a Cisco router
- ✓ Verifying and troubleshooting OSPF on a Cisco router

OSPF is a link-state routing protocol. OSPF was developed based on an open standard and is supported by several router manufacturers. OSPF is widely used as an *interior gateway protocol (IGP)*, especially in large network environments. Interior gateway protocols, including OSPF, route within a single routing domain. A *single routing domain*, also known as an *autonomous system (AS)*, is a group of routers and network addresses that use a common routing system. For example, a network that uses OSPF on all routers is an autonomous system. This network can be connected to a large service provider network that is using another routing protocol such as *IS-IS (Intermediate System-to-Intermediate System)*. The service provider's IS-IS network is another autonomous system. The protocol used to route between autonomous systems and between large Internet service providers is called *Border Gateway Protocol (BGP)*. It is not necessary to know all the details about IGPs and BGPs, but it is important to know that OSPF is classified as an interior gateway protocol.

Introducing Open Shortest Path First (OSPF)

Link-state routing protocols build their routing tables independently based on route updates they receive from their neighbors. Link-state protocols do not merge the routing tables of neighbor routers. Link-state protocols enable routers to have a clear image of neighbors, network topology, and routes to their neighbors and beyond by maintaining not just routing tables

but also topology and neighbor tables. OSPF complies with all these link-state routing protocol characteristics.

Routing tables

OSPF maintains these routing tables:

- ◆ **Neighbor table:** This table keeps track of the neighbors of a router. Each router running OSPF maintains its own neighbor table. Thus, each router has a clear picture of its peer routers, and each router has a clear picture of the network topology in its immediate vicinity.
- ◆ **Link-state table:** This table keeps track of the state of the links on neighbor routers. In other words, this table keeps track of the state of the routes on neighbor routers. Each router running OSPF maintains its own link-state table. Thus:
 - Each router has a clear picture of the topology in the immediate vicinity of its neighbors.
 - Using the neighbor table and the link state, each router has a two-level knowledge of the network topology: the topology in its immediate vicinity and the topology in the vicinity of its neighbors.
- ◆ **Routing table:** This table keeps track of the metrics of each link tracked by the link-state table. Hence, whereas the neighbor and link-state tables are used to quantify routes, the routing table is used to qualify each route.

Characteristics of OSPF

Here are the main characteristics of the OPSF protocol:

- ◆ Route updates are only sent when routes change. Each router sends a *link-state advertisement (LSA)* whenever a change occurs in one of the routes known to the router.
- ◆ LSAs contain information about the route that changed only.
- ◆ Routers exchange “Hello” messages during the convergence process to build their neighbor tables.
- ◆ OSPF, like RIP, is supported on non-Cisco routers.
- ◆ OSPF supports variable-length subnet masking (VLSM).
- ◆ OSPF supports an unlimited number of network hops.
- ◆ OSPF scales out very well because
 - It divides the routing domain (autonomous system) into areas.
 - It classifies routers hierarchically.

- It converges very quickly.
- It sends routes updates (LSAs) only when routes change, minimizing route change traffic.
- LSA packets have a small footprint.
- LSA traffic is consolidated to the designated router.
- LSA traffic is minimized when routes are summarized.

Convergence

The OSPF routing protocol converges within seconds because neighbor routers only exchange “Hello” messages initially. During the convergence process, routers get to know each other, exchanging communication parameters and setting up their *neighbor table*.

Routers can only become neighbors if the following things occur:

- ◆ They have successfully exchanged “Hello” messages
- ◆ They have interfaces in the same routing domain (that is, in the same autonomous system)
- ◆ They have their hello timers set to the same values. Hello timers define the following:
 - The frequency at which routers send each “Hello” message to each other
 - How long neighbors wait before they consider a router out of network

Hello messages are not only sent during the convergence process but also afterward to keep track of which routers are still in the network. If a router becomes unavailable and stops sending Hello messages, one of the hello timers defines how long neighbor routers wait for a Hello message before they consider the unavailable router out of the network.

