CHAPTER 2

# Static Routing

## Objectives

Upon completion of this chapter, you should be able to answer the following questions:

- What is the role of a router in the network?
- Can you describe the relationship between router interfaces, directly connected networks, and the routing table?
- How can CDP be used with directly connected networks?
- How can static routes be used with exit interfaces?
- Can you describe the use and configuration of summary and default routes?
- How do packets get forwarded using static routes?
- What commands would you use to manage and troubleshoot static routes?

## Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary at the end of the book.

*smart serial* *page 74*

*neighbors* *page 103*

*stub network* *page 108*

*stub router* *page 108*

*recursive route lookup* *page 117*

*summary route* *page 127*

*route summarization* *page 127*

*quad-zero route* *page 132*

Routing is at the core of every data network, moving information across an internetwork from source to destination. Routers are the devices responsible for the transfer of packets from one network to the next.

As you learned in the previous chapter, routers learn about remote networks either dynamically using routing protocols or manually using static routes. A remote network is a network that is not one of the router's directly connected networks. In many cases, routers use a combination of both dynamic routing protocols and static routes. This chapter focuses on static routing.

Static routes are very common and do not require the same amount of processing and overhead as do dynamic routing protocols.

This chapter follows a sample topology as you learn to configure static routes and learn troubleshooting techniques. In the process, you will examine several key IOS commands and the results they display. You will also learn about the routing table using both directly connected networks and static routes.

As you work through the Packet Tracer Activities associated with these commands, take the time to experiment with the commands and examine the results. Reading the routing tables will soon become second nature.

## Routers and the Network

Routers have always played a key role in larger networks and the Internet. Over the last several years, routers have become more common in smaller and home networks. This is because of several reasons, including the need to connect multiple devices to the Internet, security, and quality of service.

### Role of the Router

The router is a special-purpose computer that plays a key role in the operation of any data network. Routers are primarily responsible for interconnecting networks by

- Determining the best path to send packets
- Forwarding packets toward their destination

Routers make routing decisions by learning about remote networks and maintaining routing information. The router is the junction or intersection that connects multiple IP networks. The router's primary forwarding decision is based on Layer 3 information, the destination IP address.

The router's routing table is used to find the best match between the destination IP of a packet and a network address in the routing table. The routing table will ultimately determine the exit interface to forward the packet from, and the router will encapsulate that packet in the appropriate data-link frame for that outgoing interface.

## Introducing the Topology

Figure 2-1 shows the topology used in this chapter. The topology consists of three routers, labeled R1, R2, and R3. Routers R1 and R2 are connected through one WAN link, and routers R2 and R3 are connected through another WAN link. Each router is connected to a different Ethernet LAN, represented by a switch and a PC. Table 2-1 outlines the addressing scheme of these devices.

**Figure 2-1** Chapter Topology

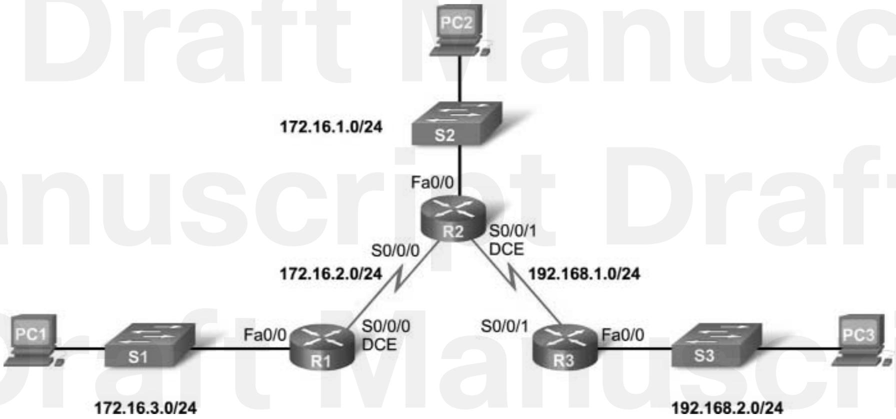


**Table 2-1** Chapter Topology Addressing Scheme

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | Fa0/0 | 172.16.3.1 | 255.255.255.0 | — |
| | S0/0/0 | 172.16.2.1 | 255.255.255.0 | — |
| R2 | Fa0/0 | 172.16.1.1 | 255.255.255.0 | — |
| | S0/0/0 | 172.16.2.2 | 255.255.255.0 | — |
| | S0/0/1 | 192.168.1.2 | 255.255.255.0 | — |
| R3 | Fa0/0 | 192.168.2.1 | 255.255.255.0 | — |
| | S0/0/0 | 192.168.1.1 | 255.255.255.0 | — |
| PC1 | NIC | 172.16.3.10 | 255.255.255.0 | 172.16.3.1 |
| PC2 | NIC | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| PC3 | NIC | 192.168.2.10 | 255.255.255.0 | 192.168.2.1 |

Each router in this example is a Cisco 1841. A Cisco 1841 router has the following interfaces:

- Two Fast Ethernet interfaces: FastEthernet 0/0 and FastEthernet 0/1
- Two serial interfaces: Serial 0/0/0 and Serial0/0/1

The interfaces on your routers can vary from those on the 1841, but you should be able to follow the commands in this chapter—with some slight modifications—and complete the hands-on labs. In addition, Packet Tracer Activities are referenced throughout the discussion of static routing so that you can practice skills as they are presented. Lab 2-1: Basic Static Route Configuration (2.8.1) mirrors the topology, configurations, and commands discussed in this chapter.

## Examining the Connections of the Router

Unlike most user PCs, a router will have multiple network interfaces. These interfaces can include a variety of connectors.

### Router Connections

Connecting a router to a network requires a router interface connector to be coupled with a cable connector. As you can see in Figure 2-2, Cisco routers support many different connector types.

### Serial Connectors

Figure 2-2 shows various LAN and WAN connectors. For WAN connections, Cisco routers support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 standards for serial connections, as shown. Memorizing these connection types is not important. Just know that a router has a DB-60 port that can support five different cabling standards. Because five different cable types are supported with this port, the port is sometimes called a five-in-one serial port. The other end of the serial cable is fitted with a connector that is appropriate to one of the five possible standards.

**Note**

The documentation for the device to which you want to connect should indicate the standard for that device.

**Figure 2-2** Connections and Connectors

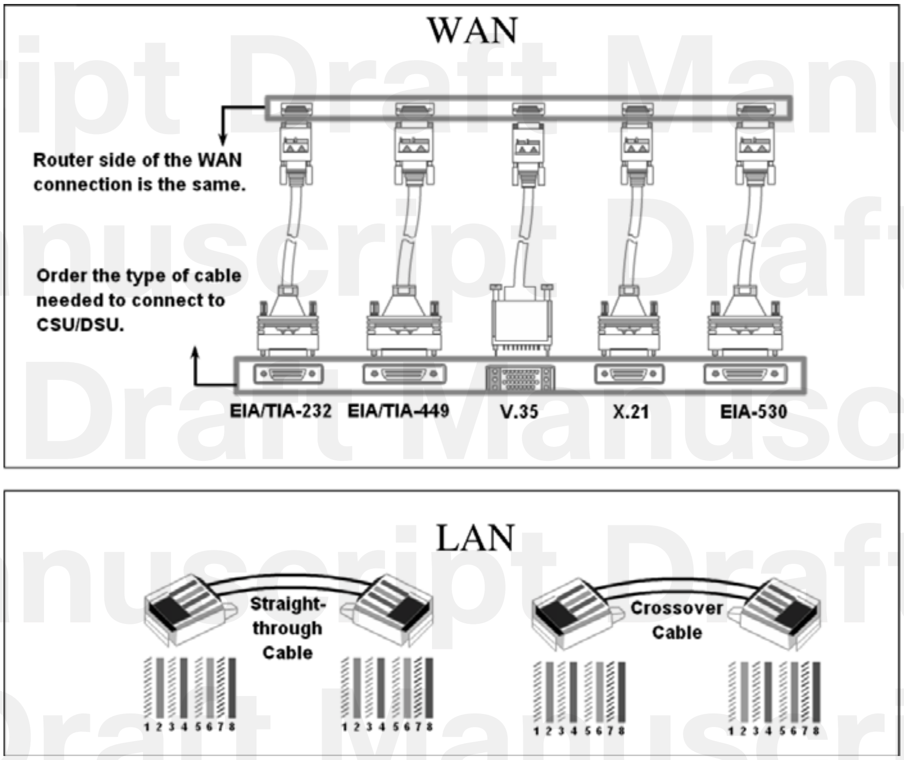
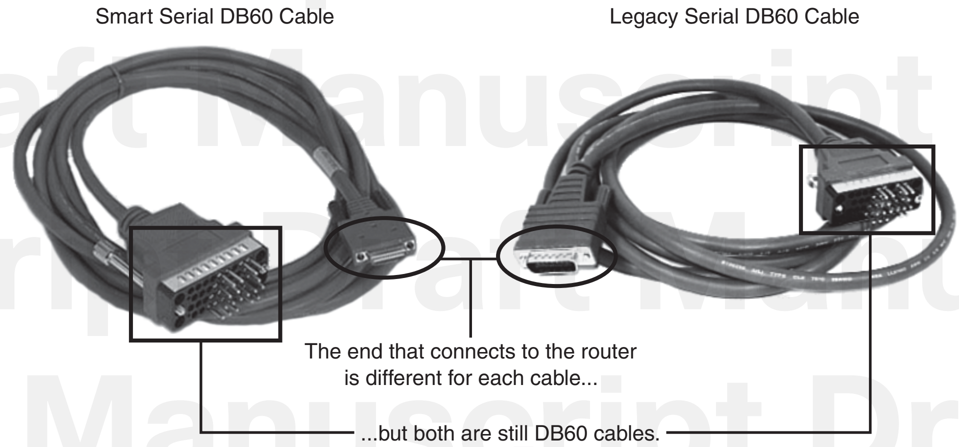


Figure 2-3 shows the two types of DB-60 serial connectors commonly used with Cisco router serial interfaces.

**Figure 2-3** DTE Serial DB-60 Cables



If your lab has 2500 series routers, you will use the cable on the right with the larger router connector. Newer routers support the ***smart serial*** interface, which allows more data to be forwarded across fewer cable pins. Your lab might have this type of cable to support 1700, 2600, and 1800 platforms. The serial end of the smart serial cable is a 26-pin connector. It is much smaller than the DB-60 connector used to connect to a five-in-one serial port. These transition cables support the same five serial standards and are available in either data terminal equipment (DTE) or data communications equipment (DCE) configurations.

**Note**

For a thorough explanation of DTE and DCE, see Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).

These cable designations are only important to you when configuring your lab equipment to simulate a "real-world" environment. In a production setting, the cable type is determined for you by the WAN service you are using.

## Ethernet Connectors

A different connector is used in an Ethernet-based LAN environment (see Figure 2-4). An RJ-45 connector for the unshielded twisted-pair (UTP) cable is the most common connector used to connect LAN interfaces. At each end of an RJ-45 cable, you should be able to see eight colored wires, or conductors, ending in eight metal pins or contacts. An Ethernet cable uses pins 1, 2, 3, and 6 for transmitting and receiving data.

**Figure 2-4** TIA/EIA 568B UTP Ethernet Cable

Two types of cables can be used with Ethernet LAN interfaces:

- A straight-through, or patch, cable, with the order of the colored pins the same on each end of the cable
- A crossover cable, with pin 1 connected to pin 3 and pin 2 connected to pin 6

Straight-through cables are used for the following connections:

- Switch-to-router
- Hub-to-router

- Switch-to-PC/server
- Hub-to-PC/server

Crossover cables are used for the following connections:

- Switch-to-switch
- PC/server-to-PC/server
- Switch-to-hub
- Hub-to-hub
- Router-to-router
- Router-to-PC/server

**Note**

Wireless connectivity is discussed in another course.

Packet Tracer
☐ **Activity**

**Build the Chapter Topology (2.1.3)**

Use the Packet Tracer Activity to build the topology that you will use for the rest of this chapter. You will add all the necessary devices and connect them with the correct cabling. Use file e2-213.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

# Router Configuration Review

To configure static routing and dynamic routing protocols, you only need to know the basic IOS commands. You should already be familiar with these commands. The following sections are only meant as a review. For more detailed explanations, see Chapter 1, "Introduction to Routing and Packet Forwarding," and the Network Fundamentals, CCNA Exploration course.

## Examining Router Interfaces

As you learned in Chapter 1, the **show ip route** command is used to display the routing table. Initially, the routing table is empty if no interfaces have been configured.

As you can see in Example 2-1, the routing table for R1, no interfaces have been configured with an IP address and subnet mask.

**Example 2-1** Routing Table Has No Routes

```
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R1#
```

**Note**

Static routes and dynamic routes cannot be added to the routing table until the appropriate local interfaces, also known as the exit interfaces, have been configured on the router. This procedure will be examined more closely in later chapters.

## Interfaces and Their Statuses

The status of each interface can be examined by using several commands.

Example 2-2 displays the **show interfaces** command for R1. The **show interfaces** command shows the status and gives a detailed description for all interfaces on the router.

**Example 2-2** **show interfaces** Command Output Provides Detailed Interface Information

```
R1# show interfaces

FastEthernet0/0 is administratively down, line protocol is down
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
```

```
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0/0 is administratively down, line protocol is down
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
     DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
<remaining output omitted for brevity>
R1#
```

Only the first two interfaces are shown. But as you can see, the output from the command can be rather lengthy. To view the same information, but for a specific interface, such as FastEthernet 0/0, use the **show interfaces** command with a parameter that specifies the interface. For example:

```
R1# show interfaces fastethernet 0/0

FastEthernet0/0 is administratively down, line protocol is down
<remaining output omitted for brevity>
```

Notice that the interface is administratively down and the line protocol is down. Administratively down means that the interface is currently in the shutdown mode, or turned off. Line protocol down means, in this case, that the interface is not receiving a carrier signal from a switch or the hub. This condition might also be because of the fact that the interface is in shutdown mode.

You will notice that the **show interfaces** command does not show any IP addresses on R1's interfaces. This is because you have not yet configured IP addresses on any of the interfaces.

## Additional Commands for Examining Interface Status

Example 2-3 displays the **show ip interface brief** command output for R1. This command can be used to see a portion of the interface information in a condensed format.

**Example 2-3** Summary of Interface Status with the **show ip interface brief** Command

```
R1# show ip interface brief

Interface         IP-Address    OK?   Method   Status                  Protocol
FastEthernet0/0   unassigned    YES   manual   administratively down   down
Serial0/0         unassigned    YES   unset    administratively down   down
FastEthernet0/1   unassigned    YES   unset    administratively down   down
Serial0/1         unassigned    YES   unset    administratively down   down
```

Example 2-4 displays the **show running-config** command output for R1.

**Example 2-4** Interface Information with the **show running-config** Command

```
R1# show running-config
!
version 12.3
!
```

```
hostname R1
!
!
enable secret 5 $1$.3RO$VLUOdBF2OqNBn0EjQBvR./
!
!
interface FastEthernet0/0
 mac-address 000c.3010.9260
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 mac-address 000c.3010.9261
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

The **show running-config** command is used to display the current configuration file that the router is using. Configuration commands are temporarily stored in the running configuration file and implemented immediately by the router. Using this command is another way to verify the configuration of an interface such as FastEthernet 0/0:

```
R1# show running-config

<some output omitted>
interface FastEthernet0/0
  no ip address
  shutdown
<some output omitted>
```

However, using **show running-config** is not necessarily the best way to verify interface configurations. Use the **show ip interface brief** command to quickly verify that interfaces are up and up (administratively up and line protocol is up).

## Configuring an Ethernet Interface

One common type of interface on many routers is an Ethernet interface. Ethernet interfaces are commonly used to connect to the corporate LAN.

### Configuring an Ethernet Interface

As shown earlier in Example 2-1, R1 does not yet have any routes. Add a route by configuring an interface with an IP address/subnet mask, and explore exactly what happens when that interface is activated. By default, all router interfaces are shut down, or turned off. To enable this interface, use the **no shutdown** command, which changes the interface from administratively down to up:

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 172.16.3.1 255.255.255.0
R1(config-if)# no shutdown
```

The following message is returned from the IOS:

```
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface
   FastEthernet0/0, changed state to up
```

Both of these messages are important. The first **changed state to up** message indicates that, physically, the connection is good. If you do not get this first message, be sure that the interface is properly connected to a switch or a hub.

