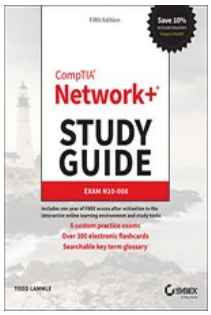

CompTIA Network+ Study Guide: Exam N10-008, 5th Edition

by Todd Lammle

Chapter 9: Introduction to IP Routing

The following Comptia Network+ Exam Objectives are Covered in This Chapter

- **2.2 Compare and contrast routing technologies and bandwidth management concepts.**
  - Dynamic routing
    - Routing Information Protocol (RIP), Open Shortest
    - Path First (OSPF), Enhanced
    - Interior Gateway Routing Protocol
    - (EIGRP), Border Gateway Protocol (BGP)
  - Link state vs. distance vector vs. hybrid
    - Static routing
    - Default route
    - Administrative distance
    - Exterior vs. interior
    - Time to live

IP routing is the process of moving packets from one network to another network using routers. The IP routing process is a super-important subject to understand because it pertains to all routers and configurations that use IP.

Before you read this chapter, you need to understand the difference between a routing protocol and a routed protocol. A *routing protocol* is a tool used by routers to dynamically find all the networks in the internetwork as well as to ensure that all routers have the same routing table. Basically, a routing protocol determines the path of a packet through an internetwork. Examples of routing protocols are Routing Information Protocol (RIP), Routing Information Protocol version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Broder Gateway Protocol (BGP).

Once all routers know about all networks, a *routed protocol* can be used to send user data (packets) through the established internetwork. Routed protocols are assigned to an interface and determine the method of packet delivery. Examples of routed protocols are Internet Protocol (IP) and Internet Protocol version 6 (IPv6).

In this chapter, I'm going to describe IP routing with routers. I will explain, in a step-by-step fashion, the IP routing process. I will also explain static and dynamic routing on a conceptual level, with more details about dynamic routing in Chapter 10, "Routing Protocols."

Note To find Todd Lammle CompTIA videos and practice questions, please see `www.lammle.com`.

Routing Basics

Once you create an internetwork by connecting your wide area networks (WANs) and local area networks (LANs) to a router, you need to configure logical network addresses, such as IP addresses, to all hosts on the internetwork so that they can communicate via routers across that internetwork.

In IT, routing essentially refers to the process of taking a packet from one device and sending it through the network to another device on a different network. Routers don't really care about hosts—they care only about networks and the best path to each network. The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

If your network has no routers, then it should be apparent that, well, you are not routing. But if you do have them, they're there to route traffic to all the networks in your internetwork. To be capable of routing packets, a router must know at least the following information:

- Destination network address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network

- How to maintain and verify routing information

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a *routing table* (a map of the internetwork) that describes how to find the remote networks. If a network is directly connected, then the router already knows how to get to it.

If a network isn't directly connected to the router, the router must use one of two ways to learn how to get to it. One way is called *static routing*, which can be a ton of work because it requires someone to hand-type all network locations into the routing table. The other way is dynamic routing.

In *dynamic routing*, a protocol on one router communicates with the same protocol running on neighbor routers. The routers then update each other about all the networks they know and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the event. If static routing is used, the administrator is responsible for updating all changes by hand into all routers. Understandably, in a large network, it's common to find that a combination of both dynamic and static routing is being used.

Before we jump into the IP routing process, let's take a look at a simple example that demonstrates how a router uses the routing table to route packets out of an interface. We'll be going into a more detailed study of this process in a minute.

Figure 9.1 shows a simple two-router network. Lab_A has one serial interface and three LAN interfaces.