Route updates

OSPF continues to update routers about available routes after they have converged. These route updates are sent in the form of link-state advertisement (LSA) packets. Routers exchange LSA packets to maintain their *link-state tables*. After they have built their neighbor and link-state tables, routers know the following:

- ◆ Their neighbors
- ◆ The network topology in their immediate vicinity
- ◆ The network topology in the vicinity of their neighbors

Next, each router evaluates the quality of each route registered in the link-state table.

Cost metric

OSPF uses the *cost* metric to evaluate the quality of each link.

Route cost is a metric calculated based on the bandwidth of each link. Cisco routers calculate the cost by dividing a default bandwidth of 100 Mbps (100 million bits per second) by the actual bandwidth of the link.

For example, the following list illustrates the default OSPF cost calculated by Cisco routers for various bandwidths:

- ◆ 64-Kbps (64,536-bits-per-second) link: $100,000,000 / 64,536 = 1,562$
- ◆ 1.544-Mbps (T1) link: $100,000,000 / 1,544,000 = 64$
- ◆ 10-Mbps link: $100,000,000 / 10,000,000 = 10$
- ◆ 100-Mbps link: $100,000,000 / 100,000,000 = 1$
- ◆ 1-Gbps link: $100,000,000 / 1,000,000,000 = 0.1$
- ◆ 10-Gbps link: $100,000,000 / 10,000,000,000 = 0.01$

OSPF chooses the route with the lowest cost. You can modify the default reference bandwidth used to calculate the OSPF cost using the `auto-cost reference-bandwidth` Cisco IOS command in global configuration mode. It is very important to set the same reference bandwidth on all routers in your network.

For example, if most links in your network are 1 Gbps, you set the reference bandwidth to 1 Gbps instead of 100 Mbps using the following commands:

```
RT6751>enable (or en)
RT6751#configure terminal (or config t)
RT6751(config)#auto-cost reference-bandwidth 1000000000
RT6751(config)#exit
RT6751#disable
RT6751>
```

OSPF Routing Hierarchy

OSPF uses the *Dijkstra shortest path first (SPF)* routing algorithm to calculate the shortest path from a router to each destination network.

The Dijkstra SPF routing algorithm does the following:

- ◆ Considers the router to be the root of a tree
- ◆ Considers each destination network (router) to be a branch or a leaf in that tree
- ◆ Calculates the shortest route from the root of the tree (the router) to each branch and to each leaf (to each destination network)

Effectively, the Dijkstra SPF algorithm calculates the shortest route from each router to each network in the OSPF routing domain (or autonomous system), because each router is the root of its own tree. This creates a shortest-path tree for each router.

However, OSPF does not need to calculate the shortest path from each router to each destination if the network is designed in a hierarchical fashion.

Router trees overlap in a hierarchical design. This improves the efficiency of OSPF because after the Dijkstra SPF algorithm calculates the shortest routes for a branch of the tree, it doesn't need to recalculate those routes as you move up the tree to the root router.

Figure 6-1 shows the recommended network topology for OSPF.

Observe the following:

- ◆ One router is the root of the OSPF tree (although you can configure more than one root router).
- ◆ The OSPF routing domain (or autonomous system) is divided into areas with at least one *designated router (DR)* in each area. It is best practice to have a *backup designated router (BDR)* in each area as well.

In this example, the tree that starts at router 10-1, going down, is

- ◆ Part of the DR-10 router tree in area 10
- ◆ Part of the BDR-10 router tree in area 10
- ◆ Part of the root tree in the area 0

This is good, because after OSPF (the Dijkstra SPF algorithm) calculates the shortest route from router 10-1 to each destination underneath, the DR-10 router, the BDR-10 router, and the root router can readily use those shortest routes to destinations under the 10-1 router.