**Note**

Although enabled with the **no shutdown** command, an Ethernet interface will not be active, or up, unless it is receiving a carrier signal from another device (switch, hub, PC, or another router).

The second **changed state to up** message indicates that the data link layer is operational. On LAN interfaces, you do not normally change the data link layer parameters. However, WAN interfaces in a lab environment require clocking on one side of the link, as discussed in Lab 1.5.1, “Cabling a Network and Basic Router Configuration,” as well as the section “Configuring a Serial Interface,” later in this chapter. If you do not correctly set the clock rate, the line protocol (the data link layer) will not change to up.

## Unsolicited Messages from IOS

Example 2-5 shows the output from an unsolicited message from the IOS.

**Example 2-5** Command Input Interrupted by IOS

```
R1(config)# int fa0/0
R1(config-if)# ip address 172.16.3.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# descri

*Mar  1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to
  up
*Mar  1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/0, changed state to upption
R1(config-if)#
```

The IOS often sends unsolicited messages similar to the **changed state to up** messages just discussed. As you can see in the previous example, sometimes these messages will occur when you are in the middle of typing a command. In the Example 2-5, this occurred while the user was entering the **description** command. The IOS message does not affect the command, but it can cause you to lose your place when typing.

To keep the unsolicited output separate from your input, enter line configuration mode for the console port and add the **logging synchronous** command, as shown in Example 2-6. Notice that the messages returned by IOS no longer interfered with the user’s entry of the **description** command. Instead, the IOS copied the command, midstream, to the next router prompt. The user then is able to easily finish the command as well as read the unsolicited message.

**Example 2-6** Synchronizing IOS Messages and Command Output

```
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-if)# descri

*Mar  1 01:28:04.242: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to
  up
*Mar  1 01:28:05.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/0, changed state to up
R1(config-if)# description
```

## Reading the Routing Table

Now look at routing table shown in Example 2-7. Notice R1 now has a “directly connected” FastEthernet 0/0 interface along with a new network.

**Example 2-7** Directly Connected Route

```
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C        172.16.3.0 is directly connected, FastEthernet0/0
```

The interface was configured with the 172.16.3.1/24 IP address, which makes it a member of the 172.16.3.0/24 network.

Examine the following line of output from the table:

```
C        172.16.3.0 is directly connected, FastEthernet0/0
```

The **C** at the beginning of the route indicates that this is a directly connected network. In other words, R1 has an interface that belongs to this network. The meaning of **C** is defined in the list of codes at the top of the routing table.

The /24 subnet mask for this route is displayed in the line above the actual route:

```
      172.16.0.0/24 is subnetted, 1 subnets
C        172.16.3.0 is directly connected, FastEthernet0/0
```

## Routers Usually Store Network Addresses

With very few exceptions, routing tables have routes for network addresses rather than individual host addresses. The 172.16.3.0/24 route in the routing table means that this route matches all packets with a destination address belonging to this network. Having a single route represent an entire network of host IP addresses makes the routing table smaller, with fewer routes, which results in faster routing table lookups. The routing table could contain all 254 individual host IP addresses for the 172.16.3.0/24 network, but that is an inefficient way of storing addresses.

A phone book is a good analogy for a routing table structure. A phone book is a list of names and phone numbers, sorted in alphabetical order by last name. When looking for a number, you can assume that the fewer names there are in the book, the faster it will be to find a particular name. A phone book of 20 pages and perhaps 2000 entries will be much easier to search than a book of 200 pages and 20,000 entries.

The phone book only contains one listing for each phone number. For example, the Stanford family might be listed as

> Stanford, Harold, 742 Evergreen Terrace, 555-1234

This is the single entry for everyone who lives at this address and has the same phone number. The phone book could contain a listing for every individual, but this would increase the size of the phone book. For example, there could be a separate listing for Harold Stanford, Margaret Stanford, Brad Stanford, Leslie Stanford, and Maggie Stanford—all with the same address and phone number. If this were done for every family, the phone book would be larger and take longer to search.

Routing tables work the same way: One entry in the table represents a "family" of devices that all share the same network or address space (the difference between a network and an address space will become clearer as you move through the course). The fewer the entries in the routing table, the faster the lookup process. To keep routing tables smaller, network addresses with subnet masks are listed instead of individual host IP addresses.

**Note**

Occasionally, a "host route" is entered in the routing table; the host route represents an individual host IP address. The host route is listed with the device's host IP address and a /32 (255.255.255.255) subnet mask. The topic of host routes is discussed in another course.

## Verifying Ethernet Addresses

After an interface is configured, it can be verified using various commands.

### Commands to Verify Interface Configuration

The **show interfaces fastethernet 0/0** command in Example 2-8 now shows that the interface is up and the line protocol is up. The **no shutdown** command changed the interface from administratively down to up. Notice that the IP address is now displayed.

**Example 2-8** Verifying Interface Status with the **show interfaces** Command

```
R1# show interfaces fastethernet 0/0

FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.3.1/24
  <output omitted>
```

The **show ip interface brief** command output in Example 2-9 also verifies this same information. Under the status and protocol, you should see "up."

**Example 2-9** Verifying Interface Status with the **show ip interface brief** Command

```
R1# show ip interface brief

Interface        IP-Address    OK?  Method   Status                 Protocol
FastEthernet0/0  172.16.3.1    YES  manual   up                     up
Serial0/0/0      unassigned    YES  unset    administratively down  down
FastEthernet0/1  unassigned    YES  unset    administratively down  down
Serial0/0/1      unassigned    YES  unset    administratively down  down
```

The following partial **show running-config** command output also shows the current configuration of this interface. When the interface is disabled, the **show running-config** command displays **shutdown**; however, when the interface is enabled, **no shutdown** is not displayed.

```
R1# show running-config

<output omitted>
interface FastEthernet0/0
ip address 172.16.3.1 255.255.255.0
<output omitted>
```

As explained in Chapter 1, a router cannot have multiple interfaces that belong to the same IP subnet. Each interface must belong to a separate subnet. For example, a router cannot have both its FastEthernet 0/0 interface configured as 172.16.3.1/24 address and mask and its FastEthernet 0/1 interface configured as 172.16.3.2/24.

IOS will return the following error message if you attempt to configure the second interface with the same IP subnet as the first interface:

```
R1(config-if)# int fa0/1
R1(config-if)# ip address 172.16.3.2 255.255.255.0

172.16.3.0 overlaps with FastEthernet0/0
R1(config-if)#
```

Typically, the router's Ethernet or Fast Ethernet interface will be the default gateway IP address for any devices on that LAN. For example, PC1 would be configured with a host IP address belonging to the 172.16.3.0/24 network, with the default gateway IP address 172.16.3.1. 172.16.3.1 is Router R1's Fast Ethernet IP address. Remember, a router's Ethernet or Fast Ethernet interface will also participate in the Address Resolution Protocol (ARP) process as a member of that Ethernet network.

## Ethernet Interfaces Participate in ARP

A router's Ethernet interface participates in a LAN network just like any other device on that network. This means that these interfaces have a Layer 2 MAC address. As shown in Example 2-8, the **show interfaces** command displays the MAC address for the Ethernet interfaces.

As demonstrated in Chapter 1, an Ethernet interface participates in ARP requests and replies and maintains an ARP table. If a router has a packet destined for a device on a directly connected Ethernet network, it checks the ARP table for an entry with that destination IP address to map it to the MAC address. If the ARP table does not contain this IP address, the Ethernet interface sends out an ARP request. The device with the destination IP address sends back an ARP reply that lists its MAC address. The IP address and MAC address information is then added to the ARP table for that Ethernet interface. The router is now able to encapsulate the IP packet into an Ethernet frame with the destination MAC address from its ARP table. The Ethernet frame, with the encapsulated packet, is then sent through that Ethernet interface.

Packet Tracer
☐ **Activity**

### Configure Ethernet Interfaces for IP on Hosts and Routers (2.2.3)

Use the Packet Tracer Activity to practice configuring Ethernet interfaces. Follow the additional instructions provided in the activity to examine the ARP process in simulation mode. Use file e2-223.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

## Configuring a Serial Interface

Next, configure the Serial 0/0/0 interface on Router R1. This interface is on the 172.16.2.0/24 network and is assigned the IP address and subnet mask of 172.16.2.1/24. The process to use for the configuration of the serial interface 0/0/0 is similar to the process you used to configure the FastEthernet 0/0 interface:

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 172.16.2.1 255.255.255.0
R1(config-if)# no shutdown
```

Example 2-10 shows the output from the **show interfaces serial 0/0/0** command.

**Example 2-10** Serial Interface with down and down

```
R1# show interfaces serial 0/0/0

Serial0/0/0 is down, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
<output omitted>
```

After entering the commands in Example 2-10, the state of the serial interface might vary depending on the type of WAN connection. For purposes here, we will be using dedicated, serial point-to-point connections between two routers. The serial interface will be in the up state only after the other end of the serial link has also been properly configured. You can display the current state of Serial 0/0/0 using the **show interfaces serial 0/0/0** command:

```
R2# show interfaces serial 0/0/0

Serial0/0/0 is administratively down, line protocol is down
```

As you can see, the link is still down. The link is down because you have not yet configured and enabled the other end of the serial link on R2.

You will now configure the other end of this link, Serial 0/0/0, for Router R2.

**Note**

There is no requirement that both ends of the serial link use the same interface, in this case, Serial 0/0/0. However, because both interfaces are members of the same network, they both must have IP addresses that belong to the 172.16.2.0/24 network. (The terms *network* and *subnet* can be used interchangeably in this case.)

R2's interface Serial 0/0/0 is configured with the IP address and subnet mask 172.16.2.2/24:

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 172.16.2.2 255.255.255.0
R2(config-if)# no shutdown
```

If you now issue the **show interfaces serial 0/0/0** command on either router, you still see that the link is up/down:

```
R2# show interfaces serial 0/0/0

Serial0/0/0 is up, line protocol is down
<output omitted>
```

The physical link between R1 and R2 is up because both ends of the serial link have been configured correctly with an IP address/mask and enabled with the **no shutdown** command. However, the line protocol is still down. This is because the interface is not receiving a clock signal. There is still one more command that you need to enter, the **clock rate** command, on the router with the DCE cable. The **clock rate** command will set the clock signal for the link. Configuring the clock signal will be discussed in the next sections.

## Examining Serial Interfaces

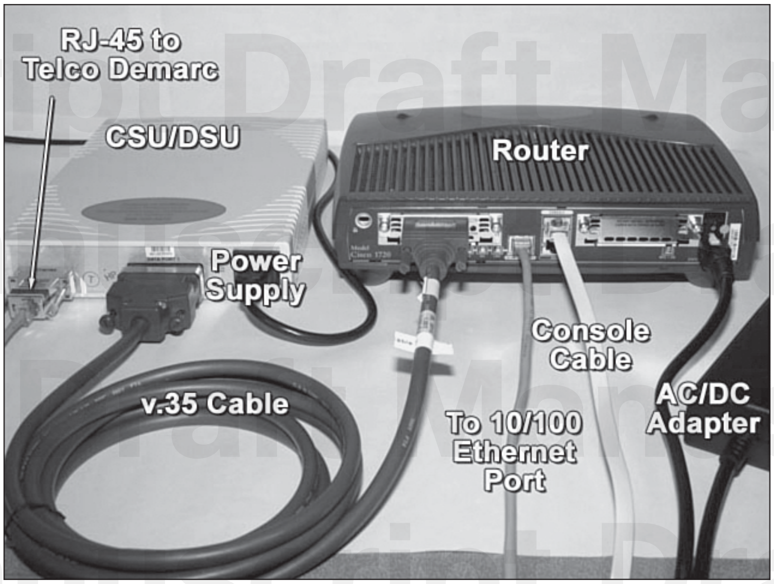
Serial interfaces can take various forms and use additional equipment such as a channel service unit/data service unit (CSU/DSU). This might also require additional commands on the router.

### Physically Connecting a WAN Interface

The WAN physical layer describes the interface between the DTE and the DCE. Generally, the DCE is the service provider and the DTE is the attached device. In this model, the services offered to the DTE are made available either through a modem or a CSU/DSU.

Figure 2-5 shows a router connected to a CSU/DSU. Typically, the router is the DTE device and is connected to a CSU/DSU, which is the DCE device. The CSU/DSU (DCE device) is used to convert the data from the router (DTE device) into a form acceptable to the WAN service provider. The CSU/DSU (DCE device) is also responsible for converting the data from the WAN service provider into a form acceptable by the router (DTE device). The router is usually connected to the CSU/DSU using a serial DTE cable.

**Figure 2-5** CSU/DSU Connection Using a DTE Cable



Source: http://www.more.net/technical/netserv/routers/cisco1720/images/dsu-router-connection-w.jpg

Serial interfaces require a clock signal to control the timing of the communications. In most environments, the service provider (a DCE device such as a CSU/DSU) will provide the clock. By default, Cisco routers are DTE devices. However, in a lab environment, we are not using any CSU/DSUs and, of course, we do not have a WAN service provider.

## Configuring Serial Links in a Lab Environment

For serial links that are directly interconnected, as in a lab environment, one side of a connection must be considered a DCE and provide a clocking signal. Although Cisco serial interfaces are DTE devices by default, they can be configured as DCE devices.

**How To**

To configure a router to be the DCE device, follow these steps:

**Step 1.** Connect the DCE end of the cable to the serial interface.

**Step 2.** Configure the clock signal on the serial interface using the **clock rate** command.

The serial cables used in the lab are typically one of two types:

- A DTE/DCE crossover cable on which one end is DTE and the other end is DCE
- A DTE cable connected to a DCE cable

In our chapter topology, the Serial 0/0/0 interface on R1 is connected with the DCE end of the cable, and the Serial 0/0/0 interface on R2 is connected to the DTE end of the cable. The cable should be labeled either DTE or DCE.

You can also distinguish DTE from DCE by looking at the connector between the two cables. The DTE cable has a male connector, whereas the DCE cable has a female connector.

If a cable is connected between the two routers and neither end of the cable is labeled, you can use the **show controllers** command to determine which end of the cable is attached to that interface. In the following command output, notice that R1 has the DCE cable attached to its Serial 0/0/0 interface and that no clock rate is set.

```
R1# show controllers serial 0/0/0

Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
<output omitted>
```

When the cable is attached, the clock can now be set with the **clock rate** command. The available clock rates, in bits per second, are 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, and 4000000. Some bit rates might not be available on certain serial interfaces. Because the Serial 0/0/0 interface on R1 has the DCE cable attached, we will configure that interface with a clock rate:

```
R1(config)# interface serial 0/0/0
R1(config-if)# clock rate 64000

01:10:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
   to up
```

**Note**

If a router's interface with a DTE cable is configured with the **clock rate** command, the IOS will disregard the command and there will be no ill effects.

## Verifying the Serial Interface Configuration

As you can see from Example 2-11, you can determine that the line protocol is now up and verify this on both ends of the serial link by using the **show interfaces** and **show ip interface brief** commands. Remember, the serial interface will be up only if both ends of the link are configured correctly. In our lab environment, we have configured the clock rate on the end with the DCE cable.

**Example 2-11** Verifying the Serial Interface Configuration

```
R1# show interfaces serial 0/0/0

Serial0/0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.16.2.1/24
<output omitted>

R1# show ip interface brief

Interface              IP-Address      OK? Method Status           Protocol
FastEthernet0/0        172.16.3.1      YES manual up                     up
Serial0/0/0            172.16.2.1      YES manual up                     up
<output omitted>
```

You can further verify that the link is up/up by pinging the remote interface, as shown in Example 2-12.