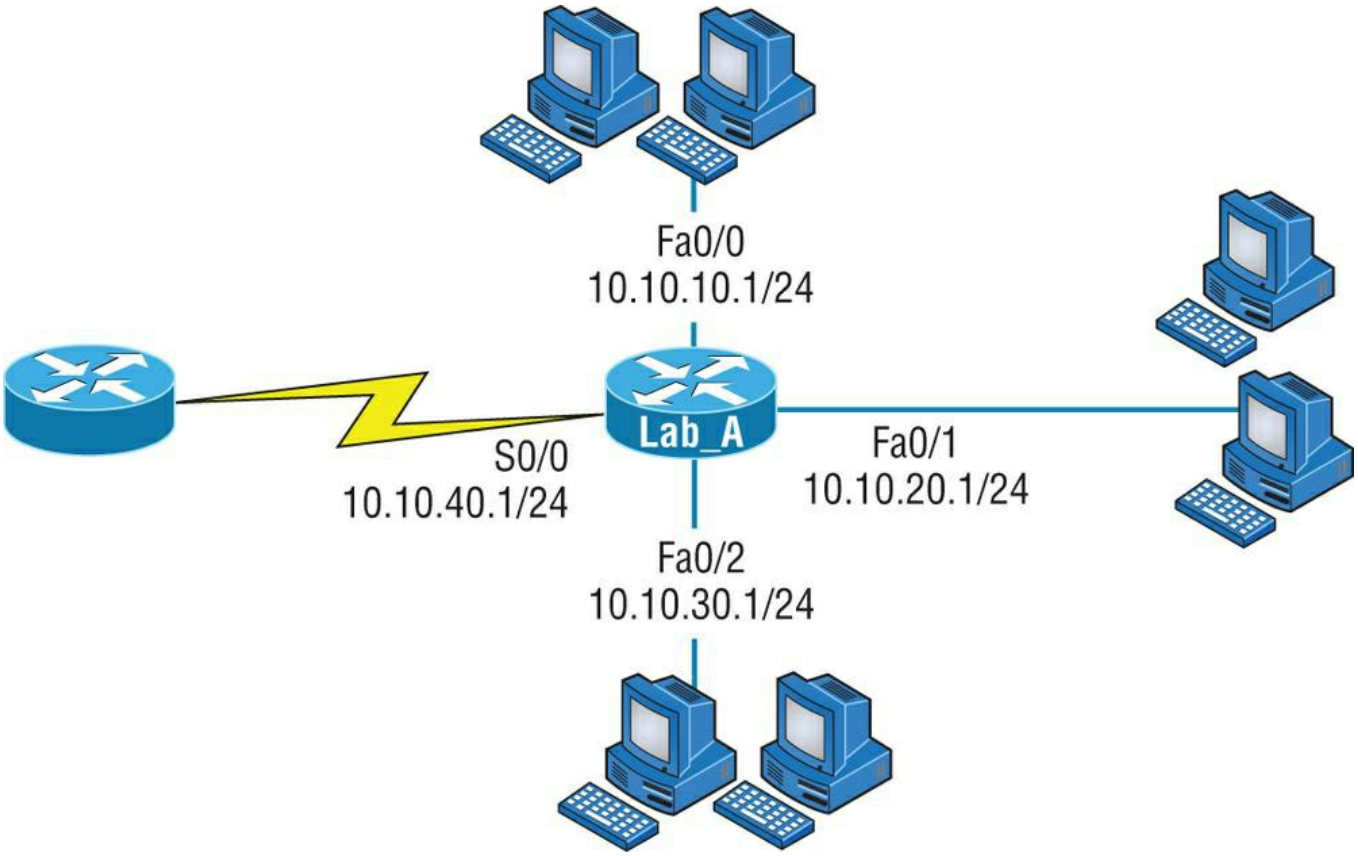

Figure 9.1: A simple routing example

Looking at Figure 9.1, can you figure out which interface Lab_A will use to forward an IP datagram to a host with an IP address of 10.10.10.10?

By using the Cisco IOS command `show ip route`, we can see the routing table (map of the internetwork) that router Lab_A will use to make all forwarding decisions:

```
Router_A#show ip route
[output cut]
Gateway of last resort is not set
C       10.10.10.0/24 is directly connected, FastEthernet0/0
C       10.10.20.0/24 is directly connected, FastEthernet0/1
C       10.10.30.0/24 is directly connected, FastEthernet0/2
C       10.10.40.0/24 is directly connected, Serial 0/0
```

The `C` in the routing table output means that the networks listed are "directly connected," and until we add a routing protocol—

something like RIP, EIGRP, and so on—to the routers in our internetwork, or use static routes, we'll have only directly connected networks in our routing table.

So, let's get back to the original question: By looking at the figure and the output of the routing table, can you tell what Lab_A will do with a received packet that has a destination IP address of 10.10.10.10? If you answered, "The router will packet-switch the packet to interface FastEthernet 0/0, and this interface will then frame the packet and send it out on the network segment," you're right.

Just because we can, let's look at a different example. Based on the output of the next routing table, which interface will a packet with a destination address of 10.10.10.14 be forwarded to?

```
Router_A#sh ip route
[output cut]
Gateway of last resort is not set
C       10.10.10.16/28 is directly connected, FastEthernet0/0
C       10.10.10.8/29 is directly connected, FastEthernet0/1
C       10.10.10.4/30 is directly connected, FastEthernet0/2
C       10.10.10.0/30 is directly connected, Serial 0/0
```

First, you can see that the network is subnetted and that each interface has a different mask. And I have to tell you, you positively can't answer this question if you can't subnet—no way! Here's the answer: 10.10.10.14 would be a host in the 10.10.10.8/29 subnet connected to the FastEthernet 0/1 interface. Don't freak if this one left you staring vacantly. Instead, if you're struggling, go back and reread Chapter 8, "IP Subnetting, Troubleshooting IP, and Introduction to NAT," until you get it. This should then make perfect sense to you.

Note When the routing tables of all routers in the network are complete (because they include information about all the networks in the internetwork), they are considered *converged*, or in a steady state. This is covered in more detail in Chapter 10.

Now, let's get into this process in more detail.

The IP Routing Process

The IP routing process is actually pretty simple, and it doesn't change, regardless of the size of your network. I'm going to use Figure 9.2 to give you a picture of this step-by-step process. The question I'm asking is this: What happens when Host_A wants to communicate with Host_B on a different network? I'll go through how to answer that question by breaking down the process with headings to make it easier to understand. First, check out Figure 9.2.

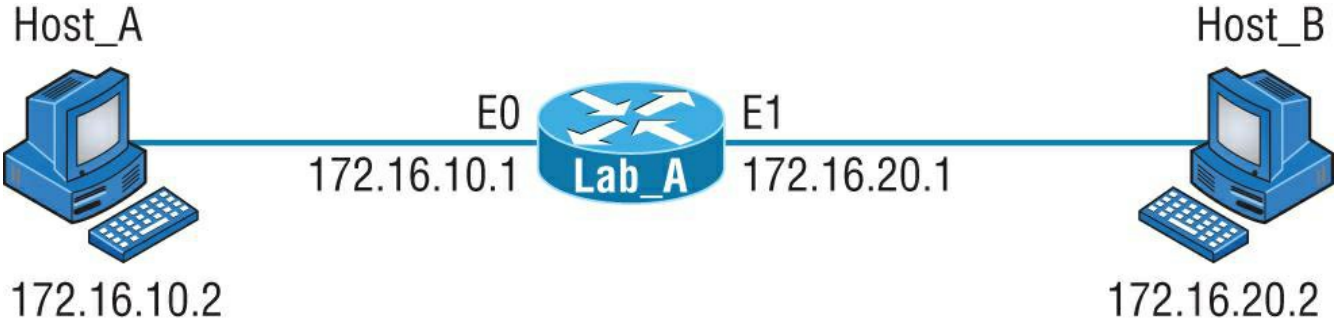

Figure 9.2: IP routing example using two hosts and one router

Suppose that a user on Host_A pings Host_B's IP address. Routing doesn't get any simpler than this, but it still involves a lot of steps. Let's work through them.

- A packet is created on the host:
    1. Internet Control Message Protocol (ICMP) creates an echo request payload (which is just the alphabet in the data field).
    2. ICMP hands that payload to IP, which then creates a packet. At a minimum, this packet contains an IP source address, an IP destination address, and a Protocol field with 01h. (Remember that Cisco likes to use *0x* in front of hex characters, so this could look like 0x01.) All of that tells the receiving host whom it should hand the payload to when the destination is reached. In this example, it's ICMP.

