2

CHAPTER

# ADVANCED ROUTER CONFIGURATION I

## Chapter Outline



## Objectives

- Describe the difference between static and dynamic routing protocols
- Describe the difference in distance vector and link state protocols
- Be able to configure a basic setup for static, RIP, and RIPv2 routing protocols
- Understand the relative amount of traffic generated by each protocol
- Understand the purpose of and be able to configure a TFTP sever

## Key Terms

routing protocols
static route
**netstat -r**
route print
loopback
**ip route**
Variable Length Subnet Masking
**show ip route** (**sh ip route**)
routing table code S
routing table code C
gateway of last resort
**show ip route static** (**sh ip route static**)
exit interface
null0 interface
**show running-config** (**sh run**)
**show startup-config** (**sh start**)
**copy run start**
**write memory** (**wr m**)
**traceroute** *destination-ip-address*
datagrams
**tracert** *destination-ip-address*
destination unreachable
load balancing
equal-cost load balancing
floating static route
Dynamic Routing Protocols
prefix length
Administrative Distance (AD)
**path determination**
**metric**
**convergence**
Hop Count
reliability
bandwidth
delay
cost
load
ticks
Distance Vector Protocol
Link State Protocol
RIP
routing loops
advertise
class network address
classful addressing
**show ip protocol** (**sh ip protocol**)
**no auto-summary**
TFTP

**Routing Protocols**
Provide a standardized format for route management.

# INTRODUCTION

This chapter introduces the basic concepts of **routing protocols**. Routing protocols provide a standardized format for route management, including route selection, sharing route status with neighbor routers, and calculating alternative routes if the best path route is down. The focus of this chapter is on the use of routing protocols in a campus network environment (in particular static, RIP, and RIPv2).

Static routing protocols are first presented in Section 2-1. This section includes examples of how to configure static routes and view the routes in a routing table. The material includes a discussion of when and where static protocols are used and when and why it is not advantageous to use a static routing protocol. Section 2-2 provides an overview of the concept of dynamic protocols. Dynamic protocols are divided into two categories: distance vector and link state. Section 2-3 provides examples of configuring the distance vector protocols RIP and RIPv2. Chapter 3, "Advanced Router Configuration II," examines configuring link state protocols. It is important to periodically back up the router configuration files configured for a router. A procedure for doing this is by using a Trivial File Transfer Protocol (TFTP) server, as examined in Section 2-4.

Each routing protocol section in this chapter contains a networking challenge that is included with the Net-Challenge Software. These challenges enable you to verify you know the proper commands used to configure each routing protocol.

## 2-1 CONFIGURING STATIC ROUTING

**Static Route**
A data traffic route that has been manually entered into either a router's or a computer's routing table.

The objective of this section is to demonstrate how data packets are routed in a network using a static routing protocol. A **static route** is an IP address to which data traffic can be forwarded and has been manually entered into either a router's or computer's routing table. A static route is specified in a PC computer in terms of the computer's default gateway, and routers sometimes use a static route when specifying where the network data traffic is to be forwarded. Examples of specifying the static route(s) for a computer are first examined.

The most common static route used in a host computer is the default gateway. The *default gateway* specifies where the data traffic is to be sent when the destination address for the data is not in the same LAN or is unknown. For example, if your PC is on the 10.10.0.0 network and it wants to send data to 100.100.20.1, the data is sent to the default gateway as specified by the TCP/IP setup on your PC. An example of setting the host computer's default gateway is shown in Figure 2-1 for both (a) Windows and (b) Mac OS X. In this example, the default IP address is 10.10.20.250 with a subnet mask of 255.255.255.0 for the computer in LAN A with the IP address of 10.10.20.1.

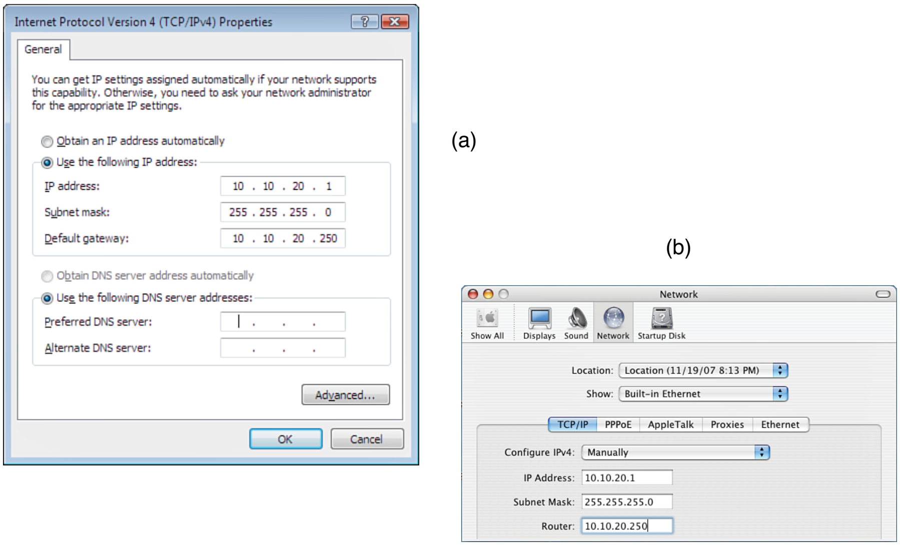



**FIGURE 2-1** Setting the default gateway address or default static route on the host computer (a) PC and (b) Mac OS X

The routing tables for the host PC computer can be obtained by entering the command **netstat -r** at the PC's command prompt and from the Mac OS X terminal screen. An example is shown in Figure 2-2 (a). The command **route print** can also be used to view the active routes from the host PC, as shown in Figure 2-2 (b).

The default route is specified in the routing table by a 0.0.0.0 network address entry with a subnet mask of 0.0.0.0. The 0.0.0.0 indicates that, if the destination address is unknown and the subnet mask is unknown, then send the data packet to the gateway. The gateway address of 10.10.20.250 is the IP address of the FastEthernet port of the router connected to the LAN. The IP address of 10.10.20.1 is the IP address for the host computer's network interface card (NIC).

The network destination of 10.10.20.0 is returned to the computer's NIC at IP address 10.10.20.1. The gateway for the network destination of 10.10.20.1 is 127.0.0.1, which is a **loopback** to the host computer. A loopback means the data is routed directly back to the source. In this case, the source is the computer's NIC. The loopback can be used to check whether the network interface is working; if it is, pinging IP address 127.0.0.1 will generate a reply.

**netstat -r**
The command used to obtain the routing table for a host PC computer.

**route print**
Produces same displayed result as **netstat -r.**

**Loopback**
The data is routed directly back to the source.

```
C:\netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 b0 d0 25 bf 48 ...... 3Com 3C920 Integrated Fast Ethernet Controller
3C905C-TX Compatible) — Packet Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination          Netmask         Gateway      Interface    Metric
            0.0.0.0          0.0.0.0    10.10.20.250    10.10.20.1        20
         10.10.20.0    255.255.255.0      10.10.20.1    10.10.20.1        20
         10.10.20.1  255.255.255.255       127.0.0.1     127.0.0.1        20
     10.255.255.255  255.255.255.255      10.10.20.1    10.10.20.1        20
          127.0.0.0        255.0.0.0       127.0.0.1     127.0.0.1        1
          224.0.0.0        240.0.0.0      10.10.20.1    10.10.20.1        20
    255.255.255.255  255.255.255.255      10.10.20.1    10.10.20.1        1
Default Gateway:        10.10.20.250
===========================================================================
Persistent Routes:
  None
```

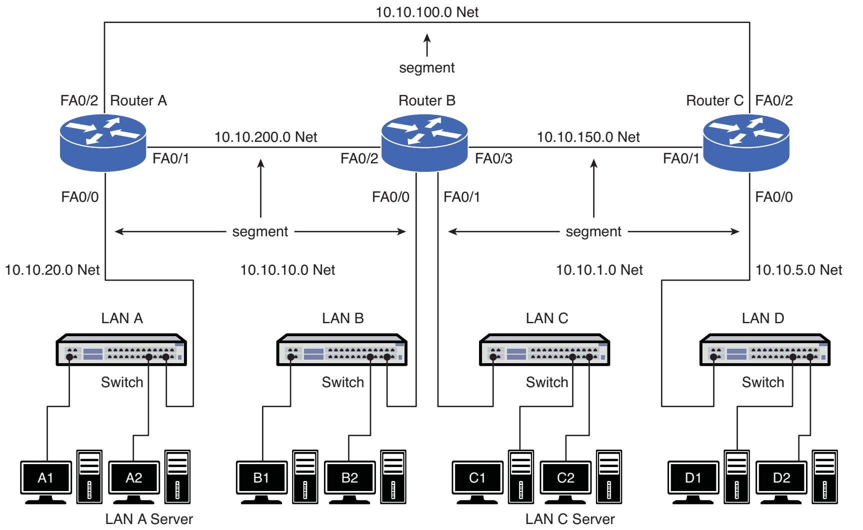
(a)

```
C:\route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 b0 d0 25 bf 48 ...... 3Com 3C920 Integrated Fast Ethernet Controller
3C905C-TX Compatible) — Packet Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination          Netmask         Gateway      Interface    Metric
            0.0.0.0          0.0.0.0    10.10.20.250    10.10.20.1        20
         10.10.20.0    255.255.255.0      10.10.20.1    10.10.20.1        20
         10.10.20.1  255.255.255.255       127.0.0.1     127.0.0.1        20
     10.255.255.255  255.255.255.255      10.10.20.1    10.10.20.1        20
          127.0.0.0        255.0.0.0       127.0.0.1     127.0.0.1        1
          224.0.0.0        240.0.0.0      10.10.20.1    10.10.20.1        20
    255.255.255.255  255.255.255.255      10.10.20.1    10.10.20.1        1
Default Gateway:        10.10.20.250
===========================================================================
Persistent Routes:
  None
```

(b)

**FIGURE 2-2** (a) A host computer's static route listing obtained using the netstat -r command; (b) a host computer's static route listing obtained using the route print command

What about setting static routes for a router in a small campus network? First, let's examine how data packets travel from one LAN to another in the three-router campus network shown in Figure 2-3. Specifically, how is information sent from a host computer in LAN A (10.10.20.0 subnet) to a host computer in LAN B (10.10.10.0 subnet)? The data packets must travel from LAN A to the Router A gateway (FA0/0 interface), from Router A to Router B via the 10.10.200.0 subnet, and then to LAN B via the Router B gateway (FA0/0 interface). This requires that a physical communications link be established between the routers and a routing protocol defined for Routers A and B before data packets can be exchanged. The physical connection from the routers to the LAN computers is typically a CAT6/5e UTP or a fiber connection. The physical connection between the routers is typically fiber.




| Router A Port Addresses (LAN A) | Router B Port Addresses (LAN B) | Router B Port Addresses (LAN C) | Router Port Addresses (LAN D) |
|---|---|---|---|
| FastEthernet 0/0 (Gateway Address) 10.10.20.250 | FastEthernet 0/0 (Gateway Address) 10.10.10.250 | FastEthernet 0/1 (Gateway Address) 10.10.1.250 | FastEthernet 0/0 (Gateway Address) 10.10.5.250 |
| FastEthernet 0/1 10.10.200.1 | FastEthernet 0/2 10.10.200.2 | FastEthernet 0/2 10.10.200.2 | FastEthernet 0/1 10.10.150.2 |
| FastEthernet 0/2 10.10.100.1 | FastEthernet 0/3 10.10.150.1 | FastEthernet 0/3 10.10.150.1 | FastEthernet 0/2 10.10.100.2 |
| **LAN A Computers** | **LAN B Computers** | **LAN C Computers** | **LAN D Computers** |
| Computer A1 10.10.20.1 | Computer B1 10.10.10.1 | Computer C1 10.10.1.1 | Computer D1 10.10.5.1 |
| Computer A2 10.10.20.2 | Computer B2 10.10.10.2 | Computer C2 10.10.1.2 | Computer D2 10.10.5.2 |
| ***Subnet Mask*** ***255.255.255.0*** | ***Subnet Mask*** ***255.255.255.0*** | ***Subnet Mask*** ***255.255.255.0*** | ***Subnet Mask*** ***255.255.255.0*** |

**FIGURE 2-3** A three-router campus network

A simplified network can be used to demonstrate what is required to develop static routes in a multiple-router network. For this example, two routers from the campus network are used. The two routers, Router A and Router B, connect to LANs A and B, as shown in Figure 2-4. This simplified network will be used to describe how data packets travel from LAN A to Router A to Router B to LAN B and what is required to define the static routes.