**Example 2-12** Using the **ping** Command to Verify Connectivity

```
R1# ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1#
```

Finally, you can see in Example 2-13 that the 172.16.2.0/24 serial network is now in the routing table for R1. If you issued the **show ip route** command on R2, you would also see the directly connected route for the 172.16.2.0/24 network.

**Example 2-13** Using the **show ip route** Command to Verify Connectivity

```
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```

Now verify the interface's configurations by using the **show running-config** command on R1, as shown in Example 2-14.

**Example 2-14** Verifying the Configuration with the **show running-config** Command

```
R1# show running-config

Building configuration...

Current configuration : 1130 bytes
!
hostname R1
!
<output omitted>
!
interface FastEthernet0/0
 description R1 LAN
 ip address 172.16.3.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 172.16.2.1 255.255.255.0
 clockrate 64000
!
<output omitted>
R1#
```

**Note**

Although the **clock rate** command is two words, IOS spells clockrate as a single word in the running configuration and startup configuration files.

# Exploring Directly Connected Networks

Before a router can forward packets to a remote network, it must have active directly connected networks. Each directly connected network on the router is a member of a different network or subnet.

## Verifying Changes to the Routing Table

The routing table is a key component in routing operations. Several commands can be used to help verify and troubleshoot the routing table.

### Routing Table Concepts

As you can see in Examples 2-15 and 2-16, the **show ip route** command reveals the content of the routing tables for R1 and R2.

**Example 2-15** Current Routing Table for R1

```
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

**Example 2-16** Current Routing Table for R2

```
R2# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
R2#
```

A routing table is a data structure used to store routing information acquired from different sources. The main purpose of a routing table is to provide the router with paths to different destination networks.

The routing table consists of a list of "known" network addresses—that is, those addresses that are directly connected, configured statically, and learned dynamically. R1 and R2 only have routes for directly connected networks.

## Observing Routes as They Are Added to the Routing Table

This section takes a closer look at how directly connected routes are added to, and deleted from, the routing table. In contrast to **show** commands, **debug** commands can be used to monitor router operations in real time. The **debug ip routing** command will display any changes that the router performs when adding or removing routes. You will configure the interfaces on the R2 router and examine this process. The following discussion will refer to Example 2-17.

**Example 2-17** Using the **debug ip routing** Command to Observe a Route Installed

```
R2# debug ip routing

IP routing debugging is on

R2(config)#int fa0/0
R2(config-if)#ip address 172.16.1.1 255.255.255.0
R2(config-if)#no shutdown

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
  up

RT: add 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: interface FastEthernet0/0 added to routing table
```

First, you enable debugging with the **debug ip routing** command so that you can see the directly connected networks as they are added to the routing table.

Next, you configure the IP address and subnet mask for the FastEthernet 0/0 interface on R2 and use the **no shutdown** command. Because the Fast Ethernet interface connects to the 172.16.1.0/24 network, it must be configured with a host IP address for that network.

In Example 2-17, notice that the following message is returned from the IOS:

```
02:35:30: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
02:35:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
   state to up
```

After the **no shutdown** command is entered and the router determines that the interface and line protocol are in the up and up state, the **debug** output shows R2 adding this directly connected network to the routing table.

```
02:35:30: RT: add 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
02:35:30: RT: interface FastEthernet0/0 added to routing table
```

The routing table for R2 now shows the route for the directly connected network 172.16.1.0/24, as shown in Example 2-18.

**Example 2-18** Routing Table for R2 with New Route Installed

```
R2# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0
```

The **debug ip routing** command displays routing table processes for any route, whether that route is a directly connected network, a static route, or a dynamic route.

You can disable **debug ip routing** by using either the **undebug ip routing** command or the **undebug all** command, as shown in Example 2-19.

**Example 2-19** Disabling Debug

```
R2# undebug all

All possible debugging has been turned off
!
or
!
R2# undebug ip routing

IP routing debugging is off
R2#
```

## Changing an IP Address

To change an IP address or subnet mask for an interface, reconfigure the IP address and subnet mask for that interface. This change will overwrite the previous entry. There are ways to configure a single interface with multiple IP addresses, as long as each address is on a different subnet. This topic will be discussed in a later course.

To remove a directly connected network from a router, use these two commands: **shutdown** and **no ip address**, as demonstrated in Example 2-20. The **shutdown** command is used to disable interfaces. This command can be used by itself if you want to retain the IP address/mask configuration on the interface but want to shut it down temporarily. In our example, this command will disable R2's Fast Ethernet interface. The IP address, however, will still be in the configuration file, running-config.

After the **shutdown** command is used, you can remove the IP address and subnet mask from the interface. The order in which you perform these two commands does not matter.

Again, using **debug ip routing**, you can see the routing table process. We will delete the configuration for R2's FastEthernet 0/0 interface. In Example 2-20, you can see the routing table process removing the directly connected route.

**Example 2-20** Removing Interface Configurations

```
R2# debug ip routing

IP routing debugging is on
R2# config t

Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# int fa0/0
R2(config-if)# shutdown
```

*continues*

*continued*

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
 down

is_up: 0 state: 6 sub state: 1 line: 1
RT: interface FastEthernet0/0 removed from routing table
RT: del 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 172.16.1.0/24

<some ouput omitted>

R2(config-if)# no ip address
R2(config-if)# end

%SYS-5-CONFIG_I: Configured from console by console
R2# undebug all

All possible debugging has been turned off
```

First, you shut down the interface. The IOS output also indicates that the interface and line protocol are now down. Then, the output from debugging shows the route being deleted from the routing table. Finally, to completely remove the configuration, enter **no ip address** and turn off debugging.

To verify that the route was removed from the routing table, use the **show ip route** command. In Example 2-21, notice that the route to 172.16.1.0/24 has been removed.

**Example 2-21** Routing Table for R2 with Route Deleted

```
R2# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
```

For the purposes of the rest of this chapter, we will assume that the addressing for FastEthernet 0/0 was not removed. To reconfigure t]he interface, simply enter the commands again:

```
R2(config)# interface fastethernet 0/0
R2(config-if)# ip address 172.16.1.1 255.255.255.0
R2(config-if)# no shutdown
```

**Caution**

The **debug** commands, especially the **debug all** command, should be used sparingly. These commands can disrupt router operations. The **debug** commands are useful when configuring or troubleshooting a network; however, they can make intensive use of CPU and memory resources. It is recommended that you run as few debug processes as necessary and disable them immediately when they are no longer needed. The **debug** commands should be used with caution on production networks because they can affect the performance of the device.

Packet Tracer
☐ **Activity**

**Configure Serial Interfaces and Verify the Routing Table (2.3.1)**

Use the Packet Tracer Activity to practice configuring serial interfaces. You will also use the **debug ip routing** command to observe the routing table processes. Use file e2-231.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

# Devices on Directly Connected Networks

Before configuring static routes or a dynamic routing protocol, it is recommended that you first verify connectivity with devices on the directly connected networks. Hosts on different networks will not be able to communicate with each other if they cannot communicate with their own default gateway, the local router.

## Accessing Devices on Directly Connected Networks

To return to our configuration in the sample topology, assume that all directly connected networks are configured for all three routers. Example 2-22 shows the rest of the configurations for Routers R2 and R3.

**Example 2-22** Remaining Interface Configurations for R2 and R3

```
R2(config)# interface serial 0/0/1
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# clock rate 64000
R2(config-if)# no shutdown
```

```
R3(config)# interface fastethernet 0/0
R3(config-if)# ip address 192.168.2.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# interface serial 0/0/1
R3(config-if)# ip address 192.168.1.1 255.255.255.0
R3(config-if)# no shutdown
```

The output from the **show ip interface brief** command shown in Example 2-23 verifies that all configured interfaces are up and up.

**Example 2-23** Verifying That All Interfaces Are up and up

```
R1# show ip interface brief

Interface          IP-Address       OK? Method Status                Protocol
FastEthernet0/0    172.16.3.1       YES manual up                    up
Serial0/0/0        172.16.2.1       YES manual up                    up
FastEthernet0/1    unassigned       YES manual administratively down  down
Serial0/0/1        unassigned       YES manual administratively down  down
```

```
R2# show ip interface brief

Interface          IP-Address       OK? Method Status                Protocol
FastEthernet0/0    172.16.1.1       YES manual up                    up
Serial0/0/0        172.16.2.2       YES manual up                    up
FastEthernet0/1    unassigned       YES manual administratively down  down
Serial0/0/1        192.168.1.2      YES manual up                    up
```

```
R3# show ip interface brief

Interface          IP-Address       OK? Method Status                Protocol
FastEthernet0/0    192.168.2.1      YES manual up                    up
Serial0/0/0        unassigned       YES manual administratively down  down
FastEthernet0/1    unassigned       YES manual administratively down  down
Serial0/0/1        192.168.1.1      YES manual up                    up
```

By reviewing the routing tables in Example 2-24, you can verify that all directly connected networks are installed for routing.

**Example 2-24** Verifying That Directly Connected Routes Are Installed

```
R1# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 2 subnets
C        172.16.2.0 is directly connected, Serial0/0/0
C        172.16.3.0 is directly connected, FastEthernet0/0
```

```
R2# show ip route

172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
C        172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

```
R3# show ip route

C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

The crucial step in configuring your network is to verify that all the interfaces are up and up and that the routing tables are complete. Regardless of what routing scheme you ultimately configure—static, dynamic, or a combination of both—verify your initial network configurations with the **show ip interface brief** command and the **show ip route** command before proceeding with more complex configurations.

When a router only has its interfaces configured, and the routing table contains the directly connected networks but no other routes, only devices on those directly connected networks are reachable:

- R1 can communicate with any device on the 172.16.3.0/24 and 172.16.2.0/24 networks.
- R2 can communicate with any device on the 172.16.1.0/24, 172.16.2.0/24, and 192.168.1.0/24 networks.
- R3 can communicate with any device on the 192.168.1.0/24 and 192.168.2.0/24 networks.

Because these routers know only about their directly connected networks, the routers can communicate only with those devices on their own directly connected LANs and serial networks.

For example, PC1 in the chapter topology (see Figure 2-1) has been configured with the IP address 172.16.3.10 and the subnet mask 255.255.255.0. PC1 has also been configured with the default gateway IP address 172.16.3.1, which is the router's FastEthernet 0/0 interface IP address. Because R1 only knows about directly connected networks, it can forward packets from PC1 to devices on the 172.16.2.0/24 network, such as 172.16.2.1 and 172.16.2.2. Packets from PC1 with any other destination IP address, such as PC2 at 172.16.1.10, would be dropped by R1.

Take a look at the routing table for R2 in Example 2-24. R2 only knows about its three directly connected networks. Try to predict what will happen if you ping the Fast Ethernet interfaces on the other routers.

In Example 2-25, notice that the pings failed, as indicated by the series of five periods.

**Example 2-25** Remote Networks Are Unreachable

```
R2# ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

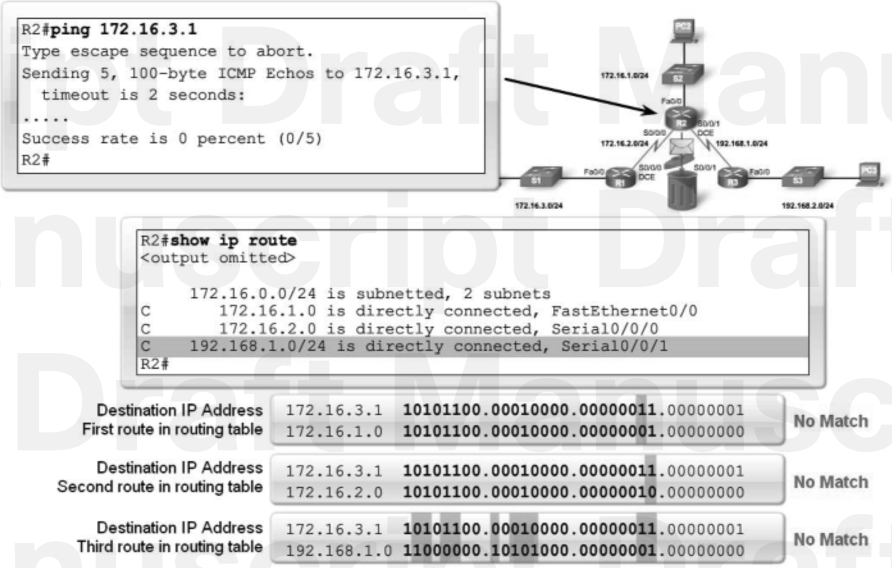
The pings failed because R2 does not have a route in its routing table that matches either 172.16.3.1 or 192.168.2.1, which is the ping packet's destination IP address. To have a match between the packet's destination IP address of 172.16.3.1 and a route in the routing table, the address must match the number of leftmost bits of the network address as indicated by the prefix of the route. For R2, all the routes have a /24 prefix; therefore, the leftmost 24 bits are checked for each route.

The sections that follow further investigate what is happening.

## Pings from R2 to 172.16.3.1

Figure 2-6 shows the unsuccessful ping output along with the unmatched routes in the routing table.

**Figure 2-6** No Route: Pings Are Discarded



```
R2#ping 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1,
  timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#
```

```
R2#show ip route
<output omitted>

      172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, FastEthernet0/0
C        172.16.2.0 is directly connected, Serial0/0/0
C     192.168.1.0/24 is directly connected, Serial0/0/1
R2#
```

```
Destination IP Address      172.16.3.1   10101100.00010000.00000011.00000001
First route in routing table 172.16.1.0  10101100.00010000.00000001.00000000   No Match

Destination IP Address      172.16.3.1   10101100.00010000.00000011.00000001
Second route in routing table 172.16.2.0 10101100.00010000.00000010.00000000   No Match

Destination IP Address      172.16.3.1   10101100.00010000.00000011.00000001
Third route in routing table 192.168.1.0 11000000.10101000.00000001.00000000   No Match
```

The first route in the table for R1 is 172.16.1.0/24:

```
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
```

The IOS routing table process checks to see whether the 24 leftmost bits of the packet's destination IP address, 172.16.3.1, match the 172.16.1.0/24 network.

If you convert these addresses to binary and compare them, as shown in Figure 2-6, you will see that the first 24 bits of this route do not match because the 23rd bit does not match. Therefore, this route is rejected:

```
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
```

In Figure 2-6, you see that the first 24 bits of the second route do not match because the 24th bit does not match. Therefore, this route is also rejected, and the process moves on to the next route in the routing table:

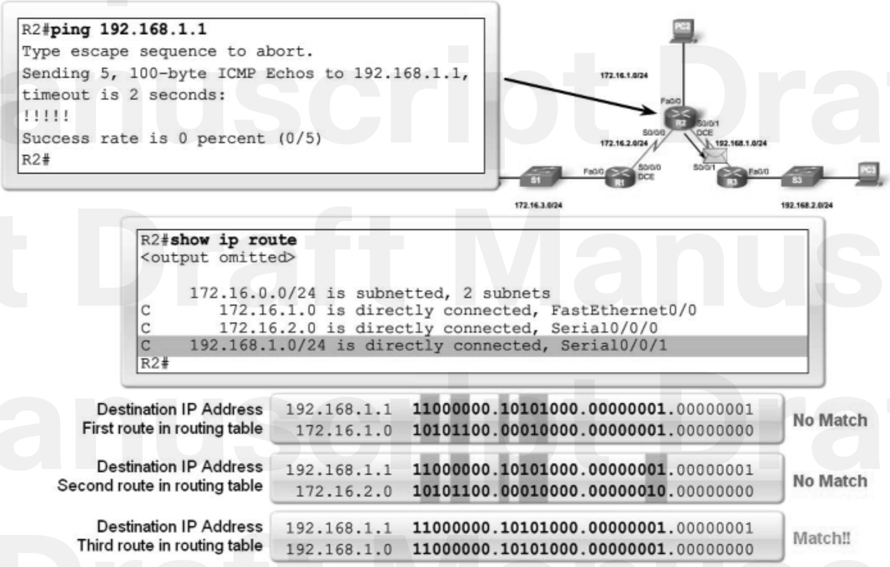
```
C 192.168.1.0/24 is directly connected, Serial0/0/1
```

The third route is also not a match. As shown, 10 of the first 24 bits do not match. Therefore, this route is rejected. Because there are no more routes in the routing table, the pings are discarded. The router makes its forwarding decision at Layer 3, a "best effort" to forward the packet, but it makes no guarantees.