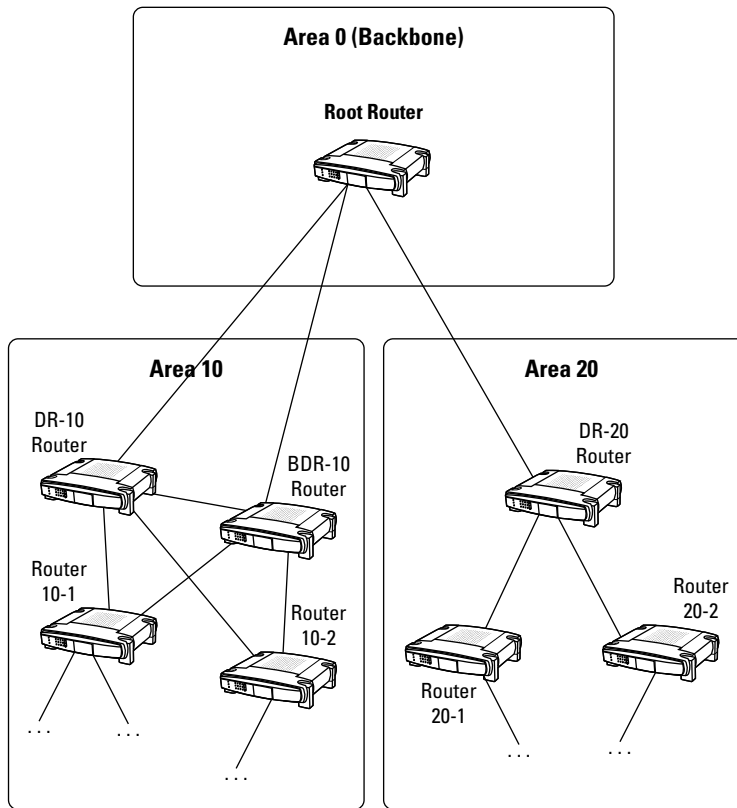


Figure 6-1:
OSPF
routing
hierarchy.

OSPF route summarization

The reuse of previously calculated shortest routes is leveraged by *route summarization*. Route summarization allows routers to identify common network IP address spaces and create a summarized route for the IP address space as opposed to creating a route for each IP address individually. This improves network throughput because routers sharing a summarized route send LSA packets upstream only when the summarized route changes, as opposed to sending LSA packets upstream for each of their (internal, or downstream) routes. For example, in Figure 6-1:

- ◆ The tree underneath router DR-10 is one IP address space (subnet).
- ◆ The tree underneath router BDR-10 is another IP address space (subnet).
- ◆ The tree underneath router 10-1 is one IP address space (subnet).
- ◆ The tree underneath router 10-2 is another IP address space (subnet).

However, the DR-10 tree includes the 10-1 and the 10-2 trees. Similarly, the BDR-10 tree includes the 10-1 and the 10-2 trees.

Suppose that networks in area 10 have the following IP addresses:

- ◆ Router DR-10: 172.10.75.0
- ◆ Router BDR-10: 172.10.76.0
- ◆ Router 10-1: 172.10.77.0
- ◆ Router 10-2: 172.10.78.0

The first 2 bytes are the same for all subnets in area 10: 172.10. The third byte is different. Table 6-1 examines these IP addresses in binary.

Table 6-1		Route Summarization		
IP Address	Byte 1 (172)	Byte 2 (10)	Byte 3 (75, 76, 77, 78)	Byte 4 (0)
172.10.75.0	1100 0000	0000 1010	0100 1011	0000 0000
172.10.76.0	1100 0000	0000 1010	0100 1100	0000 0000
172.10.77.0	1100 0000	0000 1010	0100 1101	0000 0000
172.10.78.0	1100 0000	0000 1010	0100 1110	0000 0000

Observe that the IP address of these networks is almost the same except for byte 3. Now from the perspective of the root router in area 0, this difference is irrelevant because the DR-10 and BDR-10 trees both include the 10-1 and the 10-2 trees. Hence, if the root router in area 0 knows how to get to DR-10 and to BDR-10, it knows how to get to everyone underneath. So, it makes sense to expose only one route up to the root router instead of exposing all four. That is exactly what route summarization accomplishes.

So how do you summarize these routes? Table 6-1 shows that only byte 3 varies. Specifically, only the second nibble in byte 3 varies. Assume that nibble 2 in byte 3 would be the same for all routers (for example, 0100 1011, which is 75). You would have IP address 172.10.75.0 for all networks. However, you can only do this if you modify the subnet mask.