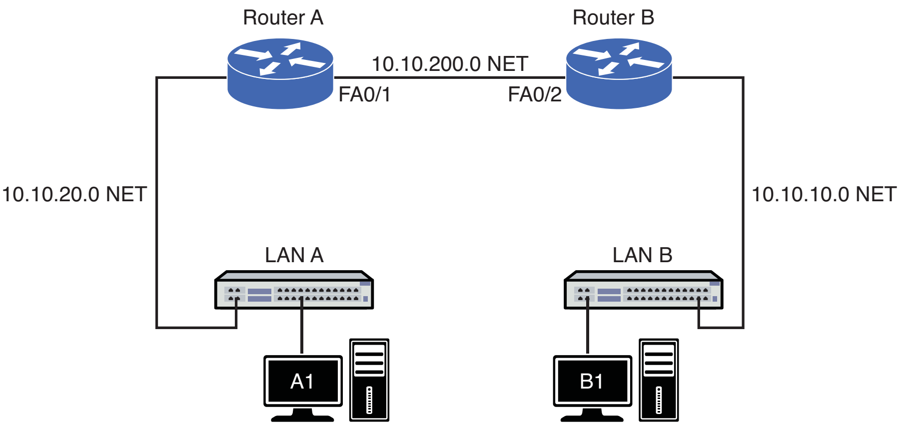



**FIGURE 2-4** A simplified two-router network

The data packets pass through three subnets (indicated by *NET*) when traveling from LAN A to LAN B. The IP subnets for each network are as follows:

- **10.10.20.0 NET**: LAN A
- **10.10.200.0 NET**: Router A connection to Router B
- **10.10.10.0 NET**: LAN B

**ip route**
The router configuration command for manually setting the next hop IP address.

In this network, there are only two routers, with Router A directly connected to Router B. This means that the only route between the routers is via the 10.10.200.0 NET, which is the connection between the FastEthernet interfaces on Routers A and B. The static route information is entered from the router's configure terminal prompt **(config)#** using the **ip route** command. The command structure for **ip route** is

```
Router(config)#ip route destination subnet-mask next-hop
```

where the *destination* is the network's destination IP address (NET), the *subnet mask* is what has been defined for the subnets, and the *next hop* is the IP address of the next router interface in the link. The command for routing the data to the 10.10.10.0 subnet is as follows:

```
RouterA(config)#ip route 10.10.10.0   255.255.255.0    10.10.200.2
```

This results in the following configuration information being entered into Router A:

- Destination subnet IP address: 10.10.10.0
- Subnet mask: 255.255.255.0
- Next hop IP address: 10.10.200.2

The next hop IP address is the IP address of the FastEthernet0/2 interface on RouterB. Now, the router knows how to deliver data packets from host computers in the 10.10.20.0 NET (LAN A) to the destination computers in the 10.10.10.0 NET (LAN B). The next hop IP address is essentially the gateway to LAN B from the Router A's perspective.

**Variable Length Subnet Masking**
Routes can be configured using different subnet masks.

**show ip route (sh ip route)**
The command that displays the routes and the routing address entry into the routing table.

Each static route can use a different subnet mask. This is called **variable length subnet masking**. For example, one static route could have a subnet mask of 255.255.255.0 and another could have a subnet mask of 255.255.255.252.

The routing address entry into the routing table can be verified by entering the command **show ip route (sh ip route)** from the router's # prompt. The following example demonstrates output from **show ip route**:

```
RouterA#show ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
S 10.10.10.0 [1/0] via 10.10.200.2
C 10.10.200.0 is directly connected, FastEthernet1
```

This shows that a static route (S) has been configured for the 10.10.10.0 network via the 10.10.200.2 next hop address.

What about data traffic flow from the 10.10.10.0 NET (LAN B) back to the 10.10.20.0 NET (LAN A)? Once again, the data packets pass through three subnets (indicated by NET) when traveling from LAN B to LAN A. The IP addresses for each subnet are as follows:

- 10.10.10.0 NET: LAN B
- 10.10.200.0 NET: Router B connection to Router A
- 10.10.20.0 NET: LAN A

In this scenario, LAN B connects directly to Router B and the only route to LAN A from Router B is via the 10.10.200.0 NET, which is the connection between Routers B and A. The destination network IP address is 10.10.20.0. The command input to Router B for routing the data to the 10.10.20.0 subnet is as follows:

```
RouterB(config)#ip route 10.10.20.0 255.255.255.0 10.10.200.1
```

The following information is entered into the router:

- Destination subnet IP address: 10.10.20.0
- Subnet mask: 255.255.255.0
- Next hop IP address: 10.10.200.1

The next hop IP address is the IP address of the FastEthernet0/1 port on RouterA. Now, a static route has been configured on Router B to route data packets from host computers in the 10.10.10.0 NET (LAN B) to destination computers in the 10.10.20.0 NET (LAN A). The entries into Router B's routing table can be confirmed by using the command **sh ip route** at the Router# prompt, as shown:

```
RouterB#sh ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
S 10.10.20.0 [1/0] via 10.10.200.1
C 10.10.200.0 is directly connected, FastEthernet0/2
```

The **sh ip route** command lists a table of codes first, followed by the routes. This listing shows a static route (**S**) 10.10.20.0 via 10.10.200.1, which indicates that a static route to the destination 10.10.20.0 subnet can be reached via the next hop of 10.10.200.1. The **C** indicates that the 10.10.200.0 network is directly connected to the FastEthernet02 port.

**routing table code S**
The router code for a static route.

**routing table code C**
The router code for specifying a directly connected network.

This simplified network has only one route; therefore, the entries for the static routes using the **ip route** command are limited but were required for each router. Static routes are sometimes used when configuring the routers for routing in a small network. Static routing is not the best choice, as we will learn, but it can be suitable if the network is small (for example, the two-router network). It can be suitable for situations in which there is only one route to the destination, such as a wide-area network or Internet feed.

What about using static routes in the three-router campus network shown in Figure 2-3? A computer in LAN A (10.10.20.0 NET) sends data to a computer in LAN B (10.10.10.0 NET). This is the same requirement specified in the two-router network example. Once again, a static route must be entered into Router A's routing table telling the router how to forward data to the 10.10.10.0 NET. However, in this example, there are two possible choices for a data packet to travel to the 10.10.10.0 NET from Router A. The IP addresses for the two possible next hops are 10.10.200.2 and 10.10.100.2. The following are the router commands required to configure the routes:

```
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.100.2
```

What about sending information from LAN A to LAN C or to LAN D? This requires four more additional **ip route** entries into the router's routing table, as shown:

```
RouterA(config)#ip route 10.10.1.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.1.0 255.255.255.0 10.10.100.2
RouterA(config)#ip route 10.10.5.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.5.0 255.255.255.0 10.10.100.2
```

But wait, we aren't done. We must enter return static routes for all the LANs back to LAN A, and then enter the static routes for the other three LANs. For troubleshooting purposes, we want to be able to ping all the Ethernet interfaces on the subnets, so we need to add static IP routes to each subnet (NET). For example, the following are the static IP route entries required for defining a route to the 10.10.150.0 NET:

```
RouterA(config)#ip route 10.10.150.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.150.0 255.255.255.0 10.10.100.2
```

This means that many static route entries must be made for the routes in this network to be completely defined. This requires a lot of time and if routes change in the network, new static entries must be made and old static routes must be deleted. The problem with using a static routing protocol in a large network is the amount of maintenance required by the network administrator just to keep the route selections up to date. Assume that the network connection uses five router hops. The entries for the static routes on each router are numerous, and if the routes change, the routing tables in all routers must be manually updated to account for the data path changes.

When static routes are used, the network administrator in essence becomes the routing protocol. In other words, the network administrator is making all the decisions regarding data traffic routing. This requires the administrator to know all network data routes, set up the routes to each subnet, and be constantly aware of any route changes. This is in contrast to dynamic routing protocols that communicate routing information between the routers to determine the best route to use to forward the data packets. The concept of a dynamic routing protocol is introduced in Section 2-2, and in Section 2-3, we examine examples of configuring the dynamic routing protocols RIP and RIPv2.

## Gateway of Last Resort

One of the most important applications for using a static route is for configuring the **gateway of last resort** on a router. The gateway of last resort is the IP address of the router in your network where data packets with unknown routes should be forwarded. The purpose of this is to configure a route for data packets that do not have a destination route configured in the routing table. In this case, a default route can be configured that instructs the router to forward the data packet(s) with an unknown route to another router. The command for doing this is as follows:

**Gateway of Last Resort**
The IP address of the router in your network where data packets with unknown routes should be forwarded.

```
ip route 0.0.0.0   0.0.0.0   next-hop-address
```

If this static route has not been configured, the router will display the following message when the **show ip route** command is entered:

```
Gateway of last resort is not set
```

This means the router does not know how to route a data packet with a destination IP address that differs from the routes stored in the routing table. A critical concept that one must realize about the gateway of last resort is that it must be directly connected to the router. This means it must be on the same network as the router's interfaces, and it must be reachable immediately by the router on the local subnet. This is not only for the routers; it applies to the default gateway of a host computer as well. Remember that the ARP broadcast is the fundamental method of how network devices communicate. If the gateway address is not on the same local subnet as the router, then the ARP broadcast will not work. Therefore, it will not be possible for a computer to forward a network packet outside the network via the gateway of last resort.

## Configuring Static Routes

The following discussion describes how to configure static routes on a Cisco router. The topology being used is the three-router campus network shown previously in Figure 2-3. This demonstration is for configuring the static routes for Router A only.

The first step is to connect to the router via a console or virtual terminal connection. Next, enter the privileged EXEC mode, as shown:

```
Router con0 is now available Press RETURN to get started!
RouterA>en
RouterA#
```

Next, enter the configure terminal mode on the router [RouterA(config)#] using the **configure terminal** (**conf t**) command. Before configuring the static routes, make sure the interfaces are configured. The FastEthernet0/1 interface is configured with the assigned IP address of 10.10.200.1 and a subnet mask of 255.255.255.0, and the FastEthernet0/2 interface is assigned the 10.10.100.1 IP address and a subnet mask of 255.255.255.0. The **no shut** command is used to enable the FastEthernet interfaces.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 10.10.200.1 255.255.255.0
Router(config-if)#no shut
00:19:07: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
up
Router(config)#int fa0/2
Router(config-if)#ip address 10.10.100.1 255.255.255.0
Router(config-if)#no shut
00:21:05: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to
up
```

Notice that the FastEthernet0/1 and FastEthernet0/2 interfaces change state to *up* after the **no shut** command is issued. It is good to verify the interface status using the **show ip interface brief** (**sh ip int brief**) command, as shown:

```
RouterA#sh ip int brief
00:22:18: %SYS-5-CONFIG_I: Configured from console
Interface          IP-Address  OK? Method Status    Protocol
FastEthernet0/1    10.10.200.1 YES manual up        down
FastEthernet0/2    10.10.100.1 YES manual up        down
```

The status for both FastEthernet ports show that they are *up*; however, the line protocol *down* tells us that there is not a physical connection established between the routers. This problem with the "protocol down" is fixed by reestablishing the physical connection between the routers.

The static routes are entered using the **ip route** command after the interfaces are configured. You don't have to enter all routes at once, but all routes must be properly entered for the network to work. The static route command syntax is **ip route** *network-address subnet-mask next-hop-ip-address*. Only the routes to the 10.10.10.0 NET have been listed to shorten the example:

```
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.100.2
```

**show ip route static (sh ip route static)**
Limits the routes displayed to only static.

There are two places to verify whether the static routes are properly configured. First, verify that the routes are in the routing table using either the **show ip route** or the **show ip route static (sh ip route static)** command. Adding the word ***static*** after **show ip route** limits the routes displayed to only *static routes*. An important note is that the routes are displayed using the **show ip route** command *only* if the line protocol is *up*.