### Pings from R2 to 192.168.1.1

Look at Figure 2-7 to see what happens if Router R2 pings the 192.168.1.1 interface on Router R3.

**Figure 2-7** Route Exists: Pings Are Sent



```
R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1,
timeout is 2 seconds:
!!!!!
Success rate is 0 percent (0/5)
R2#
```

```
R2#show ip route
<output omitted>

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
R2#
```

| | | | |
|---|---|---|---|
| Destination IP Address | 192.168.1.1 | 11000000.10101000.00000001.00000001 | No Match |
| First route in routing table | 172.16.1.0 | 10101100.00010000.00000001.00000000 | |
| Destination IP Address | 192.168.1.1 | 11000000.10101000.00000001.00000001 | No Match |
| Second route in routing table | 172.16.2.0 | 10101100.00010000.00000010.00000000 | |
| Destination IP Address | 192.168.1.1 | 11000000.10101000.00000001.00000001 | Match!! |
| Third route in routing table | 192.168.1.0 | 11000000.10101000.00000001.00000000 | |

This time the ping succeeds! It is successful because R2 has a route in its routing table that matches 192.168.1.1, which is the ping packet's destination IP address. The first two routes, 172.16.1.0/24 and 172.16.2.0/24, are rejected. But the last route, 192.168.1.0/24, matches the first 24 bits of the destination IP address. The ping packet is encapsulated in the Layer 2 High-Level Data Link Control (HDLC) protocol of Serial 0/0/1, the exit interface, and forwarded through the Serial 0/0/1 interface. R2 is now done making the forwarding decisions for this packet; the decisions made by other routers about this packet are not its concern.

**Note**

The routing table lookup process will be discussed in further detail in Chapter 8, "The Routing Table: A Closer Look."

**Packet Tracer Activity**

#### Verify Connectivity of Directly Connected Devices (2.3.2)

Use the Packet Tracer Activity to test connectivity between directly connected devices. Use file e2-232.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

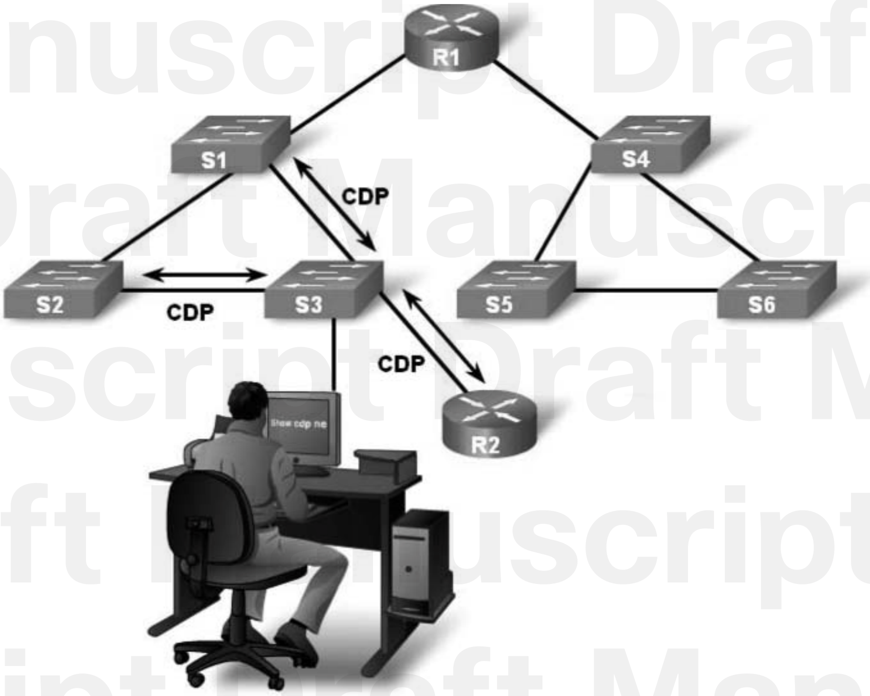
## Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a powerful network-monitoring and -troubleshooting tool. CDP is an information-gathering tool used by network administrators to get information about directly connected Cisco devices. CDP is a proprietary tool that enables you to access a summary of protocol and address information about Cisco devices that are directly connected.

### Network Discovery with CDP

By default, each Cisco device sends periodic messages to directly connected Cisco devices, as shown in Figure 2-8. These messages are known as CDP advertisements. These advertisements contain information such as the types of devices that are connected, the router interfaces they are connected to, the interfaces used to make the connections, and the model numbers of the devices.

**Figure 2-8** CDP Advertisements



Most network devices, by definition, do not work in isolation. A Cisco device frequently has other Cisco devices as ***neighbors*** on the network. Information gathered from other devices can assist you in making network design decisions, in troubleshooting, and in making changes to equipment. CDP can be used as a network discovery tool, helping you to build a logical topology of a network when such documentation is missing or lacking in detail.

Familiarity with the general concept of neighbors is important for understanding CDP as well as for future discussions about dynamic routing protocols.

### Layer 3 Neighbors

At this point in the chapter topology configuration, you only have directly connected neighbors. At Layer 3, routing protocols consider neighbors to be devices that share the same network address space.

For example, in the chapter topology (Figure 2-1) R1 and R2 are neighbors. Both are members of the 172.16.1.0/24 network. R2 and R3 are also neighbors because they both share the 192.168.1.0/24 network. But R1 and R3 are not neighbors because they do not share any network address space. If you connected R1 and R3 with a cable and configured each with an IP address from the same network, they would be neighbors.

### Layer 2 Neighbors

CDP operates at Layer 2 only. Therefore, CDP neighbors are Cisco devices that are directly connected physically and share the same data link. In Figure 2-8, the network administrator is logged in to S3. S3 will receive CDP advertisements from S1, S2, and R2 only.

Assuming that all routers and switches are Cisco devices running CDP, what neighbors would R1 have? Can you determine the CDP neighbors for each device?

In the chapter topology (Figure 2-1), you can see the following CDP neighbor relationships:

- R1 and S1 are CDP neighbors
- R1 and R2 are CDP neighbors
- R2 and S2 are CDP neighbors
- R2 and R3 are CDP neighbors
- R3 and S3 are CDP neighbors

Notice the difference between Layer 2 and Layer 3 neighbors. The switches are not neighbors to the routers at Layer 3, because the switches are operating at Layer 2 only. However, the switches are Layer 2 neighbors to their directly connected routers.

The section that follows shows how CDP can be helpful to a network administrator.

### CDP Operation

Examine the output from the **show cdp neighbors** and **show cdp neighbors detail commands** in Example 2-26. Notice that R3 has gathered some detailed information about R2 and the switch connected to the Fast Ethernet interface on R3.

**Example 2-26** Examining CDP Neighbors

```
R3# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID         Local Intrfce      Holdtme   Capability  Platform  Port ID
S3                Fas 0/0             151         S I        WS-C2950  Fas 0/6
R2                Ser 0/0/1           125          R         1841      Ser 0/0/1

R3# show cdp neighbors detail

-------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
  RELEASE SO
FTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''

-------------------------
Device ID: S3
Entry address(es):
Platform: cisco WS-C2950-24,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/11
Holdtime : 148 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1, RELEASE SOFTWARE
  (fc1)
```

*continues*

*continued*

```
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 24-Apr-02 06:57 by antonino

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
  value=00000000FFFFFFFF0
10231FF000000000000000AB769F6C0FF0000
VTP Management Domain: 'CCNA3'
Duplex: full

R3#
```

CDP runs at the data link layer connecting the physical media to the upper-layer protocols. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers that support different network layer protocols (for example, IP and Novell IPX) can learn about each other.

When a Cisco device boots up, CDP starts up by default. CDP automatically discovers neighboring Cisco devices running CDP, regardless of which protocol or suites are running. CDP exchanges hardware and software device information with its directly connected CDP neighbors.

CDP provides the following information about each CDP neighbor device:

- **Device identifiers:** For example, the configured host name of a switch
- **Address list:** Up to one network layer address for each protocol supported
- **Port identifier:** The name of the local and remote port, in the form of an ASCII character string such as ethernet0
- **Capabilities list:** For example, whether this device is a router or a switch
- **Platform:** The hardware platform of the device; for example, a Cisco 7200 series router

Packet Tracer
☐ **Activity**

### Cisco Discovery Protocol (CDP) (2.3.3)

Use the Packet Tracer Activity to explore the features of the Cisco Discovery Protocol (CDP). Practice enabling and disabling CDP both globally and on a per-interface basis. Investigate the power of using CDP to discover the topology of a network. Use file e2-233.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

## Using CDP for Network Discovery

CDP can be used to discover a variety of information about directly connected networks. CDP can be a useful tool in helping analyze and document existing networks.

### CDP show Commands

The information gathered by the CDP protocol can be examined with the **show cdp neighbors** command, as shown previously in Example 2-26. For each CDP neighbor, the following information is displayed:

- Neighbor device ID
- Local interface
- Holdtime value, in seconds
- Neighbor device capability code
- Neighbor hardware platform
- Neighbor remote port ID

The **show cdp neighbors detail** command also reveals the IP address of a neighboring device. In Example 2-26, R3 learned through CDP that R2 is using IP address 192.168.1.2. CDP will reveal the neighbor's IP address regardless of whether you can ping the neighbor. This command is very helpful when two Cisco routers cannot route across their shared data link. The **show cdp neighbors detail** command will help determine whether one of the CDP neighbors has an IP configuration error.

For network discovery situations, knowing the IP address of the CDP neighbor is often all the information needed to telnet into that device. With an established Telnet session, information can be gathered about a neighbor's directly connected Cisco devices. In this fashion, you can telnet around a network and build a logical topology. In the next Packet Tracer Activity, "Mapping a Network with CDP and Telnet (2.3.4)," you will do just that.

### Disabling CDP

Could CDP be a security risk? Yes, it could be. You might already have seen CDP packets in your packet capturing labs from a previous course. Because some IOS versions send out CDP advertisements by default, it is important to know how to disable CDP.

To disable CDP globally, for the entire device, use this command:

```
Router(config)# no cdp run
```

If you want to use CDP but need to stop CDP advertisements on a particular interface, use this command:

```
Router(config-if)# no cdp enable
```

Packet Tracer
☐ **Activity**

**Mapping a Network with CDP and Telnet (2.3.4)**

CDP **show** commands can be used to discover information about unknown devices in a network. CDP **show** commands display information about directly connected Cisco devices, including an IP address that can be used to reach the device. You can then telnet to the device and repeat the process until the entire network is mapped.

Use the Packet Tracer Activity to discover and map an unknown network using CDP and Telnet. Use file e2-234.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

# Static Routes with "Next-Hop" Addresses

As discussed previously, a router can learn about remote networks in one of two ways:

- Manually, from configured static routes
- Automatically, from a dynamic routing protocol

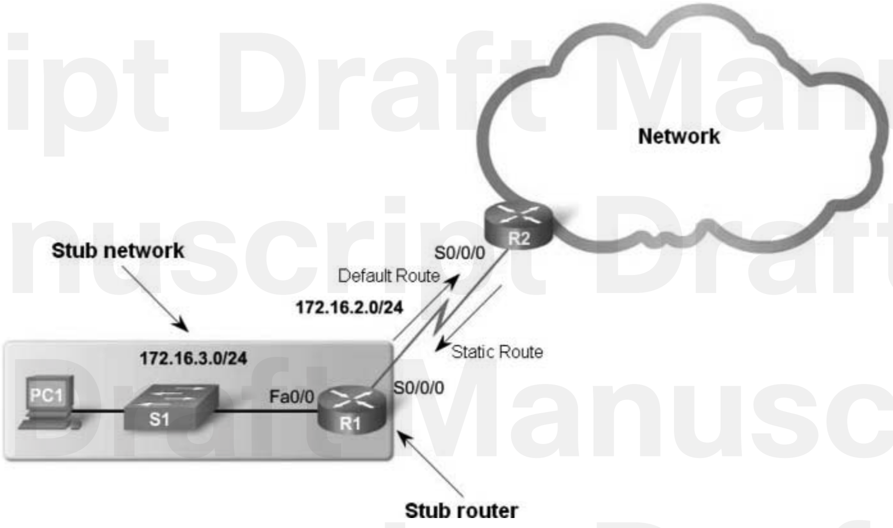
The rest of this chapter focuses on configuring static routes. Dynamic routing protocols are introduced in the next chapter.

## Purpose and Command Syntax of the ip route Command

Static routes are commonly used when routing from a network to a stub network. A ***stub network*** is a network accessed by a single route. For an example, see Figure 2-9. Here you see that any network attached to R1 would only have one way to reach other destinations, whether to networks attached to R2 or to destinations beyond R2. Therefore, network 172.16.3.0 is a stub network and R1 is a ***stub router***.

Running a routing protocol between R1 and R2 is a waste of resources because R1 has only one way out for sending nonlocal traffic. Therefore, static routes are configured for connectivity to remote networks that are not directly connected to a router. Again, referring to the figure, you would configure a static route on R2 to the LAN attached to R1. You will also see how to configure a default static route from R1 to R2 later in the chapter so that R1 can send traffic to any destination beyond R2.

**Figure 2-9** Stub Network Example



## ip route Command

The command for configuring a static route is **ip route**. The complete syntax for configuring a static route is

```
ip route prefix mask {ip-address ¦ interface-type interface-number [ip-address]}
   [dhcp] [distance] [name next-hop-name] [permanent ¦ track number] [tag tag]
```

Most of these parameters are not relevant for this chapter or for your CCNA studies. We will use a simpler version of the syntax:

```
Router(config)# ip route network-address subnet-mask {ip-address ¦ exit-interface}
```

The following parameters are used:

- *network-address*: Destination network address of the remote network to be added to the routing table. (Equivalent to the *prefix* parameter in the complete syntax.)
- *subnet-mask*: Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks. (Equivalent to the *mask* parameter in the complete syntax.)

One or both of the following parameters must also be used:

- *ip-address*: Commonly referred to as the next-hop router's IP address. (Equivalent to the *ip-address* parameter in the complete syntax.)
- *exit-interface*: Outgoing interface that would be used in forwarding packets to the destination network. (Equivalent to the **interface-type** *interface-number* parameter in the complete syntax.)

**Note**

The *ip-address* parameter is commonly referred to as the "next-hop" router's IP address. The actual next-hop router's IP address is commonly used for this parameter. However, the *ip-address* parameter could be any IP address, as long as it is resolvable in the routing table. This is beyond the scope of this course, but we've added this point to maintain technical accuracy.

## Configuring Static Routes

Remember that R1 in our chapter topology knows about its directly connected networks. Example 2-24 showed the routes currently in R1's routing table. The remote networks that R1 does not know about are as follows:

- 172.16.1.0/124: The LAN on R2
- 192.168.1.0/24: The serial network between R2 and R3
- 192.168.2.0/24: The LAN on R3

Use the **ip route** command syntax to configure static routes to these remote networks. Example 2-27 shows the command syntax.