The subnet mask changes from 255.255.255.0 (/24) to 255.255.240.0 (/20), because the variable part of the IP address now includes 4 more bits in byte 3. Table 6-2 details the following:

- ◆ The original subnet mask, where bytes 1 and 2 represent the network IP address and bytes 3 and 4 are used for variable intranetwork addresses.
- ◆ The new subnet mask for the summarized route, where byte 1 and the first nibble in byte 2 represent the network IP address. The second nibble of byte 2 and bytes 3 and 4 represent the variable intranetwork IP addresses.

Table 6-2 Subnet Mask for Summarized Route				
<i>Mask</i>	<i>Byte 1</i>	<i>Byte 2</i>	<i>Byte 3</i>	<i>Byte 4</i>
255.255.255.0	1111 1111	1111 1111	1111 1111	0000 0000
255.255.240.0	1111 1111	1111 1111	1111 0000	0000 0000

Now you can expose route 172.10.75.0/20 up to the root router in area 0. You are telling the root router in area 0 to keep track of route 172.10.75.0/20 to get to any of the networks in area 10.

In fact, you can have two summarized routes in this example, because both DR-10 and BDR-10 connect to the root router in area 0:

- ◆ One route to reach the tree under router DR-10: 172.10.75.0/20
- ◆ One route to reach the tree under router BDR-10: 172.10.76.0/20

Now instead of exposing four routes up to the root router in area 0, you only expose one (or two) summarized routes. This improves the efficiency of the root router because it needs to maintain only one (or two) route(s) for area 10 instead of maintaining four routes.

OSPF designated router (DR)

The OSPF protocol elects a *designated router* that is responsible for keeping all routers updated on shortest routes. Instead of exchanging route information with every other router in the network, routers only communicate their routes to the designated router. The designated router then updates everyone on the routes available. Consolidating the exchange of information about routes to the designated router improves the efficiency of the network because less bandwidth is consumed by having each router communicate its routes only to the designated router, instead of communicating with every other router in their area.

Routers send their LSA packets to a multicast address (224.0.0.6). The DR listens to this multicast IP address. The DR relays routing information back to

the routers by sending route updates to the multicast address 224.0.0.5. All routers running OSPF are listening to the 224.0.0.5 multicast IP address.

Selecting a designated router

The designated router is elected based on the *OSPF priority*. The OSPF priority is a value between 0 and 255 assigned to a router interface using the `ip ospf priority value` Cisco IOS command. The default OSPF priority is set to 1.

The router with the highest OSPF priority becomes the designated router. If two routers have the same OSPF priority, the *router ID (RID)* is used to decide which one becomes the DR.



It is best practice to configure a core router — or the largest, most highly available, and most powerful router — in your network to be the designated router. You can control which router is elected DR using either of the following:

- ◆ **Loopback interfaces:** Create loopback interfaces on each router in your network, and set the highest IP address on the one you want to become the DR.
- ◆ **OSPF priority:** Set the highest OSPF priority on the router and interface you want to become the DR.

Router ID (RID)

The router ID is one of the IP addresses of the router that has been chosen to identify the router. The IP address can be set by one of the following methods:

- ◆ Manually, using the `router-id` Cisco IOS command
- ◆ Automatically, using either
 - The highest IP address assigned to a loopback interface on your router
 - The highest IP address of an active interface on your router

Keep in mind that if a loopback interface is defined, its IP address is used as the router ID, even if it is not the highest IP address defined on the router.

Creating loopback interfaces

Loopback interfaces are software-based logical interfaces that point back to the router where they are created. These interfaces are used as interface support for certain features, including the OSPF DR/BDR election process.

To create a loopback interface on your router, use the `int loopback` Cisco IOS command in global configuration mode. You need to assign an IP address to your loopback interface. However, the IP address you assign is not really important:

- ◆ The loopback interface is local to your router: The IP interface is not visible to other routers, switches, or hosts on the network as a normal physical interface is.
- ◆ Even if the IP address is lower than another IP address on your router, the router always uses a loopback interface, if available, to set its RID before the IP addresses of any physical interface are compared.