```
RouterA#sh ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
S 10.10.10.0 [1/0] via 10.10.200.2
                      [1/0] via 10.10.100.2
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

The command for showing only the static routes is as follows:

```
RouterA#sh ip route static
10.0.0.0/24 is subnetted, 2 subnets
S 10.10.10.0 [1/0] via 10.10.200.2
                     [1/0] via 10.10.100.2
```

**exit interface**
A router interface will be specified as the outgoing interface that is used to forward packets to the destination network.

A static route is added to the routing table when the next hop address is reachable by the router. If the link to the next hop address is down or the destination IP address cannot be reached, then the static route is automatically removed. An alternate way to configure a static route is to specify an **exit interface** instead of a next hop address. In this case, a router interface will be specified as the outgoing interface that is used to forward packets to the destination network. By using the exit interface, the network specified in the static route command will appear as if it is directly connected to the interface. The following example will alter one of the static routes previously configured in the last example to use the exit interface.

```
RouterA(config)#no ip route 10.10.10.0 255.255.255.0 10.10.100.2
RouterA(config)#ip route 10.10.10.0 255.255.255.0 FA0/2

RouterA#sh ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 4 subnets
S 10.10.10.0 [1/0] via 10.10.200.2
                       is directly connected, FastEthernet0/2
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

The **show ip route** command output shows one of the 10.10.10.0 routes has changed to be directly connected via interface FastEthernet0/2, even though the route still remains a type S for static. Because the router assumes the network 10.10.10.0 is now a directly connected interface, every packet destined for an IP address on the 10.10.10.0 network, whether it is valid or not, the router will perform an ARP broadcast on the behalf of the network. This is different than a typical static route, where the only ARP needed is for the next hop IP address. Therefore, using the exit interface option can slow down the data traffic due to the increased number of ARP broadcasts that the router has to perform on the exit interface. The exit interface is used in the point-to-point connection where there is only one possible next hop device and the exit interface must be up in order for the static route to be inserted into the routing table.

The exit interface can be more beneficial when used in conjunction with the next hop address. When using it this way, it is possible to enforce how a static route should properly behave. As previously mentioned, a static route is removed from the routing table when the next hop address is not reachable. What if there is another path to reach the next hop address, but the path is not a desirable one? The network engineer can force the static route to be dependent on an exit interface without putting additional burden on the router.

The **ip route** *network-address subnet-mask exit-interface next-hop-address* command specifies the exit interface through which the next hop address should be found. The static route is installed only if the next hop address is reachable via the specified interface. Also, the router no longer assumes that the destination is directly connected.

**null0 interface**
A virtual bit-bucket interface where every packet gets discarded.

Another static route concept that you should be familiar with is the static route to null0. This is a useful technique for network loop prevention. A **null0 interface** is a virtual bit-bucket interface where every packet gets discarded. As we have learned, a router uses its routing table to route packets. If a route is unknown or it is not in the routing table, the data packet is forwarded to its gateway of last resort.

Assume that Router A is connecting to an ISP router and it is advertising the network 10.10.0.0/16 to the ISP, as illustrated in Figure 2-5. Now, the ISP router is sending Router A a packet with destination 10.10.90.5, which is nowhere to be found in Router A's routing table. Router A will forward the same packet back to the ISP router, which will forward the packet back to Router A again. So, the game of network ping-pong has just begun. This network loop will last until the TTL is expired. However, if the network 10.10.0.0/16 is entered as a null0 route on Router A, then the route exists in the routing table. Therefore, Router A will not forward the packet with destination 10.10.90.5 back to the ISP router.

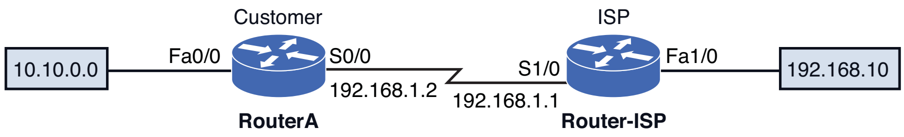



**FIGURE 2-5** An example of a connection from a customer router to the ISP router

The static route null 0 command syntax is

```
ip route network-address subnet-mask null 0
```

as demonstrated in the example that follows:

```
RouterA(config)#ip route 10.10.0.0 255.255.0.0 null 0
RouterA#sh ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is 10.10.200.3 to network 0.0.0.0
10.0.0.0/24 is subnetted, 5 subnets
S 10.10.0.0/16 is directly connected, Null 0
S 10.10.10.0/24 [1/0] via 10.10.200.2
                           is directly connected, FastEthernet0/2
C 10.10.200.0/24 is directly connected, FastEthernet0/1
C 10.10.100.0/24 is directly connected, FastEthernet0/2
```

The other place to check the routing configuration is by examining the router's running-configuration file using the command **show running-config (sh run)**, as shown in the output example that follows. The command displays the current configuration of the router, but it does not show what is currently saved in the router's nonvolatile memory (NVRAM). The command **show startup-config (sh start)** displays the router's configuration saved in NVRAM.

**show running-config (sh run)**
The command that displays the router's running-configuration.

**show startup-config (sh start)**
The command that displays the router's startup-configuration.

```
RouterA#sh run
Using 519 out of 32762 bytes
!
version 12.0
service timestamps debug uptime service timestamps log uptime no
service password-encryption
!
hostname Router
!
!
ip subnet-zero
!
interface FastEthernet0/1
ip address 10.10.200.1 255.255.255.0
 no ip directed-broadcast no keepalive
!
interface FastEthernet0/2
 ip address 10.10.100.1 255.255.255.0
 no ip directed-broadcast no keepalive
!
ip classless
ip route 10.10.10.0 255.255.255.0 10.10.200.2
ip route 10.10.10.0 255.255.255.0 10.10.100.2
```

```
!
line con 0
transport input none line aux 0
line vty 0 4
!
end
```

**copy run start**
The command for copying the running-configuration to the startup-configuration.

**write memory (wr m)**
The command that saves your configuration changes to memory.

**traceroute *destination-ip-address***
Command used to discover the routes the data packets actually take when traveling from the source to the destination.

**Datagrams**
Data packets.

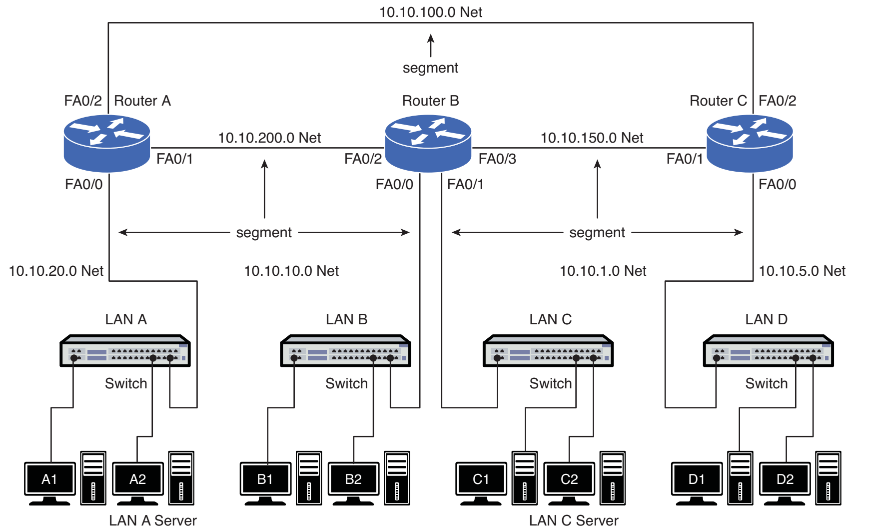
It is important that you save your configuration changes to the router as you go. Save changes to the router configuration by using the **copy running-configuration startup-configuration** command (**copy run start**) or **write memory (wr m)**, as shown:

```
RouterA#copy run start
RouterA#wr m
```

Once your network is set up, you can use the **traceroute *destination-ip-address*** command to discover the routes the data packets (**datagrams**) actually take when traveling from the source to the destination. The command is issued from the Privileged EXEC mode on a router, as shown:

```
R1#traceroute destination-ip-address
```

Referring to the three-router campus network shown in Figure 2-6, the **traceroute** command is issued from RouterA to the FastEthernet 0/0 interface on RouterB. The destination IP address is 10.10.10.250. The result of the **traceroute** is shown next.




| Router A Port Addresses (LAN A) | | Router B Port Addresses (LAN B) | | Router B Port Addresses (LAN C) | | Router Port Addresses (LAN D) | |
|---|---|---|---|---|---|---|---|
| FastEthernet 0/0 (Gateway Address) | 10.10.20.250 | FastEthernet 0/0 (Gateway Address) | 10.10.10.250 | FastEthernet 0/1 (Gateway Address) | 10.10.1.250 | FastEthernet 0/0 (Gateway Address) | 10.10.5.250 |
| FastEthernet 0/1 | 10.10.200.1 | FastEthernet 0/2 | 10.10.200.2 | FastEthernet 0/2 | 10.10.200.2 | FastEthernet 0/1 | 10.10.150.2 |
| FastEthernet 0/2 | 10.10.100.1 | FastEthernet 0/3 | 10.10.150.1 | FastEthernet 0/3 | 10.10.150.1 | FastEthernet 0/2 | 10.10.100.2 |
| **LAN A Computers** | | **LAN B Computers** | | **LAN C Computers** | | **LAN D Computers** | |
| Computer A1 | 10.10.20.1 | Computer B1 | 10.10.10.1 | Computer C1 | 10.10.1.1 | Computer D1 | 10.10.5.1 |
| Computer A2 | 10.10.20.2 | Computer B2 | 10.10.10.2 | Computer C2 | 10.10.1.2 | Computer D2 | 10.10.5.2 |
| ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** |

**FIGURE 2-6** A three-router campus network

```
R1#traceroute 10.10.10.250
Type escape sequence to abort.
Tracing the route to 10.10.10.250
1    10.10.10.250           8msec    8msec    9msec
R1#
```

The result shows that the data packets travel trough one router to arrive at the destination. What happens to the results from a traceroute if the destination is changed to the FastEthernet 0/0 interface on Router C in Figure 2-3? In this case, the data packets must travel through two routers to arrive at the destination, as shown:

```
R1#traceroute 10.10.5.250
Type escape sequence to abort.
Tracing the route to 10.10.10.250
1    10.10.10.250       8msec     8msec     9msec
2    10.10.5.250        8msec    10msec    10msec
R1#
```

Notice that in this case, the datagrams pass through two routers indicated by 1 and 2 and there are three times listed. These three times represent the three datagrams that are sent when the **traceroute** command is issued. The times listed for "1" are the times it took for the datagrams to hit the first router. The datagrams timeout as soon as they arrive at the first router. The times it took for the datagrams to hit the second router are listed in "2".

You can also trace packets from the PC by using the **tracert** ***destination-ip-address*** command. An example is provided. Once again using the three-router campus network shown in Figure 2-6, the **traceroute** command is issued from computer A1 to the FastEthernet 0/0 interface on Router B.

**tracert** ***destination-ip-address***
The command used to trace packets on a PC.