**Example 2-27** R1 Static Route Configuration to R2's LAN

```
R1# debug ip routing

<some debug output omitted>
R1# conf t
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2

00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]

R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

To have IOS messages display when the new route is added to the routing table, you can use the **debug ip routing** command.

Then, use the **ip route** command to configure static routes on R1 for each of these networks. Example 2-27 shows the first route configured.

Examining each element in this output reveals the following:

- **ip route:** Static route command
- **172.16.1.0:** Network address of remote network
- **255.255.255.0:** Subnet mask of remote network
- **172.16.2.2:** Serial 0/0/0 interface IP address on R2, which is the next hop to this network

When the IP address is the actual next-hop router's IP address, this IP address is reachable from one of this router's directly connected networks. In other words, the next-hop IP address 172.16.2.2 belongs to router R1's directly connected Serial 0/0/0 network 172.16.2.0/24.

## Verifying the Static Route

The output from the **debug ip routing** command shows that this route has been added to the routing table:

```
00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
```

Entering **show ip route** on R1 displays the new routing table. The static route entry is highlighted.

Examine this output:

- **S:** Routing table code for static route.
- **172.16.1.0:** Network address for the route.
- **/24:** Subnet mask for this route; this is displayed in the line above, known as the parent route, and discussed in Chapter 8.
- **[1/0]:** Administrative distance and metric for the static route (explained in a later chapter).
- **via 172.16.2.2:** IP address of the next-hop router, the IP address of R2's Serial 0/0/0 interface.

Any packets with a destination IP address that have the 24 leftmost bits matching 172.16.1.0 will use this route.

## Configuring Routes to Two More Remote Networks

Example 2-28 shows the commands to configure the routes for the other two remote networks. Debugging has been disabled.

**Example 2-28** Configuring Routes for Remote Networks

```
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)# end
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

Notice that all three static routes configured on R1 have the same next-hop IP address: 172.16.2.2. Using the chapter topology as a reference (Figure 2-1), you can see that this is true because packets for all the remote networks must be forwarded to router R2, the next-hop router.

In Example 2-28, the **show ip route** command is used again to examine the new static routes in the routing table:

```
S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [1/0] via 172.16.2.2
```

The /24 subnet masks are located on the same line as the network address. For now, this difference is not important. It will be explained in detail in Chapter 8.

The static routes that have been configured can also be verified by examining the running configuration with the **show running-config** command, as shown in Example 2-29. Now is a good time to save the configuration to NVRAM with the **copy running-config startup-config command**.

**Example 2-29** Verifying Static Route Commands

```
R1# show running-config

Building configuration...

Current configuration : 849 bytes
!
hostname R1
!
<output omitted>
!
ip classless
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
!
<output omitted>
!
end

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

## Routing Table Principles and Static Routes

Refer to the chapter topology (see Figure 2-1). Now that three static routes are configured on R1, can you predict whether packets destined for these networks will reach their destination? If so, will return packets from all these networks be successfully routed back to R1?

Review the three routing table principles, as described by Alex Zinin in his book *Cisco IP* Routing[1]:

**Principle 1: Every router makes its decision alone, based on the information it has in its own routing table.**

R1 has three static routes in its routing table and makes forwarding decisions based solely on the information in the routing table. R1 does not consult the routing tables in any other routers, nor does it know whether those routers have routes to other networks. Making each router aware of remote networks is the responsibility of the network administrator.

**Principle 2: The fact that one router has certain information in its routing table does not mean that other routers have the same information.**

R1 does not know what information other routers have in their routing table. For example, R1 has a route to the 192.168.2.0/24 network through Router R2. Any packets that match this route belong to the 192.168.2.0/24 network and will be forwarded to Router R2. R1 does not know whether R2 has a route to the 192.168.2.0/24 network. Again, the network administrator would be responsible for ensuring that the next-hop router also has a route to this network.

Using Principle 2, you still need to configure the proper routing on the other routers (R2 and R3) to make sure that they have routes to these three networks.

**Principle 3: Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.**

Most of the communication over networks is bidirectional. This means that packets must travel in both directions between the end devices involved. A packet from PC1 can reach PC3 because all the routers involved have routes to the destination network 192.168.2.0/24. However, the success of any returning packets going from PC3 to PC1 depends on whether the routers involved have a route to the return path, PC1's 172.16.3.0/24 network.

Using Principle 3 as guidance, you will configure proper static routes on the other routers to make sure that they have routes back to the 172.16.3.0/24 network.

## Applying the Principles

With these principles in mind, how would you answer the questions posed regarding packets that originate from PC1?

**Would packets from PC1 reach their destination?**

In this case, packets destined for 172.16.1.0/24 and 192.168.1.0/24 networks would reach their destination. This is because Router R1 has a route to these networks through R2. When packets reach Router R2, these networks are directly connected on R2 and are routed using its routing table.

However, packets destined for the 192.168.2.0/24 network would not reach their destination. R1 has a static route to this network through R2. However, when R2 receives a packet, it will drop it because R2 does not yet contain a route for this network in its routing table.

**Does this mean that any return packets from remote networks destined for the 172.16.3.0/24 network will reach their destination?**

If R2 or R3 receives a packet destined for 172.16.3.0/24, the packet will not reach its destination, because neither router has a route to the 172.16.3.0/24 network.

We finish the static routing configuration for the chapter topology by configuring static routes on R2 and R3. With the commands shown in Example 2-30, all routers now have routes to all remote networks.

**Example 2-30** Configure R2 and R3 Static Routes

```
R2(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

```
R3(config)# ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.3.0 255.255.255.0 192.168.1.2
```

Examine the routing tables in Example 2-31 to verify that all routers now have routes to all remote networks.

**Example 2-31** Verify Static Routes Are in Routing Tables

```
R1# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

```
R2# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 [1/0] via 172.16.2.1
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
```

```
R3# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
S       172.16.2.0 [1/0] via 192.168.1.2
S       172.16.3.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Connectivity can be further verified by pinging remote router interfaces from Router R1, as shown in Example 2-32.

**Example 2-32** Verify End-to-End Connectivity

```
R1# ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
R1# ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1# ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R1# ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#
```

Full connectivity is now achieved for the devices in our topology. Any PC, on any LAN, can now access PCs on all other LANs.

## Resolving to an Exit Interface with a Recursive Route Lookup

Before any packet is forwarded by a router, the routing table process must determine the exit interface to use to forward the packet. This is known as *route resolvability*. Examine this process by looking at the routing table for R1 in Example 2-31. R1 has a static route for the remote network 192.168.2.0/24, which forwards all packets to the next-hop IP address 172.16.2.2:

```
S       192.168.2.0/24 [1/0] via 172.16.2.2
```

Finding a route is only the first step in the lookup process. R1 must determine how to reach the next-hop IP address 172.16.2.2. It will do a second search looking for a match for 172.16.2.2. In this case, the IP address 172.16.2.2 matches the route for the directly connected network 172.16.2.0/24:

```
C       172.16.2.0 is directly connected, Serial0/0/0
```

The 172.16.2.0 route is a directly connected network with the exit interface Serial 0/0/0. This lookup tells the routing table process that this packet will be forwarded out that interface. Therefore, it takes two routing table lookup processes to forward any packet to the 192.168.2.0/24 network. When the router has to perform multiple lookups in the routing table before forwarding a packet, it is performing a process known as a ***recursive route lookup***. In this example:

1. The packet's destination IP address is matched to the static route 192.168.2.0/24 with the next-hop IP address 172.16.2.2.
2. The next-hop IP address of the static route, 172.16.2.2, is matched to the directly connected network 172.16.2.0/24, with the exit interface of Serial 0/0/0.

Every route that references only a next-hop IP address, and does not reference an exit interface, must have the next-hop IP address resolved using another route in the routing table that has an exit interface.

Typically, these routes are resolved to routes in the routing table that are directly connected networks, because these entries will always contain an exit interface. In the next section, you will see that static routes can be configured with an exit interface. This means that they do not need to be resolved using another route entry.

## Exit Interface Is Down

Consider what would happen if an exit interface goes down. For example, what would happen to R1's static route to 192.16.2.0/24 if its Serial 0/0/0 interface went down? If the static route cannot be resolved to an exit interface, in this case Serial 0/0/0, the static route is removed from the routing table.

Examine this process with the **debug ip routing** command on R1, and then configure the Serial 0/0/0 to **shutdown**, as shown in Example 2-33.

**Example 2-33** R1 Static Routes Depend on Exit Interface

```
R1# debug ip routing

IP routing debugging is on
R1# config t

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# int s0/0/0
R1(config-if)# shutdown
R1(config-if)# end

is_up: 0 state: 6 sub state: 1 line: 0
RT: interface Serial0/0/0 removed from routing table
RT: del 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 172.16.2.0/24
RT: del 192.168.1.0 via 172.16.2.2, static metric [1/0]
RT: delete network route to 192.168.1.0
RT: del 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
RT: delete subnet route to 172.16.1.0/24
R1# show ip route

<output omitted>
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
```

From Chapter 1, you know that the network attached to the Serial 0/0/0 interface is removed from the routing table. But also notice from the debug output that all three static routes were also deleted, because all three static routes were resolved to Serial 0/0/0. Now R1 only has one route in its routing table.

However, the static routes are still in R1's running configuration. If the interface comes back up (is enabled again with **no shutdown**), the IOS routing table process will reinstall these static routes into the routing table.

## Static Routes with Exit Interfaces

In the previous section, you saw how a static route can be configured with a next-hop address. Using a next-hop address is a correct method in configuring static routes. However, in some situations, using an exit interface can result in a more efficient route lookup process.

The simpler **ip route** command syntax is repeated here for easy reference:

```
Router(config)# ip route network-address subnet-mask {ip-address | exit-interface}
```

## Configuring a Static Route with an Exit Interface

Consider another way to configure the same static routes. Currently, R1's static route for the 192.168.2.0/24 network is configured with the next-hop IP address of 172.16.2.2. In the running configuration, note the following line:

```
ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

This static route requires a second routing table lookup to resolve the 172.16.2.2 next-hop IP address to an exit interface. However, most static routes can be configured with an exit interface, which allows the routing table to resolve the exit interface in a single search instead of two searches.

### Static Route and an Exit Interface

Reconfigure this static route to use an exit interface instead of a next-hop IP address. The first thing to do is to delete the current static route. This is done using the **no ip route** command, as shown in Example 2-34.

**Example 2-34** Static Route with an Exit Interface

```
R1(config)# no ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/0
R1(config)# end
R1# 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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#
```

Next, configure R1's static route to 192.168.2.0/24 using the exit interface Serial 0/0/0.

Then use the **show ip route** command to examine the change in the routing table. Notice that the entry in the routing table no longer refers to the next-hop IP address but refers directly to the exit interface. This exit interface is the same one that the static route was resolved to when it used the next-hop IP address:

```
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

Now, when the routing table process matches a packet to this static route, it will be able to resolve the route to an exit interface in a single lookup. As you can see from the routing table, the other two static routes still must be processed in two steps, resolving to the same Serial 0/0/0 interface.

**Note**

The static route displays the route as directly connected. It is important to understand that this does not mean that this route is a directly connected network or directly connected route. This route is still a static route. We will examine the importance of this fact when we discuss administrative distances in the next chapter. You will learn that this type of static route still has an administrative distance of 1. For now, just note that this route is still a static route with an administrative distance of 1 and is not a directly connected network.

## Static Routes and Point-to-Point Networks

Static routes that are configured with exit interfaces instead of next-hop IP addresses are ideal for most serial point-to-point networks. Point-to-point networks that use protocols such as HDLC and PPP do not use the next-hop IP address in the packet-forwarding process. The routed IP packet is encapsulated in an HDLC Layer 2 frame with a broadcast Layer 2 destination address.

These types of point-to-point serial links are like pipes. A pipe has only two ends. What enters one end can only have a single destination: the other end of the pipe. Any packets that are sent through R1's Serial 0/0/0 interface can only have one destination: R2's Serial 0/0/0 interface. R2's serial interface happens to be the IP address 172.16.2.2.

**Note**

Under certain conditions, the network administrator will not want to configure the static route with an exit interface but with the next-hop IP address. This type of situation is beyond the scope of this course but is important to note.

## Modifying Static Routes

There are times when a previously configured static route needs to be modified:

- The destination network no longer exists, and therefore the static route should be deleted.

- There is a change in the topology, and either the intermediate address or the exit interface has to be changed.

There is no way to modify an existing static route. The static route must be deleted and a new one configured.

To delete a static route, add **no** in front of the **ip route** command, followed by the rest of the static route to be removed.

For example, in the previous section, you removed the static route:

```
ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

with the following **no ip route** command:

```
no ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

As you will recall, the static route was deleted because you wanted to modify it to use an exit interface instead of a next-hop IP address. You configured a new static route using the exit interface:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/0
```

It is more efficient for the routing table lookup process to have static routes with exit interfaces, at least for serial point-to-point outbound networks. Reconfigure the rest of the static routes on R1, R2, and R3 to use exit interfaces as shown in Example 2-35.

**Example 2-35** Convert All Static Routes to Exit Interfaces

```
R1(config)# no ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)# no ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
R2(config)# no ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)# no ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0/1
```

```
R3(config)# no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)# no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)# no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

As you can see, as you delete each route, you will configure a new route to the same network using an exit interface.

## Verifying the Static Route Configuration

Whenever changes are made to static routes (or to other aspects of the network), verify that the changes took effect and that they produce the desired results.

### Verifying Static Route Changes

In the previous section, you deleted and reconfigured the static routes for all three routers, which can be verified with the **show running-config** command, as demonstrated in Example 2-36.

**Example 2-36** Verify Static Route Configuration with the **show running-config** Command

```
R1# show running-config

<output omitted>
ip route 172.16.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.2.0 255.255.255.0 Serial0/0/0
<output omitted>
```

```
R2# show running-config

<output omitted>
ip route 172.16.3.0 255.255.255.0 Serial0/0/0
ip route 192.168.2.0 255.255.255.0 Serial0/0/1
<output omitted>
```

```
R3# show running-config

<output omitted>
ip route 172.16.1.0 255.255.255.0 Serial0/0/1
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
<output omitted>
```

Remember, the running configuration contains the current router configuration—the commands and parameters that the router is currently using. Verify your changes by examining the running configuration. Example 2-36 shows only the static route portion of each router's running configuration.

Example 2-37 shows the routing table for all three routers. Notice that static routes with exit interfaces have been added to the routing table and that the previous static routes with next-hop addresses have been deleted.

**Example 2-37** Verify That New Routes Are Installed in the Routing Table

```
R1# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

```
R2# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 is directly connected, Serial0/0/1
```

```
R3# show ip route

<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

The ultimate test is to route packets from source to destination, as shown in Example 2-38.

**Example 2-38** Test End-to-End Connectivity with the **ping** Command

```
R1# ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

```
R2# ping 172.16.3.1

Type escape sequence to abort.
```

*continues*

*continued*

```
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R2#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3# ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

Using the **ping** command, you can verify that packets from each router are reaching their destination and that the return path is also working properly. Example 2-38 shows successful ping outputs.

Now it's time for you to practice configuring and verifying static routes.

Packet Tracer
☐ **Activity**

### Removing and Configuring Static Routes (2.5.6)

Use the Packet Tracer Activity to practice removing static routes and reconfiguring static routes using the exit interface argument. Then verify the new configuration and test connectivity. Use file e2-256.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

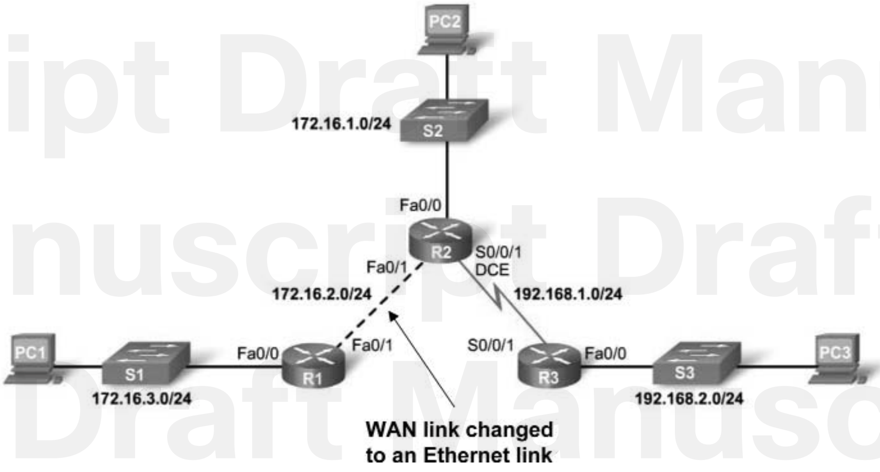
## Static Routes with Ethernet Interfaces

Sometimes the exit interface is an Ethernet network. An Ethernet interface on a router participates in the same processes as any other host on that Ethernet network, including ARP.