OSPF backup designated router (BDR)

The backup designated router becomes the designated router in case the designated router is down. The BDR receives the route updates (LSA packets) that routers send to the DR. In fact, routers send their LSA packets to a multicast address (224.0.0.6). Both the DR and the BDR listen to the multicast address 224.0.0.6. Hence, both the DR and the BDR receive the LSA packets. The routing information is in sync on the DR and on the BDR.

The router with the second-highest OSPF priority becomes the backup designated router.

Configuring OSPF

You configure OSPF on a Cisco router similarly to RIP and EIGRP. Follow these steps:

1. Start up OSPF on each router.
2. Enable OSPF on interfaces on each router.
3. Configure OSPF options.

The following sections outline the details of these steps.

Start up OSPF

To start OSPF, run the `router ospf process_id` Cisco IOS command in global configuration mode.

The `process_id` is a number between 1 and 65536 that identifies the OSPF routing process on the router. The OSPF process ID can be a different number on routers that communicate using OSPF.

Enable OSPF on router interfaces

To enable OSPF on the interfaces of your router, run the `network int_IP wildcard_mask area area_id` Cisco IOS command in global configuration mode:

- ◆ The `int_IP` portion is the IP address that identifies the interface on which you enable OSPF.
- ◆ The `wildcard_mask` portion identifies which IP addresses are part of this network. In other words, OSPF exposes to a certain network area all interfaces identified by the IP addresses represented by the wildcard mask. For example, the `172.10.75.0 0.0.0.255 int_IP wildcard_mask` combination configures the router to expose all addresses in the space 172.10.75: any router interface in the 172.10.75 network.
- ◆ The `area area_id` portion is the OSPF operation area. Recall that OSPF divides the routing domain (or autonomous system) into areas.

Understanding wildcards

The `172.10.75.0 0.0.0.255 int_IP/wildcard_mask` combination configures the router to expose all addresses in the space 172.10.75: any router interface in the 172.10.75 network. Read on to find out more about wildcards.

Wildcards are essentially bit masks. A *bit mask* is a set of bits that are either 0 or 1. In this case, OSPF wildcard bits have the following meaning:

- ◆ Number 0 means to match exactly the corresponding bit in the IP address.
- ◆ Number 1 means that the corresponding bit in the IP address can be any number.

If you look at the IP address as a whole, divided into 4 bytes (8 bits each), you can specify wildcards between 0.0.0.0 and 255.255.255.255 with the `network` command:

- ◆ Number 0 means to match exactly the corresponding byte in the IP address. Here, a 0 in decimal represents eight 0s in binary.
- ◆ Number 255 means that the corresponding byte in the IP address can be any number. Here, 255 in decimal represents eight 1s in binary.

For example, wildcard 0.0.0.0 matches exactly the IP address specified in the `network` command. In other words, if you use `172.10.75.0 0.0.0.0`, only address 172.10.75.0 is exposed as a route. This may be what you want in some cases. However, usually you want to match a range of addresses as

opposed to a specific address when using the `network` command. In other words, you tell OSPF to expose all router interfaces that match the wildcard.

Referring to Figure 6-1, recall the IP addresses of each router:

- ◆ Router DR-10: 172.10.75.0
- ◆ Router BDR-10: 172.10.76.0
- ◆ Router 10-1: 172.10.77.0
- ◆ Router 10-2: 172.10.78.0

The following sections describe configuring OSPF on router interfaces in area 10.

Enable and configure OSPF on router DR-10

```
DR-10>enable (or en)
DR-10#configure terminal (or config t)
DR-10(config)#router ospf 1
DR-10(config-router)#network 172.10.75.0 0.0.0.255 area 10
DR-10(config-router)#network 172.10.75.0 0.0.15.255 area 0
DR-10(config-router)#exit
DR-10(config)#exit
DR-10#disable
DR-10>
```

You configure the DR-10 router to expose interfaces to area 10 and to area 0:

- ◆ **Area 10:** DR-10 exposes to area 10 any address in the IP space 172.10.75: any router interface in the 172.10.75 network using the 172.10.75.0 0.0.0.255 IP/wildcard_mask combination.
- ◆ **Area 0:** DR-10 exposes to area 0 any address in the IP space 172.10.7_: any IP address that starts with 172.10.7. In other words, you expose to area 0 a summary route that reaches area 10. You use the 172.10.75.0 0.0.15.255 IP/wildcard_mask combination.