```
C:\>tracert 10.10.10.250
Tracing route to 10.10.10.250 over a maximum of 30 hops:

 1    9ms    5ms    9ms    10.10.20.250
 2   17ms   12ms   14ms    10.10.10.250

Trace complete.
```

In this case, the data packets travel from the PC through the FA0/0 interface on Router A and arrive at the FA0/0 interface on Router B passing through two routers. In some cases, a "time exceeded" error message is displayed indicating that the TTL (Time to Live) for the datagram has been exceeded and the packet has been discarded. In the case that the TTL timer expires before a response is received, a * is displayed. An example is provided for a trace route issued from Router A to the FastEthernert 0/0 interface on Router C for the LAN shown in Figure 2-6. In this case, a datagram expired before being delivered to the destination of 10.10.5.250. Reasons for this happening could be traffic congestion or a momentary loss of connectivity.

```
Router1#traceroute 10.10.5.250

Type escape sequence to abort.
Tracing the route to 34.0.0.4
  1 10.10.200.2    4 msec 4 msec 4 msec
  2 10.10.5.250   16 msec *  16 msec
```

**destination unreachable**
This error is displayed indicating that the destination node received the packet and discarded it because it could not deliver the packet.

**Load Balancing**
Technique used to equally distribute data traffic on a per-packet basis.

**Equal-Cost Load Balancing**
A way to distribute traffic equally among multiple paths.

**Cost Paths**
A cost it takes to route traffic along the path from the source to the destination.

Another situation occurs when a "**destination unreachable**" error is displayed, indicating that the destination node received the packet and discarded it because it could not deliver the packet.

## Load Balancing and Redundancy

This section examines the technique used to configure load balancing on a network that is configured for static routing. **Load balancing** is a technique used to equally distribute data traffic on a per-packet basis. Static routes support **equal-cost load balancing**, which is a way to distribute traffic equally among multiple paths. On Cisco routers, load balancing is automatic if several equal **cost paths** to a destination exist on multiple interfaces. Cost path is used by a routing protocol to calculate the cost along the path to route from the source to the destination. The cost path calculation is different depending on a routing protocol. Some routing protocol use the bandwidth, some use hop count along the path. This concept will be discussed throughout this and the next chapter.

To configure load balancing using static routing, one simply needs to create multiple static routes for more than one interface. As a matter of fact, the static route configuration examples of Router A to 10.10.10.0 network shown throughout this section already demonstrate the load balancing technique. Two independent static routes for the network 10.10.10.0 were configured. The result of the **show ip route** command also confirms that the 10.10.10.0 network can be reached on two paths: one is via 10.10.100.2 and another is via 10.10.200.2.

Not only can these paths be used for load balancing, they can be used to increase the redundancy and reliability of the network. When a network failure happens on one path, the other path will act as a backup path and assume the sole responsibility of routing traffic to the destination. This situation could happen if the next hop address is unreachable, which causes its static route to be removed from the routing table.

**floating static route**
Static backup route.

If load balancing is not required, static routing can offer redundancy via a backup route. A backup route (secondary route) is used when the primary route or preferred route fails. Sometimes, a static backup route is referred to as a **floating static route**. It the route is less preferred than other routes in the routing table, the route does not appear in the routing table until the more preferred route fails. The Administrative Distance (AD) is the number used to determine the preferability of the static routes. The AD ranges from 0–255, where the lower the AD number, the more preferred the route. By default, a static route already has the lower AD of 1. To create a floating route, you must assign a higher AD number. The concept of Administrative Distance (AD) will be discussed more in Section 2-2, "Dynamic Routing Protocols." The following example demonstrates how to assign a floating static route to Router A.

```
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.200.2
RouterA(config)#ip route 10.10.10.0 255.255.255.0 10.10.100.2 250

RouterA#sh ip route
Codes: C connected, S static, I IGRP, R RIP, M mobile, B BGP D EIGRP,
EX EIGRP external, O OSPF, IA OSPF inter area
```

```
N1 OSPF NSSA external type 1, N2 OSPF NSSA external type 2
E1 OSPF external type 1, E2 OSPF external type 2, E EGP
i IS-IS, L1 IS-IS level-1, L2 IS-IS level-2, * candidate default
U per-user static route, o ODR T traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 4 subnets
S 10.10.10.0 [1/0] via 10.10.200.2
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

Notice that an administrative distance of 250 is specified on the route with the next hop address of 10.10.100.2. This forces this route to be less desirable than the route with the next hop address of 10.10.200.2. Remember, a static route already has the lower AD of 1. The output from **show ip route** shows that only the more preferred static route is in the routing table. The floating static route via 10.10.100.2 is no longer in the table.

Table 2-1 provides a summary of the commands used when configuring the static routes.

TABLE 2-1 **Summary of Commands Used to Configure the Static Routing Protocol**

| Command | Use |
|---|---|
| **ip route** | Specifies the destination IP address, the subnet mask, and the next hop IP address |
| **show ip route** | Displays the IP routes listed in the routing table |
| **show ip route static** | Displays only the static IP routes listed in the routing table |
| **show running-configuration** | Displays the router's running-configuration |
| **show startup-configuration** | Displays the router's saved configuration in NVRAM |
| **write memory** | Copies the current router changes to memory (NVRAM) |
| **copy run start** | Copies the current router changes to memory (NVRAM) |
| **traceroute** *destination-IP* | Used on a router to run a trace to a specified destination IP address |
| **tracert** *destination-IP* | Used on a PC to run a trace to a specified destination IP address |

### Networking Challenge—Static Routes

Use the Network Challenge Software included with the text's companion CD-ROM to demonstrate that you can configure static routes for a router. Place the CD-ROM in your computer's drive. Open the Net-Challenge folder and double click the *Net-Challenge V3-2.exe* file. Select the Chapter 7—Static Routes challenge. Use the software to demonstrate that you can complete the following tasks.

This challenge requires you to configure the static routes for Router A:

1. Click the Router A select button and press Return to get started.
2. Configure the default gateway address for computerA1 in LAN A (10.10.20.250). To do so, click the computer A1 icon in LAN A to bring up the TCP/IP Properties menu. Click OK on the menu, and press Enter to see the check.
3. Configure the IP addresses for the FastEthernet0/0 and FastEthernet0/1 ports. *Note:* Click the Router A symbol in the topology to display the IP addresses and subnet mask for the router.
4. Use the **no shut** command to enable both FastEthernet ports.
5. Use the **show ip int brief** command to view the current interface status.
6. Use the **ip route** command to configure two routes to the 10.10.10.0 subnet (NET). *Note:* Click the RouterB and RouterC symbols in the network topology to display the IP addresses for the router interfaces. (Use a 255.255.255.0 subnet mask.)
7. Use the **show ip route** command to view whether the routes are entered into the router's routing table.
8. Use the **show run** command to verify whether the static routes are listed in the router's running-configuration.
9. Use the proper command to set the FA 0/0 for Router A as the exit interface.
10. Use the proper command to incorporate null 0 features to prevent network loops to the 10.10.5.0 network.

## 2-2 DYNAMIC ROUTING PROTOCOLS

The concept of configuring a network using a static routing protocol was presented in this chapter's introduction. It became obvious that the time required for entering and maintaining the static routes was a problem. Therefore, a static routing protocol is of limited use for campus-wide network routing, but is essential when configuring the default route (gateway of last resort) on routers. However, static routes are used in situations such as configuring small networks with a limited number of routes.

**Dynamic Routing Protocols**
The routing table is dynamically updated to account for loss or changes in routes or changes in data traffic.

This section introduces an improvement over static routing through the use of **dynamic routing protocols**. Dynamic routing protocols enable the router's routing tables to be dynamically updated to account for a loss or a change in routes or changes in data traffic. The routers update their routing tables using information obtained from adjacent routers. The following list defines the features of dynamic routing protocols:

- What information is exchanged between routers
- When updated routing information is exchanged
- Steps for reacting to changes in the network
- Criteria for establishing the best route selection

The routing protocol is responsible for managing the exchange of routing information between the routers, and the choice of protocol defines how the routing information is exchanged and used.

A router could be running more than one routing protocol. This is sometimes necessary when a router is connecting to another router with a different routing protocol. A router could be learning about the same particular network from different routing protocols at the same time or the same network could be advertised with multiple paths. These are just some of the complications. Nonetheless, the router will learn network routes from its neighbor and install the best route in its routing table or routing information base (RIB). This will be used to allow the router to make a decision as to which is the best route to forward packets to a particular network. To determine the best route to a destination, a router considers three elements. These are listed in the order used to select the best route:

1. Prefix length
2. Administative Distance
3. Metric

The **prefix length** is the number of bits used to identify the network. The longer the prefix length means the route is more specific. For example, the network 10.10.10.0/24 has a longer prefix length than the network 10.10.0.0/16. Therefore, the network 10.10.10.0/24 is said to be a more specific route. The router will always prefer a more specific route no matter what routing protocol is being used.

**Prefix Length**
The number of bits used to identify the network.

**Administrative Distance (AD)**
A number assigned to a protocol or route to declare its reliability.

If you have the same route to a destination configured with static route and the RIP routing protocol, the preferred route is with static route. This preference is accomplished with a parameter called **Administrative Distance (AD)**. The AD is a number assigned to a protocol or a route to declare its reliability. The lower the AD number, the better the protocol or route. Each routing protocol has a default administrative distance.

A router uses the administrative distance to resolve which routing protocol is chosen when there are conflicts. For example, a router might learn a route to a 10.0.0.0 network using RIP. The same router might also learn of a route to the 10.0.0.0 network using a static route. RIP has an administrative distance of 120 and static has an administrative distance of 1. Static has the lower administrative distance number; therefore, the router will select the static route. Table 2-2 provides a summary of administrative distances for selected routing protocols.

TABLE 2-2 **Administrative Distances and Routing Protocols**

| Protocol | Administrative Distance |
|---|---|
| Connected | 0 |
| Static route | 1 |
| eBGP | 20 |
| EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |

The metric is a numerical parameter that allows a router to choose the best path within a routing protocol. So, the metric can be used to determine the best path when a single routing protocol advertises multiple paths to the same network. A metric is sometime referred to as "distance" or "cost" depending on the routing protocol. A metric is one of the four key issues associated with dynamic routing protocols. The four key issues are **path determination**, **metric**, **convergence**, and **load balancing**. These issues are defined in Table 2-3.

TABLE 2-3 **Four Key Issues in Dynamic Routing Protocols**

| Item | Issue | Purpose |
|---|---|---|
| 1 | Path determination | A procedure in the protocol that is used to determine the best route. |
| 2 | Metric | A numeric measure assigned to routes for ranking the routes best to worst; the smaller the number, the better. |
| 3 | Convergence | This happens when a router obtains a clear view of the routes in a network. The time it takes for the router to obtain a clear view is called the convergence time. |
| 4 | Load balancing | A procedure in the protocol that enables routers to use any of the multiple data paths available from multiple routers to reach the destination. |

Examples of route metrics are as follows:

- **Hop count:** The number of routers the data packet must pass through to reach the destination network.
- **Reliability:** A measure of the reliability of the link, typically in terms of the amount of errors.
- **Bandwidth:** Having to do with the data capacity of the networking link; a FastEthernet 100 Mbps link has greater data capacity than a 10 Mbps Ethernet link.