### Ethernet Interfaces and ARP

For this discussion, you need to modify the chapter topology as shown in Figure 2-10.

**Figure 2-10** Modified Chapter Topology



Suppose the network link between R1 and R2 is an Ethernet link and that each router's FastEthernet 0/1 interface is connected to that network. A static route, using a next-hop IP address for the 192.168.2.0/24 network, can be set using this command:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

As discussed in the section "Configuring an Ethernet Interface," earlier in this chapter, the IP packet must be encapsulated into an Ethernet frame with an Ethernet destination MAC address. If the packet should be sent to a next-hop router, the destination MAC address will be the address of the next-hop router's Ethernet interface. In this case, the Ethernet destination MAC address will be matched to the next-hop IP address 172.16.2.2. R1 checks its FastEthernet 0/1 ARP table for an entry with 172.16.2.2 and a corresponding MAC address.

## Sending an ARP Request

If this entry is not in the ARP table, R1 sends an ARP request through its FastEthernet 0/1 interface. The Layer 2 broadcast is requesting that if any device has the IP address 172.16.2.2, it should respond with its MAC address. Because R2's FastEthernet 0/1 interface has the IP address 172.16.2.2, it sends back an ARP reply with the MAC address for that interface.

R1 receives the ARP reply and adds the 172.16.2.2 IP address, and the associated MAC address, to its ARP table. The IP packet is now encapsulated into an Ethernet frame with the destination MAC address found in the ARP table. The Ethernet frame with the encapsulated packet is then sent out the FastEthernet 0/1 interface to Router R2.

### Static Routes and Ethernet Exit Interfaces

Configure a static route with an Ethernet exit interface instead of a next-hop IP address. Change the static route for 192.168.2.0/24 to use an exit interface with this command:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 fastethernet 0/1
```

The difference between an Ethernet network and a point-to-point serial network is that a point-to-point network has only one other device on that network: the router at the other end of the link. With Ethernet networks, many different devices can be sharing the same multiaccess network, including hosts and even multiple routers. By only designating the Ethernet exit interface in the static route, the router will not have sufficient information to determine which device is the next-hop device.

R1 knows that the packet needs to be encapsulated in an Ethernet frame and sent out the FastEthernet 0/1 interface. However, R1 does not know the next-hop IP address, and therefore it cannot determine the destination MAC address for the Ethernet frame.

Depending on the topology and the configurations on other routers, this static route might or might not work. Recommended practice dictates that when the exit interface is an Ethernet network, you do not use only the exit interface in the static route.

You might ask: Is there any way to configure a static route over an Ethernet network so that it does not have to use the recursive lookup of the next-hop IP address? Yes, this can be done by configuring the static route to include both the exit interface and the next-hop IP address.

As you can see in Figure 2-10, the exit interface would be FastEthernet 0/1 and the next-hop IP address would be 172.16.2.2:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 fastethernet 0/1 172.16.2.2
```

The routing table entry for this route would be:

```
S     192.168.2.0/24 [1/0] via 172.16.2.2 FastEthernet0/1
```

The routing table process will only need to perform a single lookup to get both the exit interface and the next-hop IP address.

### Advantages of Using an Exit Interface with Static Routes

There is an advantage to using exit interfaces in static routes for both serial point-to-point and Ethernet outbound networks. The routing table process only has to perform a single lookup to find the exit interface instead of a second lookup to resolve a next-hop address.

For static routes with outbound point-to-point serial networks, it is best to configure static routes with only the exit interface. For point-to-point serial interfaces, the next-hop address in the routing table is never used by the packet delivery procedure, and so it is not needed.

For static routes with outbound Ethernet networks, it is best to configure the static routes with both the next-hop address and the exit interface.

**Note**

For more information about the issues that can occur with static routes that only use an Ethernet or Fast Ethernet exit interface, see *Cisco IP Routing*, by Alex Zinin.

# Summary and Default Static Routes

A router might have a specific route entry in its routing table for a destination network, or that same network can be part of a less specific route entry. The less specific route entry might be a summary route or a default route.

## Summary Static Routes

A ***summary route*** is a single route that can be used to represent multiple routes. Summary routes are generally a set of contiguous networks that have the same exit interface and/or next-hop IP address.

**Note**

The networks represented in a summary route do not have to be contiguous. This is explained later in Chapter 8.

### Summarizing Routes to Reduce the Size of the Routing Table

Creating smaller routing tables makes the routing table lookup process more efficient, because there are fewer routes to search. If one static route can be used instead of multiple static routes, the size of the routing table will be reduced. In many cases, a single static route can be used to represent dozens, hundreds, or even thousands of routes.

You can use a single network address to represent multiple subnets. For example, the networks 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16, 10.5.0.0/16, all the way through 10.255.0.0/16 can be represented by a single network address: 10.0.0.0/8.

### Route Summarization

Multiple static routes can be summarized into a single static route if they meet both of the following criteria:

- The destination networks can be summarized into a single network address.
- The multiple static routes all use the same exit interface or next-hop IP address.

This is called ***route summarization***.

In our static route configuration of the chapter topology (Figure 2-1), R3 has three static routes. All three routes are forwarding traffic out the same Serial 0/0/1 interface. The three static routes on R3 are

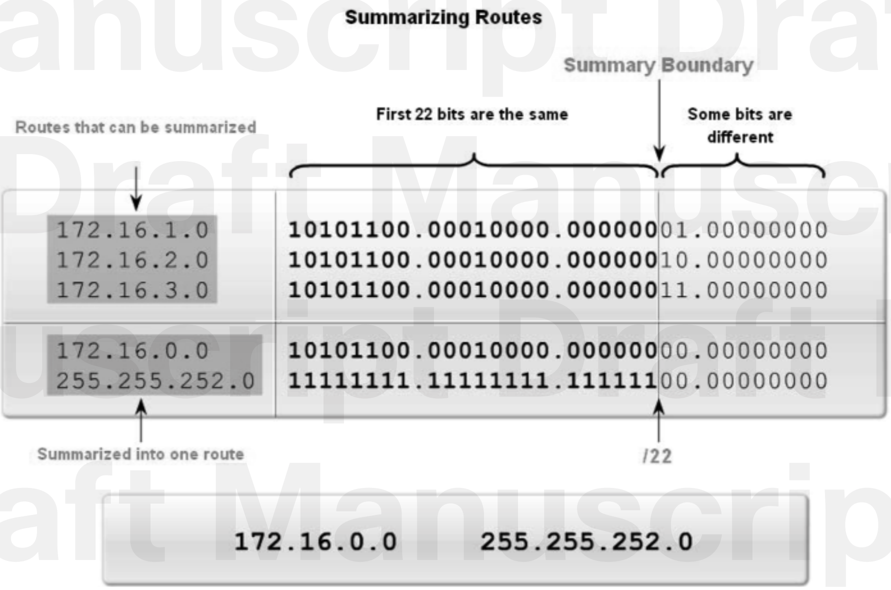
```
ip route 172.16.1.0 255.255.255.0 Serial0/0/1
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

If possible, you'll want to summarize all of these routes into a single static route. The networks 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 can be summarized to the 172.16.0.0/22 network. Because all three routes use the same exit interface, they can be summarized to the single 172.16.0.0 255.255.252.0 network, and you can create a single summary route.

## Calculating a Summary Route

Here's the process of creating the summary route 172.16.1.0/22, as shown in Figure 2-11:

**Figure 2-11** Summarizing Routes



**How To**

**Step 1.** Write out the networks that you want to summarize in binary.

**Step 2.** To find the subnet mask for summarization, start with the leftmost bit.

**Step 3.** Work your way to the right, finding all the bits that match consecutively.

**Step 4.** When you find a column of bits that do not match, stop. You are at the summary boundary.

**Step 5.** Count the number of leftmost matching bits, which in our example is 22. This number becomes your subnet mask for the summarized route, /22 or 255.255.252.0.

**Step 6.** To find the network address for summarization, copy the matching 22 bits and add all 0 bits to the end to make 32 bits.

By following these steps, you can discover that the three static routes on R3 can be summarized into a single static route, using the summary network address of 172.16.0.0 255.255.252.0:

```
ip route 172.16.0.0 255.255.252.0 Serial0/0/1
```

## Configuring a Summary Route

To implement the summary route, you must first delete the three current static routes:

```
R3(config)# no ip route 172.16.1.0 255.255.255.0 serial0/0/1
R3(config)# no ip route 172.16.2.0 255.255.255.0 serial0/0/1
R3(config)# no ip route 172.16.3.0 255.255.255.0 serial0/0/1
```

Next, you will configure the summary static route:

```
R3(config)# ip route 172.16.0.0 255.255.252.0 serial0/0/1
```

Example 2-39 shows the change in the routing table with three static routes now represented by a single summary static route. To verify the new static route, examine R3's routing table with the **show ip route** command, as shown in the example.

**Example 2-39** Three Static Routes Summarized into One Summary Route

```
R3# show ip route

<output omitted>

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0

R3# show ip route

<output omitted>
```

*continues*

*continued*

```
Gateway of last resort is not set

        172.16.0.0/22 is subnetted, 1 subnets
S           172.16.0.0 is directly connected, Serial0/0/1
C       192.168.1.0/24 is directly connected, Serial0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
```

With this summary route, the destination IP address of a packet only needs to match the leftmost 22 bits of the 172.16.0.0 network address. Any packet with a destination IP address belonging to the 172.16.1.0/24, 172.16.2.0/24, or 172.16.3.0/24 network matches this summarized route.

As shown in Example 2-40, you can test the reconfiguration using the **ping** command to verify that proper connectivity exists throughout the network.

**Example 2-40** Verify the Summary Route with the **ping** Command

```
R3# ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R3#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#
```

**Note**

As of March 2007, there are more than 200,000 routes in the Internet core routers. Most of these are summarized routes.

## Default Static Route

A default route is used to represent all routes with zero or no bits matching. In other words, when there are no routes that have a more specific match, the default route will be a match. The following section will discuss a default static route. Default routes will be discussed and used throughout this book.

### Most Specific Match

The destination IP address of a packet can match multiple routes in the routing table. For example, consider having the following two static routes in the routing table:

```
         172.16.0.0/24 is subnetted, 3 subnets
S           172.16.1.0 is directly connected, Serial0/0/0
S           172.16.0.0/16 is directly connected, Serial0/0/1
```

Consider a packet with the destination IP address 172.16.1.10. This IP address matches both routes. The routing table lookup process will use the most specific match. Because 24 bits match the 172.16.1.0/24 route, and only 16 bits of the 172.16.0.0/16 route match, the static route with the 24-bit match will be used. This is the most specific or longest match. The packet will then be encapsulated in a Layer 2 frame and sent through the Serial 0/0/0 interface. Remember, the subnet mask in the route entry is what determines how many bits must match the packet's destination IP address for this route to be a match.

**Note**

This process is the same for all routes in the routing table, including static routes, routes learned from a routing protocol, and directly connected networks. The routing table lookup process will be explained in more detail in Chapter 8.

A default static route is a route that will match all packets. Default static routes are used

- To represent destination networks outside the router's own routing domain. A common use is when connecting a company's edge router to the ISP network.
- When no other routes in the routing table match the packet's destination IP address, in other words, when a more specific match does not exist.
- When a router has only one other router to which it is connected. This condition is known as a stub router.

This will become more evident in later chapters when discussing dynamic routing protocols.

### Configuring a Default Static Route

The syntax for a default static route is similar to any other static route, except that the network address is 0.0.0.0 and the subnet mask is 0.0.0.0:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface ¦ ip-address ]
```

The 0.0.0.0 0.0.0.0 network address and mask is called a ***quad-zero route***.

Look back at Figure 2-9. Remember that in this topology, R1 is a stub router and is connected only to R2. Although the chapter topology (Figure 2-1) shows an R3 router, R1 doesn't need specific routing information to reach R3 networks. Currently R1 has three static routes, which are used to reach all the remote networks in our chapter topology. All three static routes have the exit interface Serial 0/0/0, forwarding packets to the next-hop Router R2.

As a review, the three static routes on R1 are

```
ip route 172.16.1.0 255.255.255.0 serial 0/0/0
ip route 192.168.1.0 255.255.255.0 serial 0/0/0
ip route 192.168.2.0 255.255.255.0 serial 0/0/0
```

As shown in Figure 2-9, R1 is an ideal candidate to have all of its static routes replaced by a single default route. First, delete the three static routes:

```
R1(config)# no ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)# no ip route 192.168.1.0 255.255.255.0 serial 0/0/0
R1(config)# no ip route 192.168.2.0 255.255.255.0 serial 0/0/0
```

Next, configure the single default static route using the same Serial 0/0/0 exit interface as the three previous static routes:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

## Verifying a Default Static Route

Verify the change to the routing table with the **show ip route** command. Example 2-41 shows the routing table before the default route configuration.

**Example 2-41** R1 Routing Table Before Default Route Is Configured

```
R1# show ip route

<output omitted>

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

Example 2-42 shows the routing table after the default route configuration.

**Example 2-42** R1 Routing Table After Default Route Is Configured

```
R1# show ip route

<some codes omitted>
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

Note that the asterisk (*) next to the S code marks the default route. That is why it is called a "default static" route. You will see in later chapters that a default route does not always have to be a static route.

The key to this configuration is the /0 mask. Previously, you learned that it is the subnet mask in the routing table that determines how many bits must match between the destination IP address of the packet and the route in the routing table. A /0 mask indicates that zero or no bits are needed to match. As long as a more specific match doesn't exist, the default static route will match all packets.

Default routes are very common on routers. Instead of routers having to store routes for all the networks in the Internet, they can store a single default route to represent any network that is not in the routing table. This topic will be discussed in more detail in Chapter 3, "Introduction to Dynamic Routing Protocols."

Now it's time for you to practice configuring and verifying default static routes.

Packet Tracer
☐ **Activity**

**Configuring a Default Route (2.6.2)**

Use the Packet Tracer Activity to practice configuring summary routes and default routes. Then verify the new configuration by testing for connectivity. Use file e2-262.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

# Managing and Troubleshooting Static Routes

It is important to be able to properly manage and troubleshoot static routes. When a static route is no longer needed, that static route should be deleted from the running and startup configuration files.

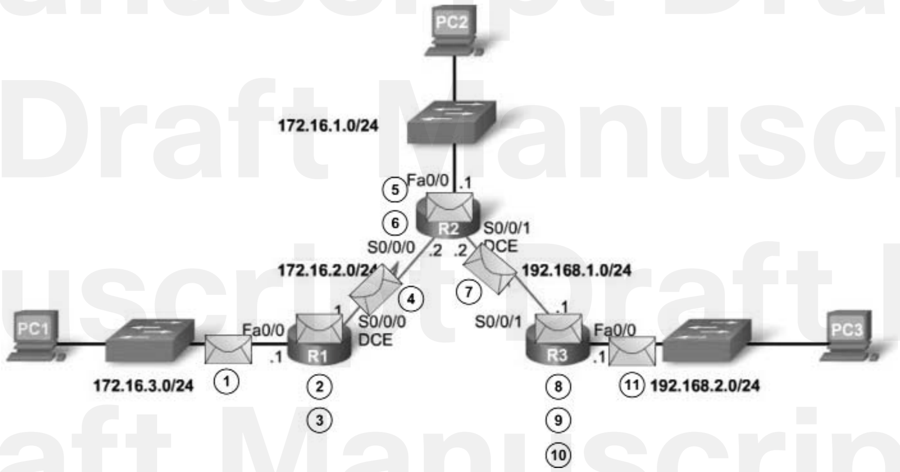
## Static Routes and Packet Forwarding

Now that you have configured static routes on all three routers in the topology, you need to learn about the process that a packet goes through as it is forwarded by these routers.