So, why did you use a 0.0.15.255 wildcard here? Consider the subnet mask of the summary route that you determined earlier (255.255.240.0), which is shown in binary in Table 6-3.

Table 6-3 Subnet Mask for Summarized Route				
<i>Subnet Mask</i>	<i>Byte 1</i>	<i>Byte 2</i>	<i>Byte 3</i>	<i>Byte 4</i>
255.255.240.0	1111 1111	1111 1111	1111 0000	0000 0000

This subnet mask tells the router that this summarized route represents an IP address space with

- ◆ Byte 1 constant: 172
- ◆ Byte 2 constant: 10
- ◆ Byte 3, nibble 1 constant: 7
- ◆ Byte 3, nibble 2 variable: 5 to 8
- ◆ Byte 4 variable: any number (0 to 254)

To represent the same filter with a wildcard mask, you need to replace all 0s with 1s and all 1s with 0s, because in a wildcard, 0 means “match exactly” and 1 means “could be anything.” The wildcard value is shown in Table 6-4.

Table 6-4 Wildcard Mask for Summarized Route				
Wildcard Mask	Byte 1	Byte 2	Byte 3	Byte 4
0.0.15.255	0000 0000	0000 0000	0000 1111	1111 1111

Next, you need to run similar configuration commands on routers BDR-10, 10-1, and 10-2.

Enable and configure OSPF on router BDR-10

```
BDR-10>enable (or en)
BDR-10#configure terminal (or config t)
BDR-10(config)#router ospf 1
BDR-10(config-router)#network 172.10.76.0 0.0.0.255 area 10
BDR-10(config-router)#network 172.10.75.0 0.0.15.255 area 0
BDR-10(config-router)#network 172.10.75.0 0.0.0.255 area 10
BDR-10(config-router)#exit
BDR-10(config)#exit
BDR-10#disable
BDR-10>
```

Router BDR-10, like router DR-10, exposes interfaces to area 10 and to area 0, because it connects both to area 10 and to area 0. Router BDR-10 also defines a route to router DR-10 (172.10.75.0) by registering a route with the 172.10.75.0 0.0.0.255 IP/wildcard_mask combination.

Enable and configure OSPF on router 10-1

```
10-1>enable (or en)
10-1#configure terminal (or config t)
10-1(config)#router ospf 1
10-1(config-router)#network 172.10.77.0 0.0.0.255 area 10
```

```
10-1(config-router)#network 172.10.75.0 0.0.0.255 area 10
10-1(config-router)#network 172.10.76.0 0.0.0.255 area 10
10-1(config-router)#exit
10-1(config)#exit
10-1#disable
10-1>
```

Router 10-1 exposes interfaces to area 10 only because it doesn't connect to area 0. Router 10-1 also defines routes to router DR-10 (172.10.75.0) and to router BDR-10 (172.10.76.0) using the 172.10.75.0 0.0.0.255 and the 172.10.76.0 0.0.0.255 IP/wildcard_mask combinations, respectively.

Enable and configure OSPF on router 10-2

```
10-2>enable (or en)
10-2#configure terminal (or config t)
10-2(config)#router ospf 1
10-2(config-router)#network 172.10.78.0 0.0.0.255 area 10
10-2(config-router)#network 172.10.75.0 0.0.0.255 area 10
10-2(config-router)#network 172.10.76.0 0.0.0.255 area 10
10-2(config-router)#exit
10-2(config)#exit
10-2#disable
10-2>
```

In this configuration, router 10-2, like router 10-1, does the following:

- ◆ Exposes interfaces to area 10 only, because it doesn't connect to area 0.
- ◆ Defines a route to router DR-10 (172.10.75.0) using the 172.10.75.0 0.0.0.255 IP/wildcard_mask combination
- ◆ Defines a route to router BDR-10 (172.10.76.0) using the 172.10.76.0 0.0.0.255 IP/wildcard_mask combination

Configure OSPF options

Now you can configure optional parameters to customize the operation of OSPF on your routers.