- **Delay:** The time it takes for a data packet to travel from source to destination.
- **Cost:** A value typically assigned by the network administrator that takes into account bandwidth and expense.
- **Load:** Having to do with the network activity on a link or router.
- **Ticks:** The measured delay time in terms of clock ticks, where each tick is approximately 55 milliseconds (1/18 second).

There are two types of dynamic routing protocols: distance vector and link state. These protocols are briefly introduced in this section. The procedures for configuring a router to use a dynamic routing protocol is examined in Section 2-3. The procedures for configuring link state protocols is discussed in Chapter 3.

## Distance Vector Protocols

A **distance vector protocol** is a routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router. When the neighboring router receives the table, it assigns a distance vector number to each route. The distance vector number is typically specified by some metric, such as hop count.

**Distance Vector Protocol**
A routing algorithm that periodically sends the entire routing table to its neighboring or adjacent router.

In a distance vector protocol, the router first determines its neighbors or adjacent routers. All the connected routes will have a distance or hop count of 0, as illustrated in Figure 2-7. Routers use the hop count metric to determine the best route to forward a data packet. Figure 2-8 provides an example of determining the hop count to a destination subnet.

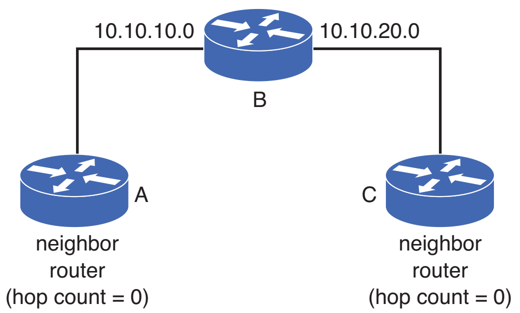
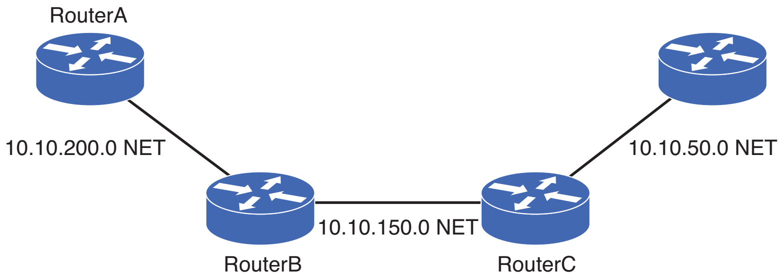



**FIGURE 2-7** An example of router neighbors (hop count = 0)

Table 2-4 lists the hop count from Router A to the 10.10.200.0, 10.10.150.0, and 10.10.50.0 subnets.

TABLE 2-4 **Hop Counts from Router A to Subnets**

| From | To | Hop Count |
|---|---|---|
| Router A | 10.10.200.0 | 0 |
| Router A | 10.10.150.0 | 1 |
| Router A | 10.10.50.0 | 2 |




Hop Count

| From: | To: | Hop Count |
|---|---|---|
| Router A | 10.10.200.0 | 0 |
| Router A | 10.10.150.0 | 1 |
| Router A | 10.10.50.0 | 2 |

**FIGURE 2-8** An example of determining the router hops

In a distance vector protocol, each router determines its neighbors, builds its list of neighboring routers, and sends its routing table to its neighbors. The neighboring routers update their routing table based on the received information. When complete, each router's routing table provides a list of known routes within the network.

## Link State Protocols

**Link State Protocol**
Establishes a relationship with a neighboring router and uses route advertisements to build routing tables.

**Link state protocols** establish a relationship with a neighboring router. The routers exchange link state advertisements to update neighbors regarding route status. The link state advertisements are sent only if there is a change or loss in the network routes and the link state protocols converge to route selection quickly. This is a distinct advantage over distance vector protocols that exchange updated routing tables at fixed time intervals and are slow to converge. In fact, link state routing protocols are replacing distance vector protocols in most computer networks. Link state protocols are also called *shortest-path first protocols*, based on the algorithm developed by E. W. Dijkstra. An example of a link state protocol is Open Shortest Path First (OSPF), examined in more detail in Chapter 3. Link state protocols use Hello packets to verify that communication is still established with neighbor routers. The key issues of link state protocols are as follows:

- Finds neighbors/adjacencies
- Uses route advertisements to build routing table
- Sends Hello packets
- Sends updates when routing changes

## 2-3 CONFIGURING RIPV2

Routing Information Protocol (**RIP**) is a dynamic routing protocol, meaning the routers periodically exchange routes. RIP is classified as a distance vector protocol using router hop count as the metric. RIP permits a maximum of 15 hops to prevent **routing loops**. Routing loops occur when a router forwards packets back to the router that sent them, as graphically shown in Figure 2-9. RIP and other distance vector routing protocols send the entire routing table to neighbor routers at regular time intervals. Sometimes, the routing tables can be quite large and the transfer can consume network bandwidth. This is of great concern in networks with limited bandwidth because the periodic exchange can lead to slowdowns in data traffic. The default time interval for RIP for exchanging routing tables is 30 seconds. This results in slow route convergence, and if there are multiple routers sharing RIP routes, there will be even longer convergence time.

**RIP**
Routing Information Protocol.

**Routing Loop**
Data is forwarded back to the router that sent the data packets.

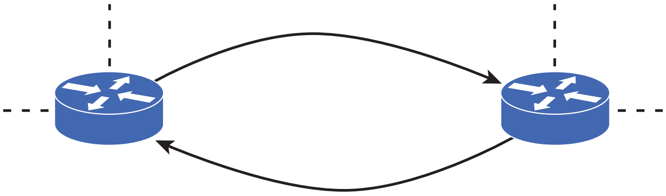


**FIGURE 2-9** An example of data packet travel in a routing loop. Note that the packets never leave the routes between the two routers.

The RIP routing protocol is enabled on the router by entering the command **router rip** at the Router(config)# prompt. Next, network statements are required to declare what networks will be advertised by the RIP routing protocol. To **advertise** the network means the routing table containing the network is shared with its neighbors. The **network** command requires the use of a **class network address** (Class A, Class B, Class C) after the **network** command. This is called **classful addressing**. A class network address or classful address is the network portion of the address for the particular class of the network. For example, LAN A in our campus network is on the 10.10.20.0 NET, as shown in Figure 2-10. This is a class A network, and the network portion of the address is 10.0.0.0. The structure of the network command is **network** *[network-address]*, where the *network address* is the network where RIP is to be advertised; therefore, the command in RIP will be **network 10.0.0.0**.

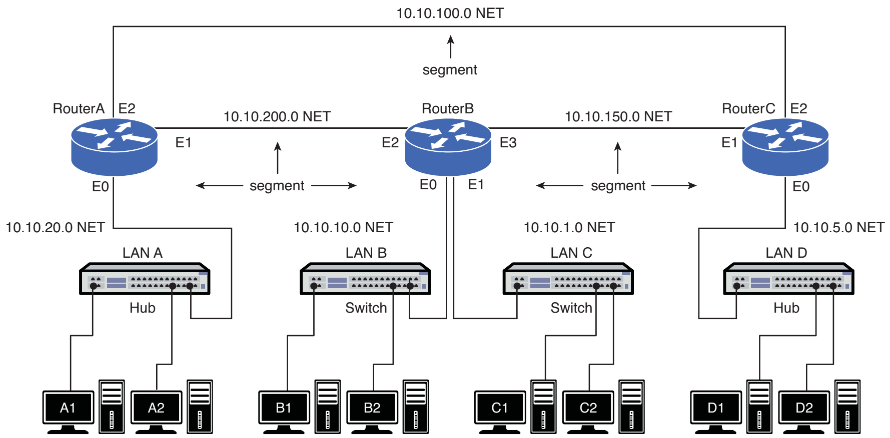
**Advertise**
The sharing of route information.

**Class Network Address**
The network portion of the IP address based on the class of the network.

**Classful Addressing**
The network portion of a particular network address.

The following discussion explains how to initialize RIP and how to set the networks attached to the router for RIP routing. After these commands are entered, any interfaces that are part of the 10.0.0.0 network will run the RIP routing protocol. Note that subnets or subnet masks are not specified in the RIP network command because the class network address is used and all IP addresses in the network (for example, 10.0.0.0) are enabled to use RIP.

```
Router(config)#router rip
Router(config-router)#network 10.0.0.0
```




| RouterA Port Addresses (LAN A) | | RouterB Port Addresses (LAN B) | | RouterB Port Addresses (LAN C) | | RouterC Port Addresses (LAN D) | |
|---|---|---|---|---|---|---|---|
| Ethernet 0 (Gateway Address) | 10.10.20.250 | Ethernet 0 (Gateway Address) | 10.10.10.250 | Ethernet 1 (Gateway Address) | 10.10.1.250 | Ethernet 0 (Gateway Address) | 10.10.5.250 |
| Ethernet 1 | 10.10.200.1 | Ethernet 2 | 10.10.200.2 | Ethernet 2 | 10.10.200.2 | Ethernet 1 | 10.10.150.2 |
| Ethernet 2 | 10.10.100.1 | Ethernet 3 | 10.10.150.1 | Ethernet 3 | 10.10.150.1 | Ethernet 2 | 10.10.100.2 |
| **LAN A Computers** | | **LAN B Computers** | | **LAN C Computers** | | **LAN D Computers** | |
| Computer A1 | 10.10.20.1 | Computer B1 | 10.10.10.1 | Computer C1 | 10.10.1.1 | Computer D1 | 10.10.5.1 |
| Computer A2 | 10.10.20.2 | Computer B2 | 10.10.10.2 | Computer C2 | 10.10.1.2 | Computer D2 | 10.10.5.2 |
| ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** | ***Subnet Mask*** | ***255.255.255.0*** |

**FIGURE 2-10** LAN A in the campus network

RIP can be used only in *contiguous* networks, meaning the networks and routes must have the same class network address. This means the router addresses for the network connecting the routers must be the same class as the LAN connected to the router. This is shown in Figure 2-11 (a) and (b). LAN A and B have a 10.#.#.# address (also called a *10 network* address). The network address connecting the two routers must also be a "10" network address. The IP address for the network connecting the two routers in Figure 2-11 (a) is 10.10.200.0. This is a "10" network address. The network shown in Figure 2-11 (b) uses the IP address of 192.168.10.0 for the network connecting the two routers. An address of 192.168.10.0 is in the 192.168.10.0 network. This is not part of the 10.0.0.0 network; therefore, the 192.168.10.0 address is not suitable for use in RIP.

RIP is a relatively simple routing protocol to configure. However, RIP is good only for very small networks that have a limited staff size for managing the network and is not suited for networks that need fast convergence. RIP is a standard protocol, not a proprietary protocol, meaning that the use of the protocol is not limited to certain equipment manufacturers.