       The packet is forwarded:
    3. After the packet is created, IP determines whether the destination IP address is on the local network or a remote one.
    4. Because IP has discovered that this is a remote request, the packet needs to be sent to the default gateway so the packet can be routed to the correct remote network. The Registry in Windows is parsed to find the configured default gateway.
    5. The default gateway of host 172.16.10.2 (Host_A) is configured to 172.16.10.1. For this packet to be sent to the default

gateway, the hardware address of the router's interface Ethernet 0 (configured with the IP address of 172.16.10.1) must be known. Why? So the packet can be handed down to the Data Link layer, framed, and sent to the router's interface that's connected to the 172.16.10.0 network. Because hosts only communicate via hardware addresses on the local LAN, it's important to recognize that for Host_A to communicate to Host_B, it has to send packets to the Media Access Control (MAC) address of the default gateway on the local network.

Note MAC addresses are always local on the LAN and never go through and past a router.

6. The Address Resolution Protocol (ARP) cache of the host is checked to see whether the IP address of the default gateway has already been resolved to a hardware address. If it has, the packet is then free to be handed to the Data Link layer for framing. (The hardware-destination address is also handed down with that packet.) To view the ARP cache on your host, use the following command:

```
C:\>arp -a
Interface: 172.16.10.2 --- 0x3
  Internet Address      Physical Address      Type
  172.16.10.1           00-15-05-06-31-b0     dynamic
```

   If the hardware address isn't already in the ARP cache of the host, an ARP broadcast is sent out onto the local network to search for the hardware address of 172.16.10.1. The router responds to that request and provides the hardware address of Ethernet 0, and the host caches this address.

7. After the packet and destination hardware address have been handed to the Data Link layer, the LAN driver is used to provide media access via the type of LAN being used (in this example, it's Ethernet). A frame is then generated, encapsulating the packet with control information. Within that frame are the hardware-destination and source addresses plus, in this case, an Ether-Type field that describes the Network layer protocol that handed the packet to the Data Link layer—in this instance, IP. At the end of the frame is something called a Frame Check Sequence (FCS) field that houses the result of the cyclic redundancy check (CRC). The frame would look something like what I've detailed in Figure 9.3. It contains Host_A's hardware (MAC) address and the hardware-destination address of the default gateway. It does not include the remote host's MAC address—remember that because it's important!

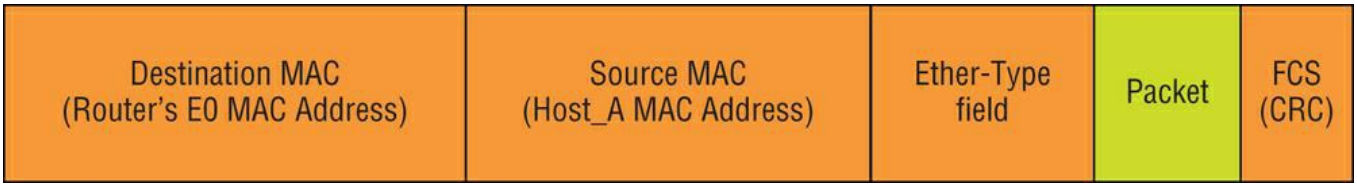

Figure 9.3: Frame used from Host_A to the Lab_A router when Host_B is pinged

8. When the frame is completed, it's handed down to the Physical layer to be placed onto the physical medium one bit at a time. In this example, the physical medium is twisted-pair wire.

   The router receives the packet:

9. Every device within the collision domain receives these bits and builds the frame. They each run a CRC and check the answer in the FCS field. If the answers don't match, the frame is discarded. But if the CRC matches, then the hardware-destination address is checked to see if it matches, too (in this example, it's the router's interface, Ethernet 0). If it's a match, then the Ether-Type field is checked to find the protocol used at the Network layer.

10. The packet is pulled from the frame, and what is left of the frame is discarded. The packet is then handed to the protocol listed in the Ether-Type field—it's given to IP.

    The router routes the packet:

11. IP receives the packet and checks the IP destination address. Because the packet's destination address doesn't match any of the addresses configured on the receiving router's interfaces, the router will look up the destination IP network address in its routing table.

12. The routing table must have an entry for the network 172.16.20.0 or the packet will be discarded immediately and an ICMP message will be sent back to the originating device with a Destination Unreachable message.

13. If the router does find an entry for the destination network in its table, the packet is switched to the exit interface—in this example, interface Ethernet 1. The following output displays the Lab_A router's routing table. The `C` means "directly connected." No routing protocols are needed in this network because all networks (all two of them) are directly connected:

```
Lab_A>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, ia
   - IS-IS intearea * - candidate default, U - per-user static
   route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.10.0 is directly connected, Ethernet0
C       172.16.20.0 is directly connected, Ethernet1
```

14. The router packet-switches the packet to the Ethernet 1 buffer.

15. Now that the packet is in the Ethernet 1 buffer, IP needs to know the hardware address of the destination host and first checks the ARP cache. If the hardware address of Host_B has already been resolved and is in the router's ARP cache, then the packet and the hardware address are handed down to the Data Link layer to be framed. Let's take a look at the ARP cache on the Lab_A router by using the `show ip arp` command:

    ```
    Lab_A#sh ip arp
    Protocol  Address     Age(min) Hardware Addr  Type   Interface
    Internet  172.16.20.1   -     00d0.58ad.05f4  ARPA   Ethernet1
    Internet  172.16.20.2   3     0030.9492.a5dd  ARPA   Ethernet1
    Internet  172.16.10.1   -     0015.0506.31b0  ARPA   Ethernet0
    Internet  172.16.10.2  12     0030.9492.a4ac  ARPA   Ethernet0
    ```

    The dash (-) means that this is the physical interface on the router. From this output, we can see that the router knows the 172.16.10.2 (Host_A) and 172.16.20.2 (Host_B) hardware addresses. Cisco routers will keep an entry in the ARP table for four hours. But if the hardware address hasn't already been resolved, the router then sends an ARP request out E1 looking for the hardware address of 172.16.20.2. Host_B responds with its hardware address, and the packet and hardware-destination address are both sent to the Data Link layer for framing.