OSPF priority

You can manually set the *OSPF priority* of a router interface using the `ip ospf priority value` Cisco IOS command in global configuration mode.

Changing the OSPF priority allows you to control the OSPF DR (designated router) and BDR (backup designated router) election process. OSPF elects the DR and the BDR based on the OSPF priority of the router interface.

OSPF cost

You can manually set the *OSPF cost* of an interface on your router using the `ip ospf cost value` Cisco IOS command in global configuration mode.

Verifying and Monitoring OSPF Operation

You can verify the following elements to monitor OSPF operation and ensure optimum routing:

- ◆ Inspect the routing table
- ◆ Inspect the OSPF protocol configuration
- ◆ Inspect the OSPF interface configuration
- ◆ Inspect the OSPF neighbor information
- ◆ Inspect the OSPF routing database

Inspect the routing table

This is not an OSPF-specific technique: Inspecting the routing table shows you all IP routing protocols enabled on your router and the state of their routing tables. You look at the routing tables on a Cisco router using the `show ip route` Cisco IOS command in privileged EXEC mode. The output includes the following:

- ◆ Network IP information
- ◆ Available subnets
- ◆ Routes currently stored in the routing table

For each route, the command displays these items:

- The IP address of the destination network reached by that route
- The word *connected*, if the router you run the command on is directly connected to the destination network of that route
- The IP address of the gateway (router) to the destination network of that route if the router you run the command on is not directly connected to the destination network of that route
- The router interface that connects either to the destination network or to the gateway that reaches the destination network

Inspect the OSPF protocol configuration

This is not an OSPF-specific technique: Inspecting the IP routing protocols shows you all IP routing protocols enabled on your router and their configuration. You use the `show ip protocols` Cisco IOS command in privileged EXEC mode to look at the IP routing protocol configuration on a Cisco router. The output displays one section for each IP routing protocol enabled on your router. For OSPF, it shows these items:

- ◆ OSPF process ID
- ◆ Whether an outgoing update filter is set
- ◆ Whether an incoming update filter is set
- ◆ RID (router ID)
- ◆ Number of OSPF areas active on the router where you run the command
- ◆ IP and OSPF area of networks registered for OSPF routing
- ◆ Reference bandwidth used to calculate the cost of each route
- ◆ Routing information sources: neighbor routers that exchange OSPF LSA packets with the router where you run the command
- ◆ Current administrative distance

Inspect the OSPF interface configuration

You use the `show ip ospf interface` Cisco IOS command in privileged EXEC mode to look at interface-specific OSPF configuration:

- ◆ If you run the command specifying a particular interface, it shows data only about that interface.
- ◆ Otherwise, the command displays one section for each interface enabled for OSPF on your router.

Inspect the OSPF neighbor information

You use the `show ip ospf neighbor` Cisco IOS command in privileged EXEC mode to look at information about the OSPF neighbors of your router.

Inspect the OSPF routing database

You use the `show ip ospf database` Cisco IOS command in privileged EXEC mode to inspect data stored in the OSPF routing database. The command displays information about neighboring routers and the state of the links to them.

Troubleshooting OSPF

Whenever you notice routing malfunctions that are related to OSPF, you use the `debug ip ospf` Cisco IOS command in privileged EXEC mode to look at information about the OSPF operation on your router.

The `debug` command enables *debug mode* on specific components and protocols. In this case, you enable debug mode on the OSPF protocol to capture detailed troubleshooting data about OSPF. You execute the `debug ip ospf` command in privileged EXEC mode.

To disable debugging, execute the `no debug ip ospf` command in privileged EXEC mode.