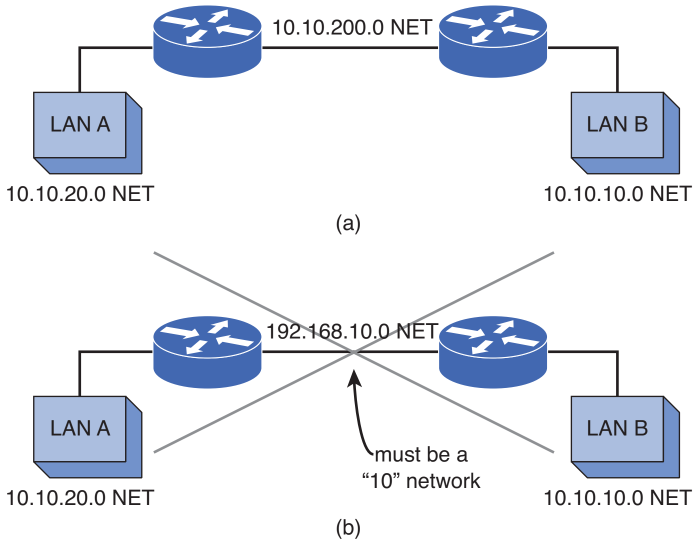



**FIGURE 2-11** An example of (a) a contiguous network and (b) a discontiguous network

## Configuring Routes with RIP

The first step in configuring the router for RIP is to set up the interfaces. This includes assigning an IP address and a subnet mask to the interface using the command **ip address** *A.B.C.D. subnet-mask*. Next, the interface is enabled using the **no shut** command. The following are the steps for configuring the FastEthernet0/1 interface on Router A in the campus network shown previously in Figure 2-10:

```
Router con0 is now available
Press RETURN to get started.
RouterA>en
Password:
RouterA# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 10.10.200.1 255.255.255.0
Router(config-if)#no shut
00:59:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1, changed state to up
```

Next, enter the router's configuration mode [Router(config)#] and input the command **router rip** to use the RIP routing protocol. The next step is to specify the network that uses RIP for routing. These two steps are shown here:

```
Router(config)#router rip
Router(config-router)#network 10.0.0.0
```

The command **router rip** enables the RIP routing protocol, and the command **network 10.0.0.0** instructs the router to use RIP on the "10" network. Remember, RIP requires the use of a class network address (for example, 10.0.0.0). Notice that the **router rip** command places the router in the (config-router) mode, as shown in the prompt. This indicates that the router is in the state for specifying the networks using RIP.

It's a good idea to periodically check that the router interfaces are properly configured. The command **show ip interface brief** (**sh ip int brief**) is used to check the interfaces. This is an important troubleshooting command when looking for reasons why the router is not working. Use this command to check to see if the IP address has been assigned to the interface and to check the status and protocol settings. In this case, the FastEthernet0/1 port has been assigned the IP address 10.10.200.1, the status is *up*, and the protocol is *up*. The FastEthernet 0/0 and 0/2 ports for RouterA have not been configured, as shown, and the status is administratively down and the protocol is down:

```
Router#sh ip int brief
Interface         IP-Address    OK? Method   Status
-Protocol
FastEthernet0/0   unassigned    YES  manual   administratively down   down
FastEthernet0/1   10.10.200.1   YES  manual   up                      up
FastEthernet0/2   unassigned    YES  unset    administratively down   down
```

**show ip protocol (sh ip protocol)**
Displays the routing protocol running on the router.

The command **show ip protocol (sh ip protocol)** is used to display the routing protocols running on the router, as shown. This command will display protocol information only after the routing protocol has been enabled and the network addresses are specified. Notice that there are no values specified for the FastEthernet0/0 and FastEthernet0/2 ports. Neither of these interfaces has been configured. The **show ip protocol** command also shows that router updates are being sent every 30 seconds and indicates that the next update is due in 5 seconds.

```
RouterA#sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is Incoming update
filter list for all interfaces is Redistributing: rip
Default version control: send version 1, receive any version
Interface          Send Recv Key-chain
FastEthernet0/0     0     0     0
FastEthernet0/1     1     1     2
FastEthernet0/2     0     0     0
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.10.200.1 120 00:00:14
Distance: (default is 120)
```

The routes configured for the router can be displayed using the **show ip route** (**sh ip route**) command, as shown. In this example, the FastEthernet0/0 and FastEthernet0/2 ports for Router A have been configured and are displayed:

```
Router#sh ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
I – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * candidate default
U – per-user static route, o – ODR T – traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

This shows the connected (C) networks but RIP (R) is not enabled for any networks. Why? At this point, RIP has been enabled only on Router A in the campus network. Router B and Router C also need to have RIP enabled. Use the commands **router rip** and **network** to enable RIP on Router B. RIP was next configured on Router B and the updated routing table for Router A is provided:

```
Router#sh ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B –
BGP D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
I – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * candidate default
U – per-user static route, o – ODR T – traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.1.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

Now, the networks (10.10.10.0 and 10.10.1.0) from LAN B and LAN C, respectively, are shown in this table. Router A learns these network routes via its FastEthernet0/1 interface from the IP address 10.10.200.2, which is the FastEthernet0/2 interface of Router B.

Verify the settings in the running-configuration file by using the **sh run** command, as outlined in Table 2-5. Recall that this is the abbreviated command for **show running-configuration**. The configuration list should show that the interfaces have been assigned an IP address and that RIP has been configured.

TABLE 2-5 **sh run Command Output**

| CLI | Comments |
|---|---|
| RouterA#**sh run** | ! 1. sh run command |
| Building configuration | ! 2. assembling the data file |
| ! | ! 3. ! is used for spaces or comments |
| Current configuration: | |
| ! | |
| version 12.0 | ! 6. displays the Cisco IOS version |
| service timestamps debug uptime | |
| service timestamps log uptime | |
| no service password-encryption | ! 9. the enable (line 14) and vty (line 42) passwords appear as plaintext |
| ! | |
| hostname RouterA | ! 11. the name of the router |
| ! | |
| enable secret 5 $1$6EWO$kWlakDz89zac.koh/pyG4. | ! 13. the encrypted enable secret |
| enable password Salsa | ! 14. the enable password |
| ! | |
| ip subnet-zero | ! 16. enables subnet zero routing |
| ! | |
| Interface FastEthernet0/0 | ! 18. FastEthernet0/0 settings |
| ip address 10.10.20.0 255.255.255.0 | |
| no ip directed-broadcast | |
| ! | |
| interface FastEthernet0/1 | ! 22. FastEthernet0/1 settings |
| ip address 10.10.200.1 255.255.255.0 | |
| no ip directed-broadcast | |
| no mop enabled | |
| ! | |
| interface FastEthernet0/2 | ! 27. FastEthernet0/2 settings |
| ip address 10.10.100.1 255.255.255.0 | |
| no ip directed-broadcast no mop enabled | |
| ! | |
| router rip | ! 33. enable RIP |

| CLI | Comments |
|---|---|
| network 10.0.0.0 | ! 34. specify a network class address |
| ! | |
| ip classless | |
| ! | |
| line con 0 | |
| transport input none | |
| line aux 0 | |
| line vty 0 4 | ! 41. virtual terminal settings for telnet |
| login | ! 42. This command enables login |
| password ConCarne | ! 43. telnet password<br>login |
| ! | |
| end | |

Lines 18, 22, and 27 list the assigned IP addresses for the interface. Lines 33 and 34 show that RIP has been configured for the router. The **sh run** command displays the router's running configuration. The **copy run start** command must be entered to save the changes to NVRAM.

RIP is among the oldest protocols; it was introduced in 1988. It has a number of limitations that makes it inefficient in handling a lot of newer IP features. Some of its limitations are

- RIP is a classful routing-only protocol. It, therefore, does not support Variable Length Subnet Mask (VLSM) and Classless Inter-Domain Routing (CIDR). This prevents it from being the routing protocol of choice when having to deal with different sized subnets in a network.
- RIP does not support router authentication, which can be exploited as vulnerability.
- RIP has a hop count limit of 15, which means a destination that is 15 hops away is considered to be unreachable.
- RIP uses hop count as a metric. What this means is that RIP determines the best route by counting the number of hops to reach the destination. A lower hop count wins over the higher hop count. This is a disadvantage when dealing with different bandwidth between hops. RIP does not take into consideration whether the higher hop count route might have higher bandwidth. Therefore, the lower bandwidth route could be taken.

The following example demonstrates one of RIP's limitations. In this example, the subnet mask of the LAN C network will be changed to 255.255.255.128. To accomplish this task, the FastEthernet 0/1 interface for Router B needs to be reconfigured as follows:

```
RouterB# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip address 10.10.1.250 255.255.255.128
```

Because RIP does not support VLSM, what will happen to the newly reconfigured subnet? The answer is the network 10.10.1.0 will not be advertised by RIP. The route for network 10.10.1.0 is not displayed in the routing table of Router A, as shown with the command **sh ip route**:

```
RouterA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.200.0 is directly connected, FastEthernet0/1
C 10.10.100.0 is directly connected, FastEthernet0/2
```

To address some of RIP's limitations, the second version of RIP was developed as RIP version 2 (RIPv2) in 1993. The original version of RIP is then called RIP version 1 (RIPv1). RIPv2 is not quite a redesign of RIPv1; it could be thought more of an enhanced version of RIP version 1. RIPv2 works basically just like RIPv1. It introduced new features, such as support for VLSM and CIDR, router authentication, next hop specification, route tag, and the use of multicasting. However, it still cannot resolve some of the limitations found in RIPv1, which are hop count and metric decisions.

## Configuring Routes with RIP Version 2

The steps needed to configure RIPv2 are almost exactly the same as configuring RIPv1. The only difference is the version must be specified in the **router rip** configuration. Let's take the RIP configuration that was done earlier in this section, then enter the router's configuration mode [**Router(config)#**], and input the command **router rip** to use the RIP routing protocol. The next step is to configure RIPv2 to be used with the command **version 2.** Without specifying the version, RIPv1 will be used by default. These two steps are shown here:

```
RouterA(config)#router rip
RouterA(config-router)#version 2
```

To verify that RIPv2 is the routing protocol, the command **sh ip protocol** is used. Notice the line **Default version control**. This confirms that RIP version 2 is being sent as well as being received by the RouterA.

```
RouterA#sh ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 17 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive version 2
Interface             Send  Recv  Triggered RIP  Key-chain
FastEthernet0/0       2     2
FastEthernet0/1       2     2
FastEthernet0/2       2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway         Distance      Last Update
10.10.200.2          120      00:00:20
Distance: (default is 120)
```

Even though, RIPv2 is a classless routing protocol, it still summarizes routes at the class network boundaries by default. Therefore, it may appear as if RIPv2 only advertises classful networks, like RIPv1. To disable the auto summarization function, the command **no auto-summary** is used. This command instructs the router not to summarize the network routes. The **no auto-summary** command alters this behavior by enabling RIP to advertise the actual networks, not the classful summary. The **no auto-summary** command should be used when a classful network is divided and parts of the same classful network exist in different parts of the network topology.