16. The Data Link layer creates a frame with the destination and source hardware address, Ether-Type field, and FCS field at the end. The frame is handed to the Physical layer to be sent out on the physical medium one bit at a time.

    Finally, the remote host receives the packet:

17. Host_B receives the frame and immediately runs a CRC. If the result matches what's in the FCS field, the hardware-destination address is then checked. If the host finds a match, the Ether-Type field is then checked to determine the protocol that the packet should be handed to at the Network layer—IP, in this example.

18. At the Network layer, IP receives the packet and checks the IP destination address. Because there's finally a match made, the Protocol field is checked to find out whom the payload should be given to.

19. The payload is handed to ICMP, which understands that this is an echo request. ICMP responds to this by immediately discarding the packet and generating a new payload as an echo reply.

    The destination host becomes a source host:

20. A packet is created, including the source and destination IP addresses, Protocol field, and payload. The destination device is now Host_A.

21. IP checks to see whether the destination IP address is a device on the local LAN or on a remote network. Because the destination device is on a remote network, the packet needs to be sent to the default gateway.

22. The default gateway IP address is found in the Registry of the Windows device, and the ARP cache is checked to see whether the hardware address has already been resolved from an IP address.

23. After the hardware address of the default gateway is found, the packet and destination hardware addresses are handed down to the Data Link layer for framing.

24. The Data Link layer frames the packet of information and includes the following in the header:

    - The destination and source hardware addresses
    - The Ether-Type field with 0x0800 (IP) in it
    - The FCS field with the CRC result in tow

25. The frame is now handed down to the Physical layer to be sent out over the network medium one bit at a time.

    Time for the router to route another packet:

26. The router's Ethernet 1 interface receives the bits and builds a frame. The CRC is run, and the FCS field is checked to make sure the answers match.

27. When the CRC is found to be okay, the hardware-destination address is checked. Because the router's interface is a match, the packet is pulled from the frame, and the Ether-Type field is checked to see which protocol at the Network layer the packet should be delivered to.

28. The protocol is determined to be IP, so it gets the packet. IP runs a CRC check on the IP header first and then checks the destination IP address.

    Note IP does not run a complete CRC the way the Data Link layer does—it only checks the header for errors.

    Because the IP destination address doesn't match any of the router's interfaces, the routing table is checked to see whether it has a route to 172.16.10.0. If it doesn't have a route over to the destination network, the packet will be discarded immediately. (This is the source point of confusion for a lot of administrators—when a ping fails, most people think the packet never reached the destination host. But as we see here, that's not *always* the case. All it takes is just one of the remote routers to be lacking a route back to the originating host's network and—*poof!*—the packet is dropped on the *return trip*, not on its way to the host.)

    Note Just a quick note to mention that when (if) the packet is lost on the way back to the originating host, you will typically see a Request Timed Out message because it is an unknown error. If the error occurs because of a known issue, such as a route that is not in the routing table on the way to the destination device, you will see a Destination Unreachable message. This should help you determine if the problem occurred on the way to the destination or on the way back.

29. In this case, the router does know how to get to network 172.16.10.0—the exit interface is Ethernet 0—so the packet is switched to interface Ethernet 0.

30. The router checks the ARP cache to determine whether the hardware address for 172.16.10.2 has already been resolved.

31. Because the hardware address to 172.16.10.2 is already cached from the originating trip to Host_B, the hardware address and packet are handed to the Data Link layer.

32. The Data Link layer builds a frame with the destination and source hardware addresses and then puts IP in the Ether-Type field. A CRC is run on the frame, and the result is placed in the FCS field.

33. The frame is then handed to the Physical layer to be sent out onto the local network one bit at a time.

    The original source host, now the destination host, receives the reply packet:

34. The destination host receives the frame, runs a CRC, checks the hardware destination address, and looks in the Ether-Type field to find out whom to hand the packet to.

35. IP is the designated receiver, and after the packet is handed to IP at the Network layer, IP checks the Protocol field for further direction. IP finds instructions to give the payload to ICMP, and ICMP determines the packet to be an ICMP echo reply.

36. ICMP acknowledges that it has received the reply by sending an exclamation point (!) to the user interface. ICMP then attempts to send four more echo requests to the destination host.

You've just been introduced to "Todd's 36 easy steps to understanding IP routing." The key point to understand here is that if you had a much larger network, the process would be the *same*. In a really big internetwork, the packet just goes through more hops before it finds the destination host.

It's super important to remember that when Host_A sends a packet to Host_B, the destination hardware address used is the default gateway's Ethernet interface. Why? Because frames can't be placed on remote networks—only local networks. So packets destined for remote networks must go through the default gateway.

Let's take a look at Host_A's ARP cache now by using the `arp -a` command from the DOS prompt:

```
C:\>arp -a
Interface: 172.16.10.2 --- 0x3
  Internet Address      Physical Address      Type
  172.16.10.1           00-15-05-06-31-b0     dynamic
  172.16.20.1           00-15-05-06-31-b0     dynamic
```

Did you notice that the hardware (MAC) address that Host_A uses to get to Host_B is the Lab_A E0 interface?

Hardware addresses are *always* local, and they never pass a router's interface. Understanding this process is as important to internetworking as breathing air is to you, so carve this into your memory!

Testing Your IP Routing Understanding

I want to make sure you understand IP routing because it's really that important. So, I'm going to use this section to test your understanding of the IP routing process by having you look at a couple of figures and answer some very basic IP routing questions.

Figure 9.4 shows a LAN connected to RouterA, which is, in turn, connected via a WAN link to RouterB. RouterB has a LAN connected with an HTTP server attached. Take a look.