Prep Test

- 1 The OSPF protocol is which of the following?**
 - A ☐ A link-state protocol
 - B ☐ A protocol that was developed based on open standards
 - C ☐ An interior gateway protocol (IGP)
 - D ☐ All of the above
- 2 What does the OSPF neighbor table keep track of?**
 - A ☐ Routers in the vicinity of a router
 - B ☐ Neighboring cables in an unshielded twisted-pair (UTP)
 - C ☐ Patch panels in the vicinity of a router
 - D ☐ All of the above
- 3 What does the OSPF link-state table keep track of?**
 - A ☐ The state of the links on neighbor patch panels
 - B ☐ The state of the routes on neighbor routers
 - C ☐ The state of the cable links to the default gateway
 - D ☐ All of the above
- 4 What does the OSPF routing table keep track of?**
 - A ☐ Metrics for each link on neighbor patch panels
 - B ☐ Metrics for each cable link to the default gateway
 - C ☐ Metrics for each route on neighbor routers
 - D ☐ All of the above
- 5 Describe OSPF link-state advertisement (LSA) packets.**
 - A ☐ They are sent whenever a route changes.
 - B ☐ They contain information about the route that changed only.
 - C ☐ They are sent by the route that detected a change in the state of one of its directly connected routes.
 - D ☐ All of the above.

6 How does OSPF converge?

- A ☐ Slowly, because it needs to merge routing tables from all routers and exchange them between all routers
- B ☐ Quickly, because it only exchanges hello packets to allow routers to build their neighbor tables
- C ☐ Never, because routers running OSPF do not need to exchange information about their routes
- D ☐ All of the above

7 Using OSPF, routers have knowledge about which of the following?

- A ☐ The network topology in their immediate vicinity
- B ☐ Their neighbors
- C ☐ The network topology in the vicinity of their neighbors
- D ☐ All of the above

8 How is the OSPF cost metric calculated?

- A ☐ Based on the bandwidth of the route
- B ☐ Based on the distance of the route
- C ☐ Based on both the bandwidth and the distance of a route
- D ☐ All of the above

9 OSPF uses the *Dijkstra shortest path first (SPF)* routing algorithm to calculate the shortest path from a router to each destination network. The Dijkstra SPF algorithm does which of the following?

- A ☐ Considers each router to be the root of a tree
- B ☐ Considers each destination network (router) to be a branch or a leaf in that tree
- C ☐ Calculates the shortest route from the root of the tree (the router) to each branch and to each leaf (to each destination network)
- D ☐ All of the above

10 You need to do which of the following to configure OSPF in your network?

- A ☐ Start up OSPF on each router in your network
- B ☐ Enable OSPF on interfaces on each router in your network
- C ☐ Configure optional routing protocol parameters
- D ☐ All of the above

Answers

- 1 D. All of the above. The OSPF protocol is a link-state protocol, a protocol that was developed based on open standards, and an interior gateway protocol (IGP). Refer to *"Introducing Open Shortest Path First (OSPF)."*
- 2 A. The OSPF neighbor table keeps track of routers in the vicinity of the router that owns the neighbor table. Review *"Routing tables."*
- 3 B. The OSPF link-state table keeps track of the state of the routes on neighbor routers. Check out *"Routing tables."*
- 4 C. The OSPF routing table keeps track of the metrics for each route on neighbor routers. Read *"Routing tables."*
- 5 D. All of the above. OSPF link-state advertisement (LSA) packets are sent whenever a route changes. They contain information about the route that changed only, and they are sent by the route that detected a change in the state of one of its directly connected routes. Refer to *"Route updates."*
- 6 B. OSPF converges quickly because it only exchanges hello packets to allow routers to build their neighbor tables. Look over *"Convergence."*
- 7 D. All of the above. Using OSPF, routers have knowledge about their neighbors, the network topology in their immediate vicinity, and the network topology in the vicinity of their neighbors. Review *"Route updates."*
- 8 A. The OSPF cost metric is based on the bandwidth of the route. See *"Cost metric."*
- 9 D. All of the above. The Dijkstra SPF algorithm considers each router to be the root of a tree and considers each destination network (router) to be a branch or a leaf in that tree. It then calculates the shortest route from the root of the tree (the router) to each branch and to each leaf (each destination network). Look over *"OSPF Routing Hierarchy."*
- 10 D. All of the above. To configure OSPF in your network, you need to start up OSPF on each router, enable OSPF on interfaces on each router, and configure optional routing protocol parameters. Refer to *"Configuring OSPF."*