**no auto-summary**
This instructs the router not to summarize the network routes.

```
RouterA(config)#router rip
RouterA(config-router)#no auto-summary
```

Now, let's reexamine the previous demonstration of RIPv1, where the subnet mask for the network 10.10.1.0 was changed to 255.255.255.128. This resulted in the network no longer showing up in the routing table. The same command **version 2** needs to be applied under **router rip** on Router B. With the RIP version 2 enabled, the command **sh ip route** is reissued on Router A. This time, the routing table shows that the LAN C network 10.10.1.128/25 is being displayed, even though it has a different sized subnet than the others:

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * candidate default
U - per-user static route, o - ODR T - traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.10.0 [120/1] via 10.10.200.2, 00:00:05, FastEthernet0/1
C 10.10.20.0 is directly connected, FastEthernet0/0
R 10.10.1.128/25 [120/1] via 10.10.200.2, 00:00:15, FastEthernet0/1
C 10.10.200.0 is directly connected, FastEthernet0/2
C 10.10.100.0 is directly connected, FastEthernet0/1
```

## Networking Challenge—RIP

Use the router simulator software included with the text's companion CD-ROM to demonstrate that you can configure RIP for Router A in the campus LAN. (*Note:* The campus LAN is shown in Figure 2-8 and is displayed on the computer screen if the topology button is selected.) Place the CD-ROM in your computer's drive. Open the *Net-Challenge* folder, and click NetChallenge V3-2.exe. When the software is running, click the Select Router Challenge button to open a Select Router Challenge drop-down menu. Select Chapter 2—RIPv2. This opens a checkbox that can be used to verify that you have completed all the tasks:

1. Enter the privileged EXEC mode on the router.
2. Enter the router configuration mode: Router(config).
3. Configure the FastEthernet0/0 interface with the following:

   IP address: 10.10.20.250

   Subnet mask: 255.255.255.0
4. Enable the FA0/0 interface.
5. Configure the FastEthernet0/1 interface with the following:

   IP address: 10.10.200.1

   Subnet mask: 255.255.255.0
6. Enable the FA0/1 interface.
7. Configure the FastEthernet0/2 interface with the following:

   IP address: 10.10.100.1

   Subnet mask: 255.255.255.0
8. Enable the FA0/2 interface.
9. Enable RIP V2.
10. Use the **network** command to specify the class network address to be used by RIP (10.0.0.0).
11. Use the **sh ip int brief** command to check the interface status.
12. Use the **sh ip protocol** command to see whether RIP is running. (*Note:* This requires that Steps 9 and 10 are complete or the response will be "no protocol.")

13. Use the **show ip route** command to verify whether the three FastEthernet ports are connected to the router.
14. Display the contents of the running-configuration file. Verify that RIP is enabled and the proper network address is specified.
15. Copy the router's running-configuration to the startup-configuration.
16. Display the contents of the startup-configuration.

## 2-4 TFTP—TRIVIAL FILE TRANSFER PROTOCOL

Trivial File Transfer Protocol (**TFTP**) is a simple File Transfer Protocol often used with routers and switches to save and reload the configuration files to and from a remote server. The files are saved in case of equipment failure, for rebooting, or for upgrading or archiving the configuration files. It is not uncommon for the configuration files to be backed up daily. The backup is typically done automatically. Changes to router and switch configuration files can occur on a daily basis, and an automatic or regularly scheduled backup is a safe way to ensure the configuration files are archived. Isn't it true that the configuration files can be saved to NVRAM? The answer is yes, but if there is a complete equipment failure, the current router or switch configuration will be lost. Saving the configuration files to another machine is a safer way to prevent loss. The TFTP server is also used for updating and saving the Internetwork Operating System (IOS) files stored in flash. Examples of how to save and reload files stored on the TFTP server are demonstrated later in this section.

**TFTP**
Trivial File Transfer Protocol.

TFTP uses port 69 to establish the network connection and the User Datagram Protocol (UDP) to transport the files. TFTP has no authentication or encryption capabilities and is not a secure transfer; therefore, it is recommended that file transfers should be limited to private networks or a secure TFTP version should be used.

### Configuring TFTP

Before you can save the router or switch configuration files, you must install the TFTP server software on your computer. Many freeware and shareware TFTP software packages are available on the Internet. The available software can be found by searching for "tftp server" using your Internet search engine. (Note: You must have the TFTP software running on your computer for the file transfer to work). Newer versions of the router and switch IOS now support FTP in addition to TFTP for the file transfer. The advantage of FTP is that a secure file transfer can be established using, for example, SSH File Transfer Protocol (SFTP), while TFTP is not secure. Additionally, FTP overcomes the 16-megabyte file transfer limit of some IOS versions. FTP file transfer sizes are not limited.

When you first set up the router or switch, you must make sure it is on the same subnet as the TFTP server because you don't have routing set up yet; therefore, the destination IPs for the router/switch and the TFTP server must be on the same subnet. Figure 2-12 provides an example of this. The IP address for Router C has been configured to 192.168.10.1/28. The TFTP server software has been installed on the computer, D2 and the IP address for computer D2 has been configured to 192.168.10.5/28. This places Router C and computer D2 (TFTP server) on the same subnet in the 192.168.10.0 network. Also note that both Router C and computer D2 are connected to the same switch.

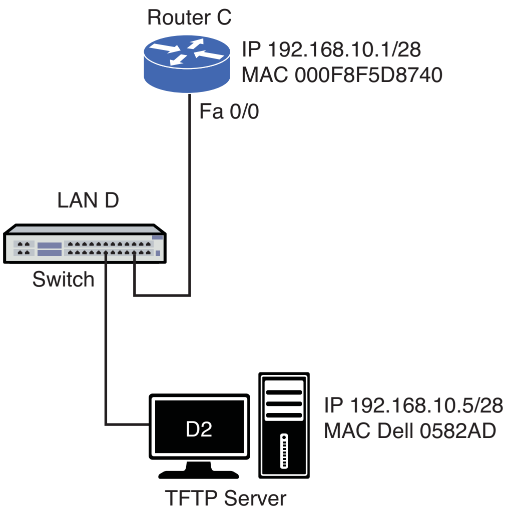



**FIGURE 2-12** An example of placing the router and the TFTP server on the same network

The following are the basic commands used to save and load files to and from the TFTP server. (Abbreviated commands that are recognized by the Net-Challenge software are provided in brackets [ ].) Your first requirement is that you place the router in the privileged EXEC mode, as shown:

1. Enter the enable mode on your router.

```
RouterC>enable
Password:
```

The router's running-configuration file can be reloaded using the command demonstrated in the next step.

2. Save to the TFTP server.

```
RouterC#copy running-config tftp [copy run tftp]
Address or name of remote host []?192.168.10.5
Destination filename [running-config]? <enter the filename to be
saved>
!!
872 bytes copied in 5.176 secs (174 bytes/sec)
```

The router's running-configuration file stored on the TFTP server can be re-loaded using the command demonstrated in the next step.

3. Load from the TFTP server.

```
RouterC#copy tftp running-config [copy tftp run]
Address or name of remote host [  ]? 192.168.10.5
Source filename [  ]? <enter the saved file name>
Destination filename [running-config]?
Accessing tftp://192.168.10.5/network-name...
Loading network-name from 192.168.10.5 (via Ethernet0): !
[OK - 872/1024 bytes]

872 bytes copied in 4.400 secs (218 bytes/sec)
router#
```

Figures 2-13 to 2-15 are captured data files of the TFTP write process using a network protocol analyzer. Figure 2-13 shows the capture for packet 2. The source is the router with an IP address of 192.168.10.1 and the destination is the TFTP server with an IP address of 192.168.10.5. The middle of Figure 2-13 shows that the User Datagram Protocol (UDP) is being used with a source port of 56401 and a destination port 69 (the Trivial File Transfer port). The bottom of Figure 2-13 shows that a write request has been requested. The filename is config, which is the destination filename. The data is being transferred in the octet mode (also called the binary image transfer mode). In this mode, the data is transferred in one-byte units.

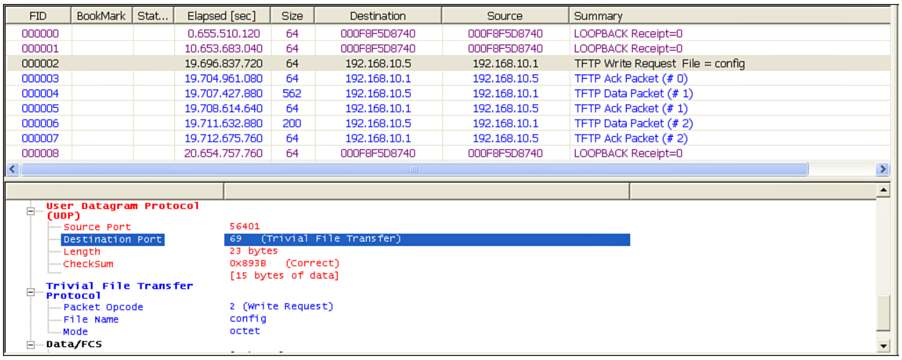



**FIGURE 2-13** A TFTP write request to port 69

Figure 2-14 (packet 3) shows that the TFTP server computer at source port (SP) 1102 replies back to the router (destination port DP 56401). Note that the TFTP server is now using port 1102. Port 69 is used initially to establish the TFTP connection, but the server will select an available port for the data transfer.

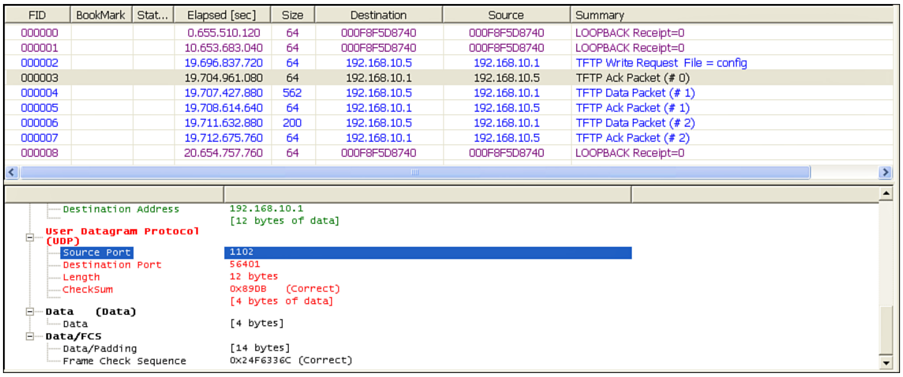



**FIGURE 2-14** A TFTP write request—port assignments

The beginning of the data transfer is shown in Figure 2-15 in packet 4 (FID 000004). The source port is 56401 (router) and the destination port is 1102 (TFTP server). The packet size of the initial data transfer is 562 bytes. The actual text of the data transfer is displayed at the bottom of Figure 2-15. Notice that the data transfer text is readable, which introduces security issues if the configuration data is being transferred over a network.

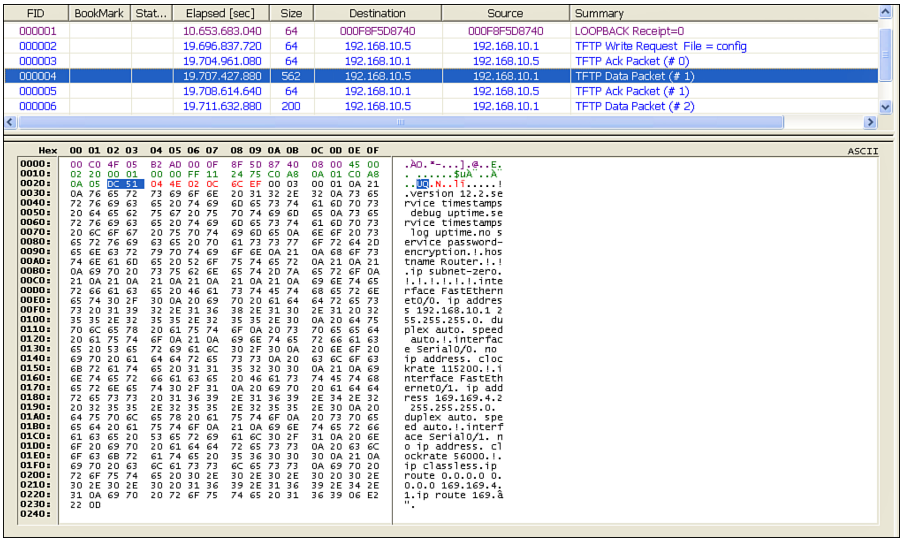



**FIGURE 2-15** A TFTP write request—data transfer

# SUMMARY

This chapter presented examples of configuring static and the RIP/RIPv2 routing protocols. The network challenge exercises provided the opportunity for the student to test her or his configuration skill prior to actually configuring a real router. The student should also have gained an understanding of advanced routing configuration concepts, such as load balancing and redundancy. Additionally, this chapter introduced the steps for configuring a TFTP server.

# QUESTIONS AND PROBLEMS

### Section 2-1

1. What is a routing table?
2. What is the most common static route used in a host computer?
3. What command is used to view a PC computer's routing table?
4. What is meant by a 0.0.0.0 network address entry with a subnet mask of 0.0.0.0 in a PC's routing table?
5. What is the 127.0.0.1 IP address, and what is it used for?
6. What is the router command to configure a static route from LAN A to LAN B for the network shown in Figure 2-16?

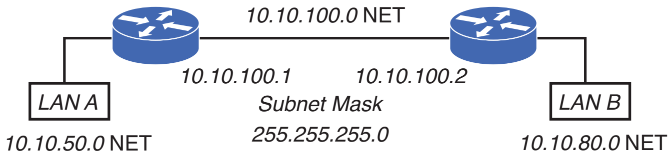



**FIGURE 2-16** The network for problem 6

7. What is the difference in a router's running-configuration and startup-configuration?
8. What is the router command that is used to view the routes entered into the router's routing table?
9. What is the router command that is used to configure a static route for a router?
10. List two static routes to route data from LAN A to LAN C. The network is shown in Figure 2-17. Assume a subnet mask of 255.255.255.0.

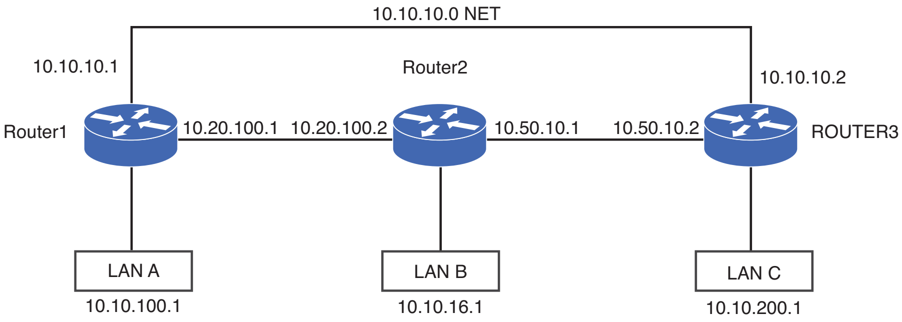



**FIGURE 2-17** The network for problems 10 through 13

11. List two static routes to route data from LAN B to LAN C in Figure 2-17. Assume a subnet mask of 255.255.255.0.

12. Which of the following are suitable subnet masks for use in configuring static routes for the network shown in Figure 2-17?

    a. 255.255.0.0.

    b. 255.0.0.0.

    c. 255.255.255.224.

    d. All of these answers are correct.

    e. None of these answers are correct.

13. A static route is configured to route data from LAN A to LAN B on Router 1 in Figure 2-17. Which of the following are appropriate static routes to achieve this goal?

    a. ip route 10.10.16.0 255.255.255.255 10.20.100.2

    b. ip route 10.10.16.0 255.255.255.0 10.20.100.2

    c. ip route 10.10.16.0 255.255.255.255 10.10.10.2

    d. ip route 10.10.16.0 255.255.255.0 10.10.10.2

14. What is the purpose of the gateway of last resort?

15. What is the command for defining the gateway of last resort if the IP address for the next hop is 192.168.45.1?

16. The command **sh ip route** is entered on a router. What does it mean if the following command is displayed?