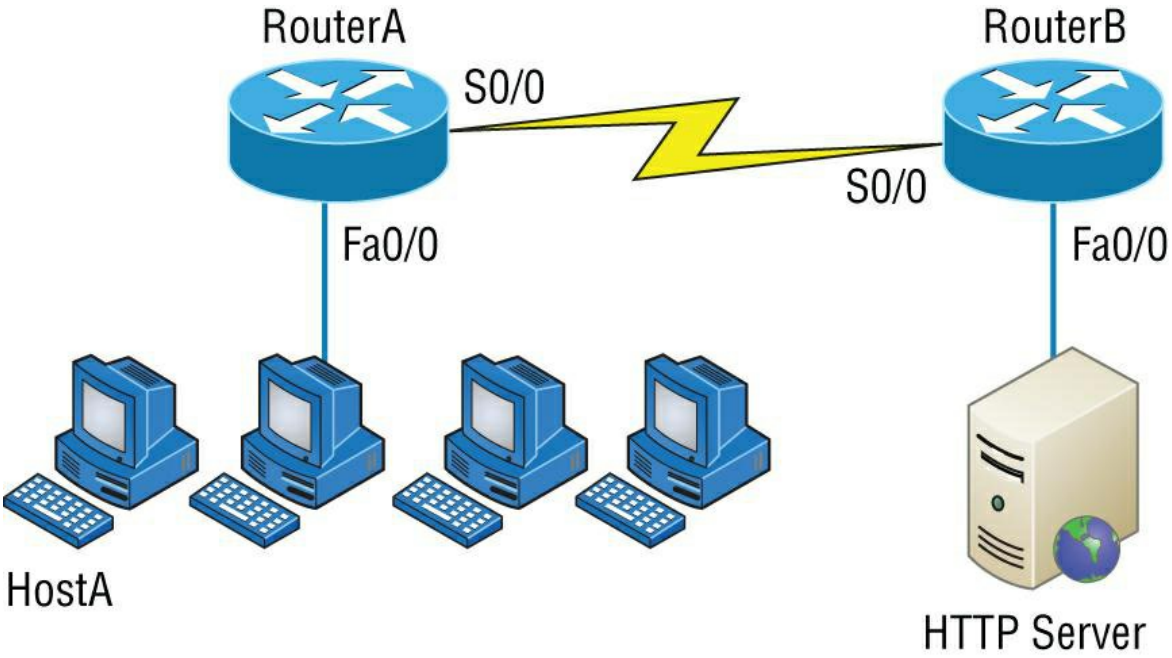

Figure 9.4: IP routing example 1

The critical information you need to glean from this figure is exactly how IP routing will occur in this example. Okay—we'll cheat a bit. I'll give you the answer, but then you should go back over the figure and see if you can answer example 2 without looking at my answers:

1. The destination address of a frame, from HostA, will be the MAC address of the Fa0/0 interface of the RouterA router.
2. The destination address of a packet will be the IP address of the network interface card (NIC) of the HTTP server.
3. The destination port number in the segment header will have a value of 80.

That example was a pretty simple one, and it was also very to the point. One thing to remember is that if multiple hosts are communicating to the server using HTTP, they must all use a different source port number. That is how the server keeps the data separated at the Transport layer.

Let's mix it up a little and add another internetworking device into the network and then see if you can find the answers. Figure 9.5 shows a network with only one router but two switches.

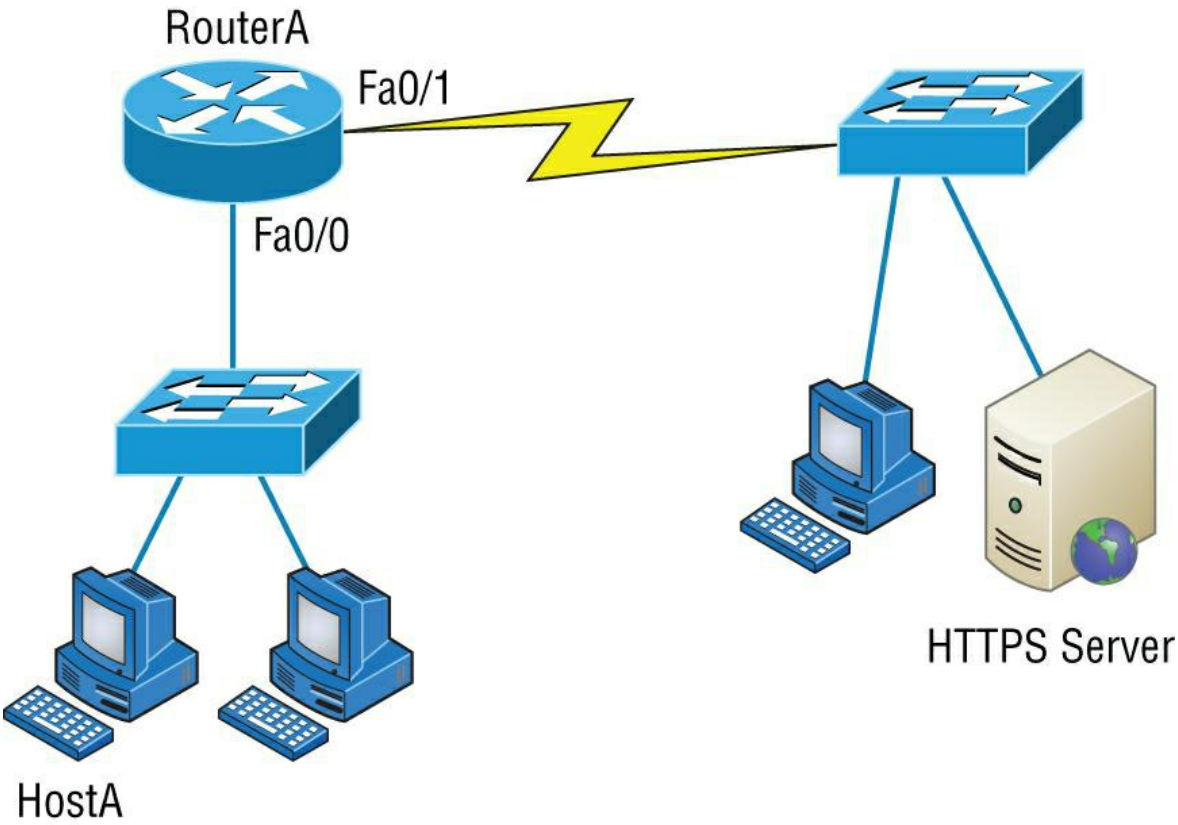

Figure 9.5: IP routing example 2

What you want to understand about the IP routing process here is what happens when HostA sends data to the HTTPS server:

1. The destination address of a frame from HostA will be the MAC address of the Fa0/0 interface of the RouterA router.
2. The destination address of a packet will be the IP address of the NIC of the HTTPS server.
3. The destination port number in the segment header will have a value of 443.