### Static Routes and Packet Forwarding

Figure 2-12 and the following steps illustrate the packet-forwarding process with static routes. In this example, R1, R2, and R3 are routing traffic between PC1 and PC3. Only the processing of traffic from PC1 to PC3 is shown. However, the same process is used for traffic from PC3 back to PC1.

**Figure 2-12** Static Routes and Packet Forwarding



The packet-forwarding process of a packet from R1 to R3 is as follows:

1. The packet arrives on the FastEthernet 0/0 interface of R1.
2. R1 does not have a specific route to the destination network, 192.168.2.0/24; therefore, R1 uses the default static route.
3. R1 encapsulates the packet in a new frame. Because the link to R2 is a point-to-point link, R1 adds an “all 1s” address for the Layer 2 destination address.

4. The frame is forwarded out the Serial 0/0/0 interface. The packet arrives on the Serial 0/0/0 interface on R2.
5. R2 decapsulates the frame, examines the packet's destination IP address, and looks for a route to the destination. R2 has a static route to 192.168.2.0/24 out Serial 0/0/1.
6. R2 encapsulates the packet in a new frame. Because the link to R3 is a point-to-point link, R2 adds an "all 1s" address for the Layer 2 destination address.
7. The frame is forwarded out the Serial 0/0/1 interface. The packet arrives on the Serial 0/0/1 interface on R3.
8. R3 decapsulates the frame, examines the packet's destination IP address, and looks for a route to the destination. R3 has a connected route to 192.168.2.0/24 out FastEthernet 0/1.
9. R3 looks up the ARP table entry for 192.168.2.10 to find the Layer 2 MAC address for PC3:
    a. If no entry exists, R3 broadcasts an ARP request out FastEthernet 0/0.
    b. PC3 responds with an ARP reply that includes the PC3 MAC address.
10. R3 encapsulates the packet in a new frame with the MAC address of interface FastEthernet 0/0 as the source Layer 2 address and the MAC address of PC3 as the destination MAC address.
11. The frame is forwarded out the FastEthernet 0/0 interface. The packet arrives on the NIC interface of PC3.

This process is no different from the process demonstrated in Chapter 1. You must be able to describe this process in detail. Knowing how a router performs its two basic functions—path determination and packet forwarding—is fundamental to all routing discussions. In Lab 2-1: Basic Static Route Configuration (2.8.1), you have an opportunity to demonstrate your knowledge of the path determination and packet-forwarding process.

## Troubleshooting a Missing Route

Troubleshooting is a skill that develops as you gain more experience. It is always best to look for the most obvious and simplest issues first, such as an interface still in shutdown mode or an interface with the wrong IP address. After these items have been verified, begin looking for more complicated possibilities like an error in the static route configuration.

### Troubleshooting a Missing Route

When end-to-end connectivity is a problem, begin by making sure that you can ping your own interface and other devices on your own directly connected networks. When this has been verified, begin testing connectivity to remote networks and from other devices as well.

Networks are subject to many different forces that can cause their status to change quite often:

- Interface failure
- Dropped connection by a service provider
- Oversaturation of links
- Incorrect configuration entered by an administrator

When there is a change in the network, connectivity might be lost. As a network administrator, you are the one responsible for pinpointing and solving the problem. What steps can you take?

By now, you should be familiar with some tools that can help you isolate routing problems:

- **ping**
- **traceroute**
- **show ip route**

Although this and preceding chapters have not discussed **traceroute**, you should be familiar with its capabilities from previous studies. Recall that the **traceroute** command will find a break in the path from source to destination.

As we go further into this course, you will discover more tools. For example, the **show ip interface brief** command gives you a quick summary of interface status. CDP can help you gather information about the IP configuration of a directly connected Cisco device using the **show cdp neighbors detail** command.

## Solving the Missing Route

The following is an example of solving a missing static route using the network topology from Figure 2-1.

Finding a missing (or misconfigured) route is relatively straightforward if you methodically use the correct tools.

Consider this problem: PC1 cannot ping PC3. A traceroute reveals that R2 is responding but that there is no response from R3. Displaying the routing table shown in Example 2-43, R2 reveals that the 172.16.3.0/24 network is configured incorrectly.

**Example 2-43** Misconfigured Static Route

```
R2# show ip route

<output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

The exit interface is configured to send packets to R3. Obviously, from the topology, you can see that R1 has the 172.16.3.0/24 network. Therefore, R2 must use Serial 0/0/0 as the exit interface, not Serial 0/0/1.

To remedy the situation, remove the incorrect route and add the route for network 172.16.3.0/24 with Serial 0/0/0 specified as the exit interface:

```
R2(config)# no ip route 172.16.3.0 255.255.255.0 serial0/0/1
R2(config)# ip route 172.16.3.0 255.255.255.0 serial 0/0/0
```

**Tip**

Always remove the incorrect static route. The command that properly configures the static route will not remove the incorrect command.

The final Packet Tracer Activity associated with this chapter explores another issue with static routes. As you will see, it is possible to inadvertently configure a loop in your network using static routes.

Packet Tracer
☐ **Activity**

### Solving the Missing Route (2.7.3)

Use the Packet Tracer Activity to see how the loop explained in this section can occur. In simulation mode, watch as R2 and R3 loop a packet for 172.16.3.10 until the Time to Live (TTL) field reaches 0. Then fix the problem and test for connectivity between PC1 and PC3. Use file e2-273.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

## Summary

In this chapter, you learned how static routes can be used to reach remote networks. Remote networks are networks that can only be reached by forwarding the packet to another router. Static routes are easily configured. However, in large networks, this manual operation can become quite cumbersome. As you will see in later chapters, static routes are still used, even when a dynamic routing protocol is implemented.

Static routes can be configured with a next-hop IP address, which is commonly the IP address of the next-hop router. When a next-hop IP address is used, the routing table process must resolve this address to an exit interface. On point-to-point serial links, it is usually more efficient to configure the static route with an exit interface. On multiaccess networks such as Ethernet, both a next-hop IP address and an exit interface should be configured on the static route.

Static routes have a default administrative distance of 1. This administrative distance also applies to static routes configured with a next-hop address as well as an exit interface.

A static route will only be entered in the routing table if the next-hop IP address can be resolved through an exit interface. Regardless of whether the static route is configured with a next-hop IP address or exit interface, if the exit interface—the directly connected network that is used to forward that packet—is not in the routing table, the static route will not be included in the routing table.

In many cases, several static routes can be configured as a single summary route. This means fewer entries in the routing table and results in a faster routing table lookup process. The ultimate summary route is a default route, configured with a 0.0.0.0 network address and a 0.0.0.0 subnet mask. If there is not a more specific match in the routing table, the routing table will use the default route to forward the packet to another router.

**Note**

The routing table lookup process is examined more closely in Chapter 8.

## Labs

The labs available in the companion *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-204-4) provide hands-on practice with the following topics introduced in this chapter:

### Lab 2-1: Basic Static Route Configuration (2.8.1)

In this lab activity, you will create a network like the one used in this chapter. You will cable the network and perform the initial router configurations required for connectivity. After completing the basic configuration, you will test connectivity among the devices on the network. You will then configure the static routes that are needed to allow communication between the hosts.

### Lab 2-2: Challenge Static Route Configuration (2.8.2)

In this lab activity, you will be given a network address that must be subnetted to complete the addressing of the network. The addressing for the LAN connected to the ISP router and the link between the HQ and ISP routers have already been completed. Static routes will also need to be configured so that hosts on networks that are not directly connected will be able to communicate with each other.

### Lab 2-3: Troubleshooting Static Routes (2.8.3)

In this lab, you will begin by loading corrupted configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

Packet Tracer
**Companion**

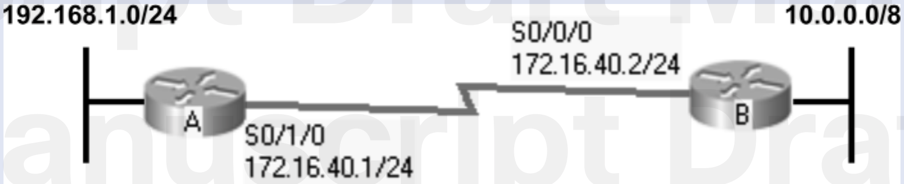
Many of the hands-on labs include Packet Tracer Companion Activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-204-4) for hands-on labs that have a Packet Tracer Companion.

## Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The section "Check Your Understanding and Challenge Questions Answer Key" at the end of this chapter lists the answers.

1. Refer to Figure 2-13. Which two commands must be configured to allow communication between the 192.168.1.0/24 and 10.0.0.0/8 networks?

**Figure 2-13** Topology for Quiz Question #1



A. A(config)# **ip route 10.0.0.0 255.0.0.0 172.16.40.2**

B. A(config)# **ip route 10.0.0.0 255.0.0.0 s0/0/0**

C. A(config)# **ip route 10.0.0.0 255.0.0.0 10.0.0.1**

D. B(config)# **ip route 192.168.1.0 255.255.255.0 172.16.40.1**

E. B(config)# **ip route 192.168.1.0 255.255.255.0 172.16.40.2**

F. B# **ip route 192.168.1.0 255.255.255.0 192.168.1.1**

2. Which statement is true concerning configuring static routes using next-hop addresses?

A. Routers cannot use more than one static route with a next-hop address.

B. When the router identifies that a packet is destined for a route associated with a next-hop address in the routing table, the router requires no further information and can immediately forward the packet.

C. Routers configured with the static route using a next-hop address must either have the exit interface listed in the route or have another route with the network of the next hop and an associated exit interface.

D. Routes associated with a next-hop address are more efficient than routes going to exit interfaces.

**3.** Refer to the following command output. The network administrator must remove the route to the 10.0.0.0 network. What command will accomplish this task?

```
R1# show ip route

<output omitted>

Gateway of last resort is not set

S    10.0.0.0/8 [1/0] via 172.16.40.2
     64.0.0.0/16 is subnetted, 1 subnets
C      64.100.0.0 is directly connected, Serial0/1
C    128.107.0.0/16 is directly connected, Loopback2
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.40.0 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEhternet0/0
C    192.168.2.0/24 [1/0] via 172.16.40.2
C    198.133.219.0/24 is directly connected, Loopback0
```

A. **no ip address 10.0.0.1 255.255.255.0 172.16.40.2**

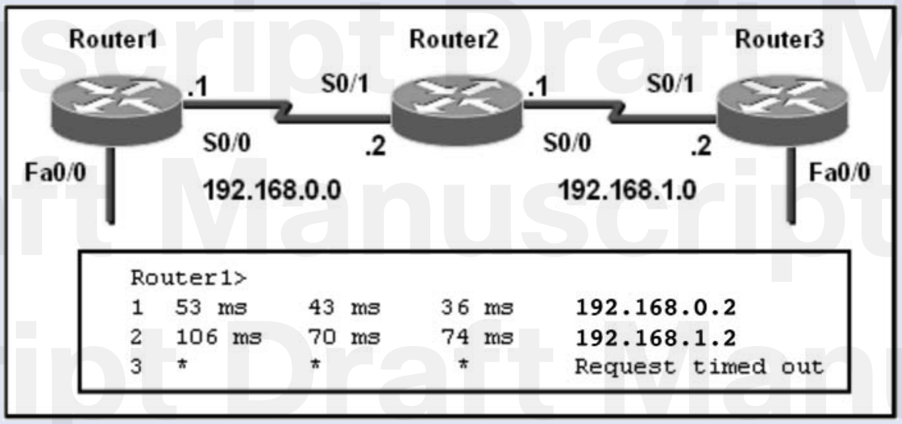
B. **no static-route 10.0.0.0 255.0.0.0**

C. **no ip route 10.0.0.0 255.0.0.0 172.16.40.2**

D. **no ip route 10.0.0.1 255.255.255.0**

**4.** Refer to Figure 2-14. What command was used on Router1 to produce the output shown in the graphic?

**Figure 2-14** Topology for Quiz Question #4



```
Router1>
1  53 ms    43 ms    36 ms    192.168.0.2
2  106 ms   70 ms    74 ms    192.168.1.2
3  *        *        *        Request timed out
```

A. **traceroute**

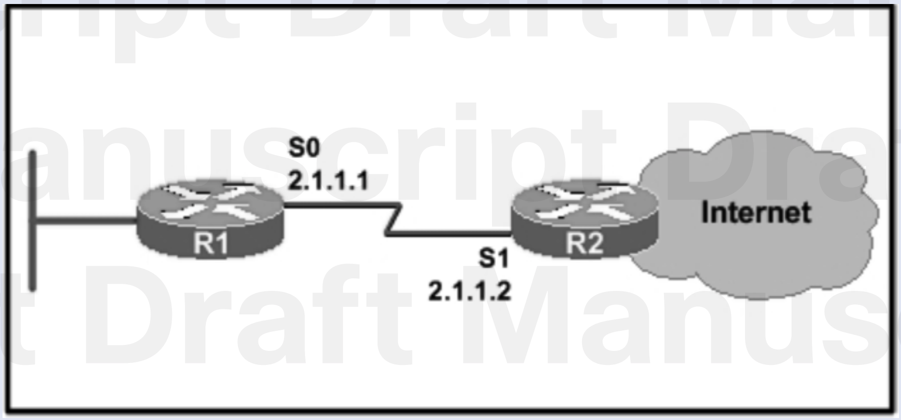
B. **extended ping**

C. **show ip route**

D. **show cdp neighbor detail**

5. Refer to Figure 2-15. Which command correctly configures a static default route on R1?

**Figure 2-15** Topology for Quiz Question #5



A. R1(config-if)# **ip route 0.0.0.0 0.0.0.0 s0**
B. R1(config)# **ip route 0.0.0.0 0.0.0.0 s1**
C. R1(config-if)# **ip route 0.0.0.0 0.0.0.0 2.1.1.2**
D. R1(config)# **ip route 0.0.0.0 0.0.0.0 2.1.1.2**
E. R1(config-router)# **default-information originate**

6. Which of the following are three characteristics of a static route?

A. Reduces the memory and processing burdens on a router
B. Ensures that there is always a path available
C. Used to dynamically find the best path to a destination network
D. Used for routers that connect to stub networks
E. Used for networks with a single route to a destination network
F. Reduces configuration time

7. Which of the following is a function of the IOS command **show cdp neighbors**?

A. It displays the port type and platform of neighboring Cisco routers.
B. It displays the device capability code of all non-Cisco routers.
C. It displays platform information for all devices in the network.
D. It displays the protocol encapsulation used by neighboring routers.

**8.** Refer to Figure 2-16. What type of connector is shown in the exhibit?

**Figure 2-16** Graphic for Quiz Question #8

A. The DB-60 DTE end of the serial cable for 1600 and 2500 series routers

B. The DTE end of a smart serial cable used with newer routers

C. The EIA/TIA-530 DCE end of a serial cable that plugs into the CSU/DSU

D. The V.35 DCE end of a serial cable that plugs into the CSU/DSU

E. The EIA/TIA-232 DCE end of a serial cable that plugs into the CSU/DSU

F. The EIA/TIA-449 DCE end of a serial cable that plugs into the CSU/DSU

**9.** Which statement is true concerning directly connected routes?

A. They appear in the routing table as soon as cables are connected to the router.

B. They appear in the routing table when an IP address is configured on an interface.

C. They appear in the routing table when the **no shutdown** command is entered in router interface configuration mode.

D. They appear in the routing table when the **show interface** command shows that the interface is up, line protocol is up.

**10.** Choose the proper command that is associated with each of the following configuration tasks.

**Configuration tasks:**

Enter global configuration mode:

Enter interface configuration mode:

Configure an IP address:

Activate the interface:

**Commands:**

A. **interface fastethernet 0/0**
B. **ip address 192.168.35.11 255.255.255.0**
C. **ip address 192.168.35.11/24**
D. **config terminal**
E. **ip 192.168.35.11 255.255.255.0**
F. **ip 192.168.35.11/24**
G. **no shutdown**
H. **show interfaces fastethernet 0/0**

**11.** Match the following **show/debug** commands with the proper outputs:

**show ip route**:

**show ip interface brief**:

**show interfaces**:

**show controllers**:

**debug ip routing**:

**show cdp neighbors**:

Output:

A. Display all known networks
B. Display detailed port information
C. Display routing troubleshooting information
D. Display basic port information
E. Display directly connected routers
F. Display DTE/DCE information

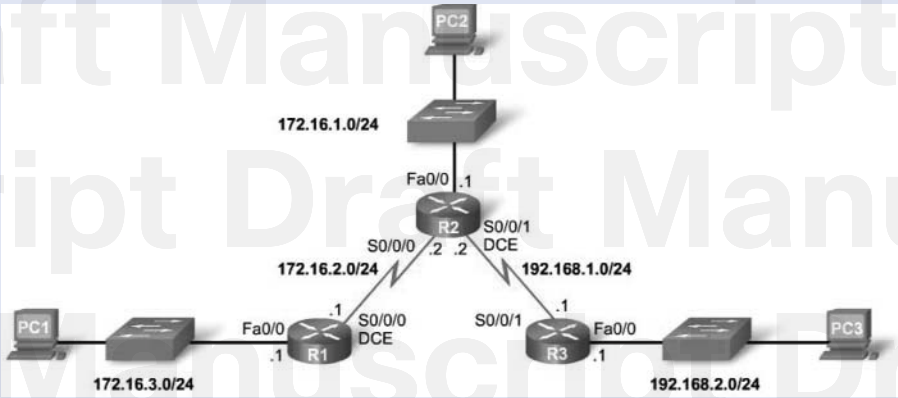
12. Describe the cabling used to connect devices to an Ethernet LAN.
13. List three commands used to display interface configuration information.
14. Explain the difference between attaching a serial interface to a service provider in a production environment and attaching a serial interface to another router in a lab environment.
15. What is CDP and why would you want to disable it?
16. What is the simpler form used for the **ip route** syntax?
17. What is a recursive route lookup and when does it occur?
18. Why must you remove a static route from the configuration before modifying it?
19. Explain the value of summary and default routes.
20. List the commands used to test and troubleshoot a network implementation.

## Challenge Questions and Activities

These questions and activities require a deeper application of the concepts covered in this chapter. You can find the answers later in the chapter.

1. On some newer computers, it does not matter whether you attach a straight-through or crossover cable to the device. The computer successfully connects to the other device. Why do you think this happens?
2. All network interfaces are up and up. PC1, PC2, and PC3 have full connectivity. Pings from R1 to R2 and R3 are successful. However, although pings from R3 to R2 are successful, R3 cannot ping either address on R1. Using Figure 2-17 and the following command output, identify the problem, explain why the ping fails, and suggest a solution.

**Figure 2-17** Topology for Challenge Question #2