```
Gateway of last resort is not set
```

17. The following information is displayed after entering the **sh ip int brief** command. What is this indicating?

```
RouterA#sh ip int brief
00:22:18: %SYS-5-CONFIG_I: Configured from console
Interface          IP-Address  OK? Method Status   Protocol
FastEthernet0/0    192.168.200.1 YES manual up       down
```

18 What is the command for showing only the static routes? Indicate the command and the router prompt.

19. What is the purpose of the exit interface?

20. Specify the command for setting the exit interface to be FA0/1 if the destination network is 10.10.20.0, the subnet mask is 255.255.255.128, and the next hop address is 10.100.25.1.

21. The **show ip route** command is entered on a router. What information does the following indicate?

```
S 192.168.10.0/24 is directly connected, Null 0
```

22. In regards to Figure 2-17, the network engineer would like to trace a route from Router 1 to 10.10.200.1. What command should be used if the 10.10.200.1 interface is a PC?

23. In regards to problem 22, how many hops will the **traceroute** require?

24. What is load balancing?

### Section 2-2

25. What is the difference between a *static* and a *dynamic* routing protocol?

26. What are the four key issues in dynamic routing protocols?

27. Define hop count.

28. Which of the following is *not* a metric used in dynamic routing protocols?

    a. Hop count

    b. Cost

    c. Runs

    d. Ticks

29. A distance vector protocol typically uses what as the metric?

30. Determine the hop count for Router 2 to subnet B in Figure 2-18.

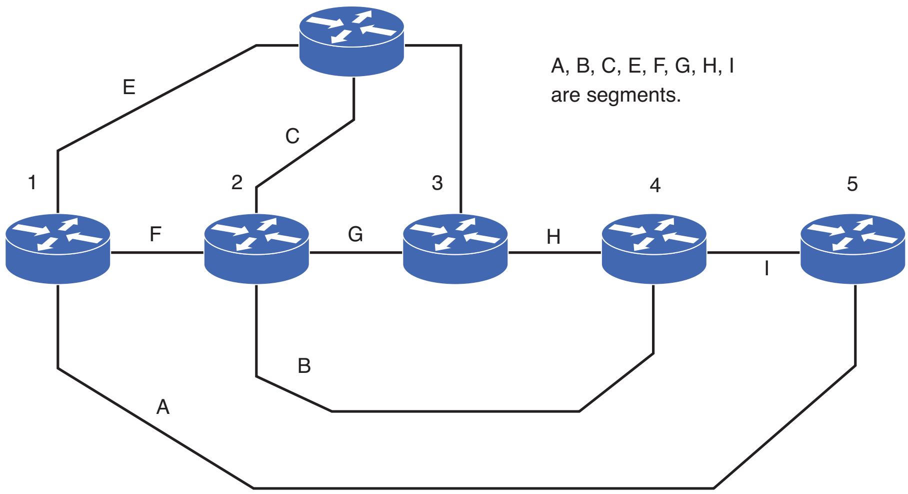



**FIGURE 2-18** The network for problems 2-30 through 2-32

31. For Figure 2-18, what is the hop count from Router5 to subnet G?
32. For Figure 2-18, what is the hop count from Router3 to subnet A?
33. Link state protocols issue what to update neighbor routers regarding route status?
    a. Hop status
    b. Link state advertisements
    c. “Hello” packets
    d. Adjacencies
34. Which of the following are key issues of link state protocols?
    a. Send updates every 90 seconds
    b. Send update when routing changes
    c. Use link lights to establish adjacencies
    d. Use a hop count metric to determine the best route to a destination

### Section 2-3

35. RIP is classified as which of the following?
    a. Distance vector protocol
    b. Dynamic routing protocol
    c. Link state protocol
    d. a and c
    e. a and b
    f. b and c
36. Define routing loops.
37. Which of the following are examples of classful addresses?
    a. 10.10.0.0
    b. 192.168.0.0
    c. 10.1.0.0
    d. 10.0.0.0
38. What is the router command to enable the RIP routing protocol on a router?
    a. **config router RIP**
    b. **router rip**
    c. **rip 10.0.0.0**
    d. **network 10.0.0.0**
39. What does it mean to *advertise* a network?
40. The network shown in Figure 2-19 is an example of which of the following?

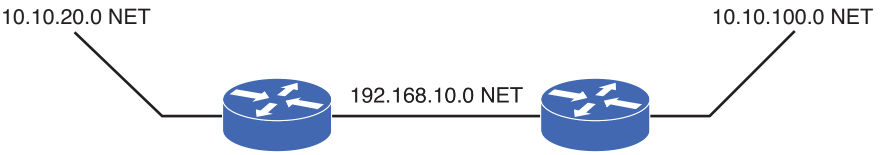



**FIGURE 2-19** The network for problem 39

    a. Contiguous network
    b. Discontiguous network
    c. Continuous network
    d. Discontinuous network
41. Write the commands to enable RIP for use on a 192.168.10.0 network.

42. The command **show ip protocol** is used on a router to
    a. Display the routing protocol that can run on the router
    b. Display the IP address of the routers running an IP protocol
    c. Display the routing protocols running on the router
    d. None of the above
43. The command **show ip interface brief** is used on a router to
    a. Check the current configuration of the interfaces
    b. Check the assigned IP addresses for the interface
    c. Check the status of the interfaces
    d. All the above
    e. None of the above
44. The command **show ip route** is used on a router to
    a. Set a static route
    b. Configure a static route
    c. Display the configured routes on a router
    d. Display how often routing updates are sent
    e. C and D
    f. B and D
45. The command used to display the router's current running-configuration is
    a. **show run**
    b. **show routing**
    c. **show interface**
    d. **show controller**
46. List four limitations of RIP.
47. What router command is issued to specify that the routing protocol is RIPv2? Specify the prompt and the command.
48. What is the hop count limit in a network using RIP?
49. RIP is specified as the routing protocol on a router. There are two possible routes to a destination. What metric does RIP use to determine which route to take?
50. RIP is configured for a 192.168.25.0 network. The subnet mask on a router interface is configured as follows:

    ```
    Router(config)#int fa0/0
    Router(config-if)#ip address 192.168.25.15  255.255.255.128
    ```

    What happens?

51. The **show ip protocol** command is issued on a router running RIP. What does this part of the message indicate?

```
Default version control: send version 2, receive version 2
```

### Section 2-4

52. What port does TFTP use?

53. List the command and prompt used to save a router configuration file to the TFTP server.

54. List the command and prompt used to load a save configuration file from the TFTP server.

### Critical Thinking

55. You are configuring a router connection to a remote network. What protocol would you select if there is only one network route to the remote network? Explain why you selected the protocol.

56. You are configuring the routing protocols for a small network. What routing protocol would you select, and why?

57. A router's interface FastEtheret0/1 is configured with the network 172.16.7.0/24. Then, a static route command of **ip route 172.16.7.0 255.255.255.0 10.10.7.254** is entered. What will happen? Discuss and explain your answer.

58. A router's interface FastEtheret0/1 is configured with the network 172.16.7.0/24. Then, a static route command of **ip route 172.16.7.0 255.255.255.128 10.10.7.254** is entered. What will happen? Discuss and explain your answer.

59. The network shown in Figure 2-17 has been configured to run RIP routing. The **sh ip route** command is issued on Router1 and the following information is displayed. Are all of the routes defined for this network? If not, then how many routes should be listed in this network, and list the missing route and interface information.

```
Router1#sh ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile,
B – BGP D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter
area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
I – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, * candidate
default
U – per-user static route, o – ODR T – traffic engineered route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 5 subnets
R 10.10.16.0 [120/1] via 10.20.100.2, 00:00:05, FastEthernet0/2
R 10.50.10.0 [120/1] via 10.20.100.2, 00:00:05, FastEthernet0/2
C 10.10.20.0 is directly connected, FastEthernet0/0
C 10.10.10.0 is directly connected, FastEthernet0/1
C 10.20.100.0 is directly connected, FastEthernet0/2
```

60. Your task is to configure static routes on Router 1 to reach every network in the network diagram shown in Figure 2-17. Be sure to use a route with less hop count as the primary route and designate the other as the backup route if there are multiple routes to the same destination. If the routes have equal cost, then pick either one as the primary. Assume that all networks are using a 255.255.255.0 subnet mask.

*This page intentionally left blank*