Notice that neither switch was used as either a default gateway or another destination. That's because switches have nothing to do with routing. I wonder how many of you chose the switch as the default gateway (destination) MAC address for HostA. If you did, don't feel bad—just take another look with that fact in mind. It's very important to remember that the destination MAC address will always be the router's interface—if your packets are destined for outside the LAN, as they were in these last two examples.

Static and Dynamic Routing

How does a router send packets to remote networks when the only way it can send them is by looking at the routing table to find out how to get to the remote networks? And what happens when a router receives a packet for a network that isn't listed in the routing table? It doesn't send a broadcast looking for the remote network—the router just discards the packet.

There are several ways to configure the routing tables to include all the networks so that packets will be forwarded. Understand that what's best for one network isn't necessarily what's best for another. Knowing about and being able to recognize the different types of routing will really help you come up with the best solution for your specific environment and business requirements.

Note Routing convergence is the time required by the routing protocols to update the routing tables (forwarding tables) on all routers in the network.

Looking at Figure 9.6, you can see that we can configure a router with either static or dynamic routing. If we choose static routing, then we have to go to each router and type in each network and the path that IP will use to send packets. However, static routing does not scale well in large networks, but dynamic routing does because network routes are automatically added to the routing table via the routing protocol.

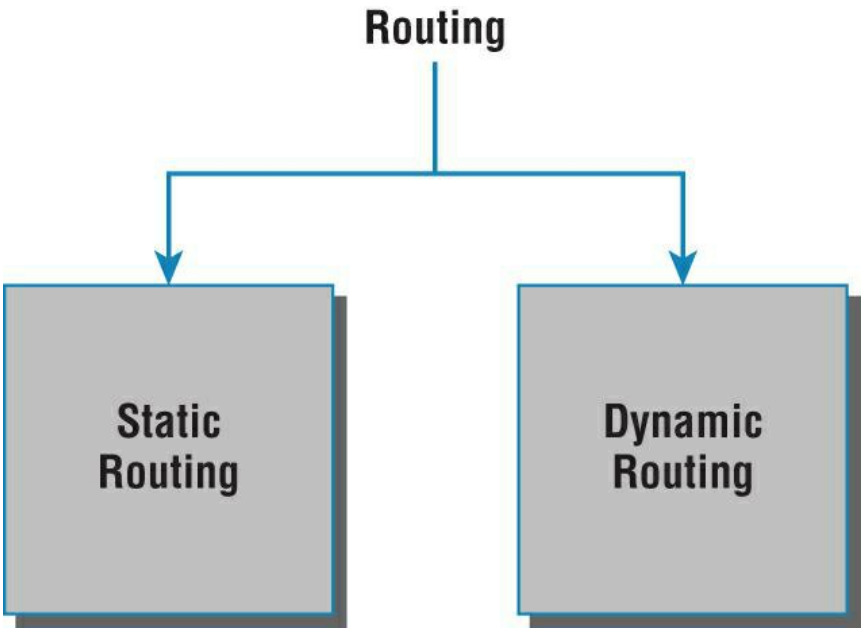

Figure 9.6: Routing options

Dynamic routing protocols break up into many different categories or types of protocols, as shown in Figure 9.7. The first split in the dynamic protocol branch is the division of interior gateway protocols (IGPs) and exterior gateway protocols (EGPs). We are going to talk about each protocol and category, but for now the difference between IGP and EGP is interior or exterior routing of an autonomous system (AS).

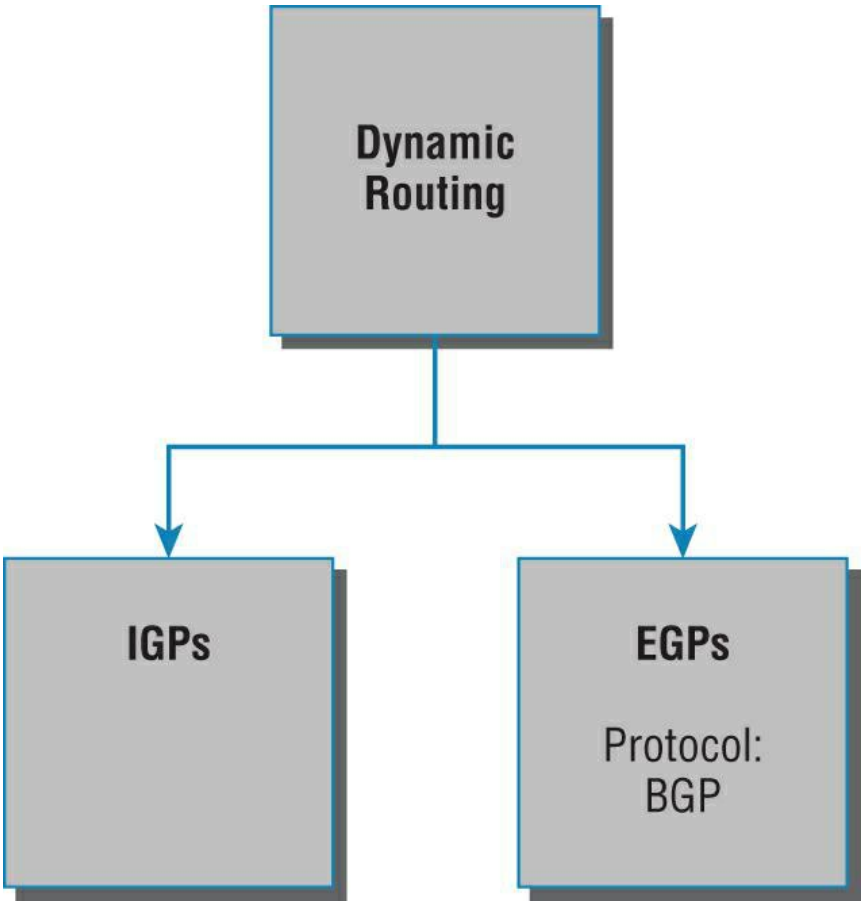

Figure 9.7: Dynamic routing options

An *autonomous system* is a collection of networks or subnets that are in the same administrative domain. This is another way of saying an administrative domain is within your company's network, and you control or administer all the subnets that are within it. You control and set the policy for what happens in the network or autonomous system. I hope you can now see that an IGP operates and routes within an AS and an EGP works outside or between more than one AS.