```
R1# show ip interface brief

Interface           IP-Address      OK? Method Status                Protocol
FastEthernet0/0     172.16.3.1      YES manual up                    up
Serial0/0/0         172.16.2.1      YES manual up                    up
FastEthernet0/1     unassigned      YES manual administratively down down
Serial0/0/1         unassigned      YES manual administratively down down
```

```
R2# show ip interface brief

Interface           IP-Address      OK? Method Status                Protocol
FastEthernet0/0     172.16.1.1      YES manual up                    up
Serial0/0/0         172.16.2.2      YES manual up                    up
FastEthernet0/1     unassigned      YES manual administratively down down
Serial0/0/1         192.168.1.1     YES manual up                    up
```

```
R3# show ip interface brief

Interface           IP-Address      OK? Method Status                Protocol
FastEthernet0/0     192.168.2.1     YES manual up                    up
Serial0/0/0         unassigned      YES manual administratively down down
FastEthernet0/1     unassigned      YES manual administratively down down
Serial0/0/1         192.168.1.1     YES manual up                    up
```

3. Use the output from the **show cdp neighbors** commands that follow to draw the topology on a piece of paper. Show connections between devices and label the interfaces. All devices are unique. For example, there is only one EAST router and one S1 switch.

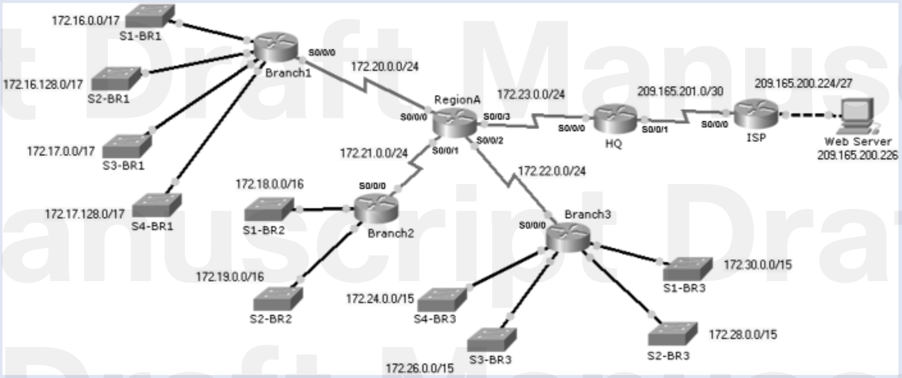
```
HQ# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability   Platform    Port ID
S4            FastEthernet0/0  151            S        WS-C2960    Fas 0/16
EAST          Serial0/0         163            R         C1841       Ser 0/1
WEST          Serial0/1         169            R         C1841       Ser 0/0
```

```
EAST# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability   Platform    Port ID
S1            FastEthernet0/1  177            S        WS-C2960    Fas 0/3
HQ            Serial0/1         128            R         C1841       Ser 0/0
S2            FastEthernet0/0  133            S        WS-C2960    Fas 0/3
```

```
WEST# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability   Platform    Port ID
S1            FastEthernet0/0  176            S        WS-C2960    Fas 0/4
HQ            Serial0/0         126            R         C1841       Ser 0/1
S3            FastEthernet0/1  156            S        WS-C2960    Fas 0/12
```

4. In Figure 2-18, all the Branch routers need to be configured with a default route to RegionA. RegionA needs a default route to HQ, and HQ needs a default route to ISP. RegionA can summarize each of the LANs attached to each Branch router with one static route pointing to each of the Branch routers. HQ and ISP can summarize all the LANs with just one static route. Using the exit interface argument, what are the static default routes for each Branch router, for RegionA, and for HQ? What are the summary static routes configured on RegionA, HQ, and ISP? Build the topology in Packet Tracer, and test your static and default routing commands. The Web Server should be able to ping every interface on every router.

**Figure 2-18** Topology for Challenge Question #4



## To Learn More

Static routes can have other uses besides what we have seen in this chapter. Other common static routes include floating static routes and discard routes.

### Floating Static Routes

A floating static route is a backup route to a route that is either a dynamic route or another static route. The default administrative distance of a static route is 1. See whether you can create a static route using a different exit interface or next-hop IP address, which would only be added to the routing table if the primary static route fails.

Hint: Remember, if the router has two routes to the same destination network with two different administrative distance values, it will add the route with the lower administrative distance. A static route will be removed from the routing table if the exit interface or next-hop IP address is no longer available.

## Discard Route

A common configuration in many networks is to have a static default route on the edge router forwarding packets to the ISP. The ISP router then has a static route pointing to the customer's network.

For example, customer A has the network address of 172.16.0.0/16, which is subnetted into several /24 subnets. The edge router of customer A has a static default route forwarding all other traffic to the ISP router:

```
ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

The ISP router has a static default route for forwarding traffic to customer A's network:

```
ip route 172.16.0.0 255.255.0.0 serial 0/0/1
```

A problem can occur when packets are originated from the customer A's network for a subnet that does not exist. Customer A's edge router will use its default route to forward those packets onto the ISP. The ISP router will receive those packets and send them back to customer A's edge router because they are part of the 172.16.0.0/16 network. The edge router will once again send them back to the ISP. The packets are caught in a loop until the TTL of the packet expires.

Configure a static route on customer A's edge router to discard those packets instead of forwarding them onto the ISP router.

## Further Reading on Static Routing

Although static routes can be easily understood and configured, there are some situations when the IOS processing of static routes can be quite complex. This is especially true when there are various static routes configured that cover the same range of networks.

Alex Zinin's book, *Cisco IP Routing*, covers static routing and IOS's static route processing in detail. This book goes beyond just the configuration and looks at the inner workings of the Cisco IOS and its routing processes.

## End Notes

1. Zinin, A. *Cisco IP Routing: Packet Forwarding and Intra-domain Routing Protocols*. Indianapolis, IN: Addison-Wesley; 2002.

# Check Your Understanding and Challenge Questions Answer Key

## Check Your Understanding

1. A, D. The **ip route 10.0.0.0 255.0.0.0 172.16.40.2** command is used by Router A to reach Router B's remote network. The **ip route 192.168.1.0 255.255.255.0 172.16.40.1** command is used by Router B to reach Router A's remote network. Both commands used the IP address of the next-hop router.
2. C. All routes in the routing table must be resolved to an exit interface in the routing table. If a route only has a next-hop IP address, that next-hop address must eventually be resolved to another route in the routing table that does include an exit interface, such as a directly connected network. Some static routes, such as those with Ethernet exit interfaces, can include both an exit interface and a next-hop IP address.
3. C. The 10.0.0.0/8 route is a static route. The way to remove a static route is to use the static route command prefaced with the **no** option.
4. A. This output was displayed using the **traceroute** command. The numbers in the column on the left indicate a router in the path.
5. D. R1(config)# **ip route 0.0.0.0 0.0.0.0 2.1.1.2** is the correct command because it is configured from global configuration mode, uses the network/mask of 0.0.0.0 0.0.0.0, and uses 2.1.1.2 as the correct next-hop IP address.
6. A, D, E. Configuring a static route does not ensure that the path is always available. If the exit interface or next-hop IP address is in the up state, the static route will be included in the routing table, regardless of whether the destination network is available. Dynamic routing protocols are typically a better option when there are multiple routes to the same destination network. The routing protocol will be able to automatically determine the best path.
7. A. The **show cdp neighbors** command displays the port type and platform of neighboring Cisco routers. It will not necessarily show non-Cisco devices.
8. B. This is a DTE end of a smart serial cable. It is a DTE end because the connector is male.
9. D. Directly connected networks will only be added to the routing table when the interface and line protocol are up, which can be displayed using the **show interface** command. For the interface and line protocol to be up, the interface must be configured with an IP address and subnet mask.

10. Enter global configuration mode: D

    Enter interface configuration mode: A

    Configure an IP address: B

    Activate the interface: G

11. **show ip route:** A

    **show ip interface brief**: D

    **show interfaces**: B

    **show controllers**: F

    **debug ip routing**: C

    **show cdp neighbors**: E

12. Straight-through cables are used to connect PCs and routers to hubs and switches. Crossover cables are used to connect PCs to routers, hubs to switches, routers to routers, and switches to switches.

13. **show interfaces**, **show ip interface brief**, **show running-config**

14. In a production environment, serial interfaces are attached to service provider equipment. Normally, the service provider sets the clocking speed. In a lab environment, routers are directly connected through the serial interface. Therefore, one of the routers must provide the clocking speed.

15. CDP, or Cisco Discovery Protocol, is a proprietary protocol for gathering information about directly connected Cisco devices. For example, a Cisco router and a Cisco switch both send CDP advertisements by default over the data link layer of the shared link that is active. The information revealed in CDP advertisements (including IP addresses, device platform, and IOS versions) presents a security risk. CDP can be disabled on an interface-by-interface basis or disabled globally.

16. 
    ```
    Router(config)# ip route network-address subnet-mask {ip-address | exit-interface}
    ```

17. A recursive route lookup is another search of the routing table to find an exit interface for an outbound packet. A recursive route lookup occurs when the initial route lookup resolves to an IP address for the next hop. Because IOS needs an exit interface, it must look up the exit interface for the next-hop IP address.

18. A static route cannot just be changed. The original route must also be removed from the configuration. Otherwise, both the original route and the new route will be stored in the configuration.

19. Summary and default routes decrease the size of the routing tables. If a router has a large collection of static routes pointing out the same interface, sometimes these routes can be summarized into one routing table entry. Without default routing, every router would need a route to every location in the network.

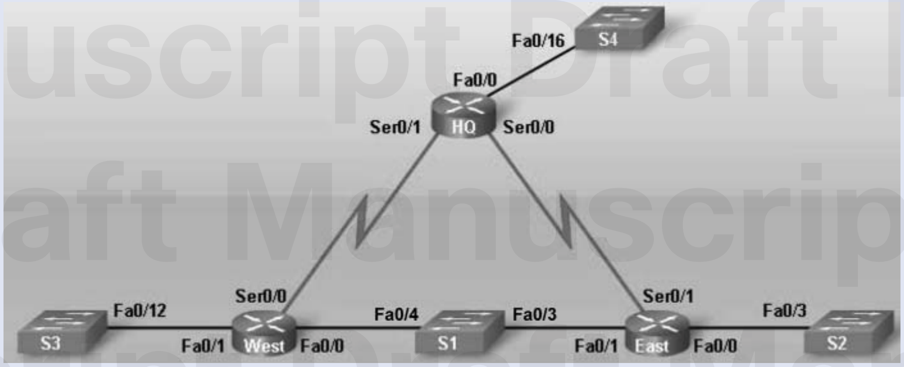
20. **ping**, **traceroute**, **show ip route**, **show ip interface brief**, **show cdp neighbors**

## Challenge Questions and Activities

1. In older computers, only a crossover cable would work between two computers. However, many manufacturers (Dell, for example) are designing the on-board NIC to autodetect what type of device is on the other end of the connection and then internally switch the transmit and receive pins, if necessary. For example, connecting two newer Dell computers directly will work with a straight-through cable. One of the computer switches the 1 and 3 pins to be the receive pair, which creates the same connection as a crossover cable.

2. R2 and R3 are sharing the same IP address on the 192.168.1.0/24 network. When R1 pings R3 at 192.168.1.1, R2 replies, not R3. To see this, the network administrator would have to traceroute to 192.168.1.1. When R3 pings R1, the ping is sourced from the Serial 0/0/1 interface with an IP address 192.168.1.1 as the source address. R1 receives the ping request and replies. However, R2 accepts the ping reply sent to 192.168.1.1 as belonging to R2. Therefore, the ping reply is not routed to R2. To fix the problem, configure R2 with a different IP address from the 192.168.1.0/24 network (192.168.1.2 is used in the chapter example).

3. **Figure A-1** Topology for Challenge Question #3



4. Branch1, Branch2, and Branch3 all have the same default static route:

```
ip route 0.0.0.0 0.0.0.0 s0/0/0
```

RegionA has the following static route configuration:

```
ip route 0.0.0.0 0.0.0.0 serial 0/0/3
ip route 172.16.0.0 255.254.0.0 serial0/0/0
ip route 172.18.0.0 255.254.0.0 serial0/0/1
ip route 172.24.0.0 255.248.0.0 serial0/0/2
```

HQ has the following static route configuration:

```
ip route 0.0.0.0 0.0.0.0 serial 0/0/1
ip route 172.16.0.0 255.240.0.0 serial0/0/0
```

ISP has the following static route configuration:

```
ip route 172.16.0.0 255.240.0.0 serial0/0/0
```