The most popular protocol for an EGP is Border Gateway Protocol (BGP), which is typically used by ISPs or really large corporations. As an administrator of a small to medium network, you'll probably never use BGP. (BGP will be discussed in Chapter 10.)

Now that we have that out of the way, let's talk about all the great things that dynamic routing protocols do for us. The thing that comes to mind first is the amount of time and energy we save configuring routers. We won't have to go to every single router and define for it, with a static route, what and where every destination network is. If that were the only way to configure routing, there would probably be a lot fewer of us interested in doing this for a living. Thankfully, we have routing protocols that do much of the work for us. We still have to know what the routing protocols are going to do and how they will do it, but the protocols will take care of most of the updating and sending information to each other.

That is the end of the EGP branch of the tree, but the IGP branch continues to split out as we go down further. Looking at Figure 9.8, with the IGP split, you can see that there are two primary categories: distance-vector (DV) and link-state (LS) routing protocols.

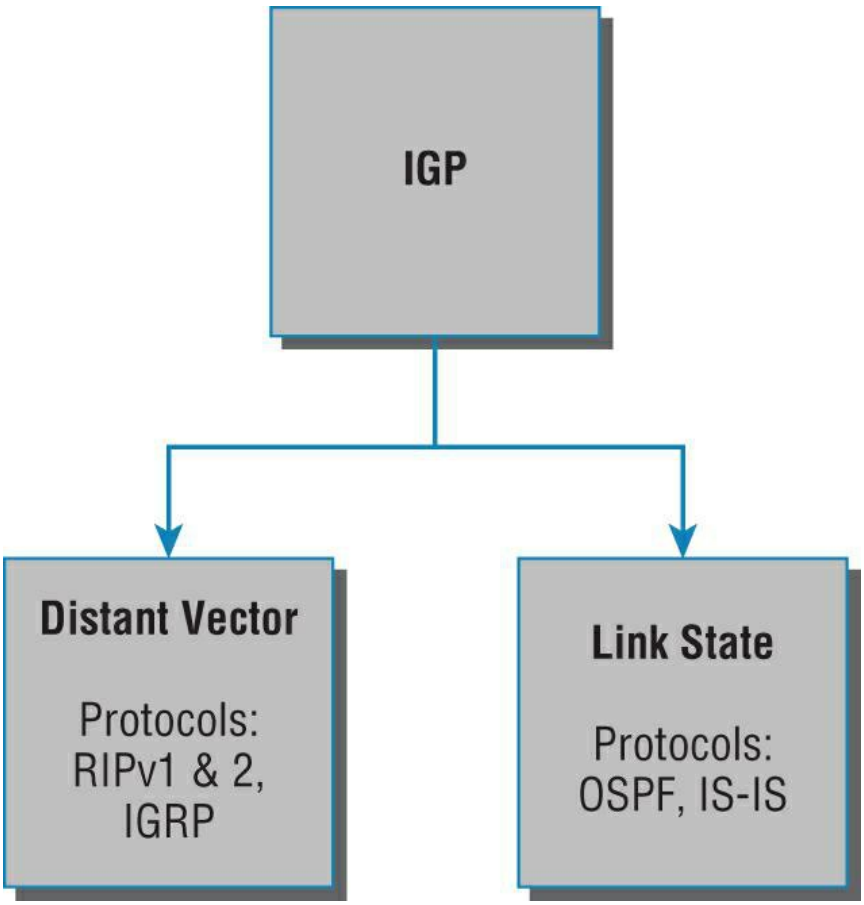

Figure 9.8: DV and LS routing protocols

No worries—I'm going to discuss all of these types of protocols in Chapter 10, "Routing Protocols." But in the distance-vector category, for example, we have RIP and Interior Gateway Routing Protocol (IGRP). Under the link-state category are the nonproprietary OSPF and Intermediate System-to-Intermediate System (IS-IS) that were designed to work in larger internetworks.

Now, in Figure 9.9, you can see from the diagram that there is a third category: the hybrid protocol category.

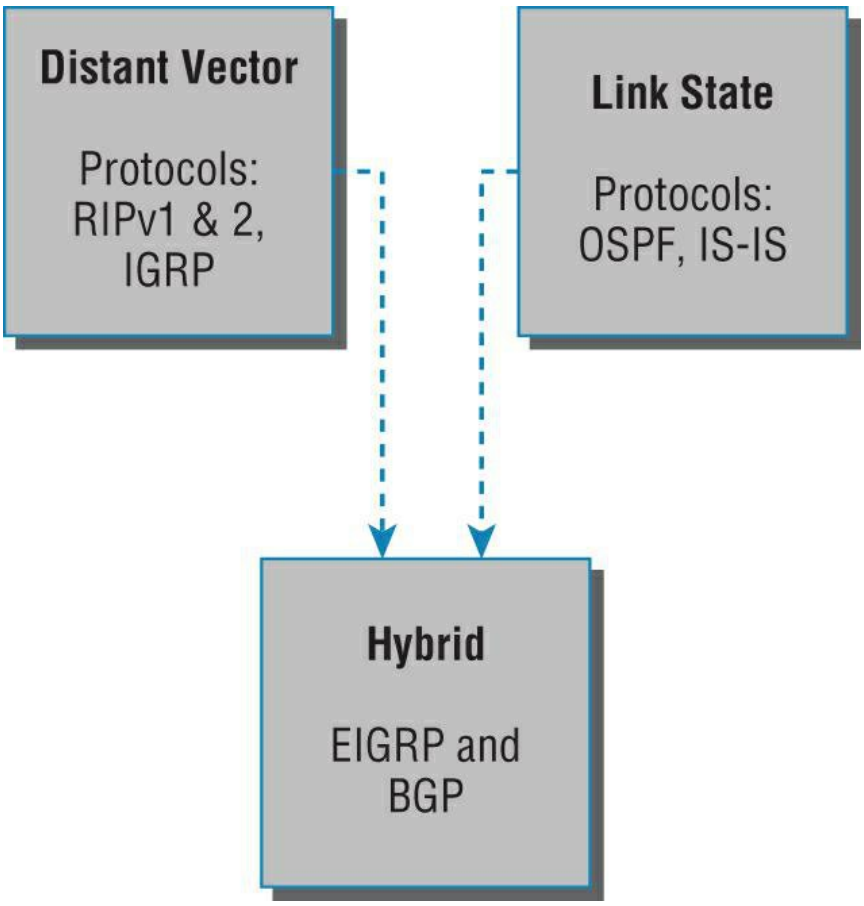

Figure 9.9: Hybrid routing

The only protocols under this category are EIGRP and BGP. It is Cisco proprietary (or used to be, but people mostly just run this with Cisco gear) and uses the features of both DV and LS. Now that we have a handle on IP routing, let's move on to Chapter 10 and discuss the IGP routing protocols introduced in this chapter.

Summary

This chapter covered the IP routing process in detail. It's extremely important that you really understand the basics we covered in this chapter because everything that's done on a router typically will have some type of IP routing configured and running.

You learned in this chapter how IP routing uses frames to transport packets between routers and to the destination host. Understanding the process of how packets and frames traverse a network is critical to your fundamental understanding of IP routing.

After I covered the basics of IP routing, I went through some examples to test your understanding and to emphasize the importance of the IP routing fundamentals that you need. I finished the chapter with an introduction to static and dynamic routing and explained IGP and EGP as well as the difference between distance-vector and link-state routing protocols. In the next chapter, we'll continue with dynamic routing by discussing the various dynamic routing protocols.

Exam Essentials

Understand the basic IP routing process. You need to remember that the frame changes at each hop but that the packet is never changed or manipulated in any way until it reaches the destination device.

Understand that MAC addresses are always local. A MAC (hardware) address will only be used on a local LAN. It will never pass a router's interface.

Understand that a frame carries a packet to only two places. A frame uses MAC (hardware) addresses to send a packet on a LAN. The frame will take the packet to either a host on the LAN or a router's interface if the packet is destined for a remote network.

Remember the difference between static and dynamic routing. Static routing is where you, as the administrator, by hand, add every route into every routing table on every router on the network. This is as much work as it sounds like, which is why we use dynamic routing protocols that do the work for us. Of course, we'll discuss dynamic routing protocols more in the next chapter, but the main job of a routing protocol is to update routing tables.

Written Lab

You can find the answers to the written labs in Appendix A. Write the answers to the following questions:

1. True/False: RIPv2 is a hybrid routing protocol.
2. True/False: RIPv1 is a link state routing protocol.
3. True/False: EIGRP was created by the ISO.
4. What defines a collection of networks or subnets that are in the same administrative domain?
5. You need a routing protocol that can be run in a very large network with routers from multiple vendors. What routing protocol would be your best choice?
6. Which type of routing are you performing if you have to go to each router and type in each network and the path that IP will use to send packets?
7. You are trying to reach a server on another subnet. What will be the destination hardware address of a frame sent from your host?
8. You are trying to reach a server on another subnet. What will be the destination IP address of a packet sent from your host?
9. A server has received a frame from your remote host. What will be the source hardware address of the frame?
10. A server has received a packet from your remote host. What will be the destination IP address of the packet?

Answers

1. False. RIP and RIPv2 are both distance-vector protocols.
2. False. RIP and RIPv2 are both distance-vector protocols.
3. False. EIGRP was created by Cisco as a proprietary routing protocol; however, it is no longer proprietary.
4. Autonomous system
5. RIP does not work well in large networks, so OSPF would be the best answer, and both RIP and OSPF are nonproprietary.
6. Static routing
7. The MAC address of your default gateway (router)
8. The IP address of the server
9. The MAC address of the router sending the frame to the server
10. The IP address of the server

Review Questions

You can find the answers to the review questions in Appendix B.

1. Which is not a routing protocol?

   A. RIP

   B. RIPv2

   C. RIPv3

   D. EIGRP

2. Which of these best describes dynamic routing?

   A. All network addresses must be hand-typed into the routing table.

   B. Only a portion of the network address must be hand-typed into the routing table.

   C. Routing tables are updated automatically when changes occur in the network.

   D. A and B.

3. Which is true regarding dynamic routing?

   A. Static routes are best in large networks and thus better to use than dynamic routing protocols.

   B. Static routes are automatically added to the routing table but dynamic routes must be added by hand.

   C. You must use a DNS and WINS server when configuring dynamic routing.

   D. Dynamic routes are automatically added to the routing table.

4. Which of the following is true for MAC addresses?

   A. MAC addresses are never local on the LAN and always pass through a router.

   B. MAC addresses are always local on the LAN and never go through or past a router.

   C. MAC addresses will always be the IP address of the Fa0/0 interface.

D. None of the above.

5. What is it called when protocols update their forwarding tables after changes have occurred? ?

A. Name resolution

B. Routing

C. Convergence

D. ARP resolution

6. What command would be used to view the ARP cache on your host? ?

A. `C:\ >show ip route`

B. `C:\ >show ip arp`

C. `C:\ >show protocols`

D. `C:\ >arp -a`

7. What happens when a router receives a packet for a network that isn't listed in the routing table? ?

A. It forwards the packet to the next available router.

B. It holds the packet until the address is updated in the routing table.

C. The router will use RIP to inform the host that it can't send the packet.

D. None of the above.

8. Which of the following is not a distance-vector protocol? ?

A. RIPv1

B. RIPv2

C. OSPF

D. IGRP

9. Which two of the following are link-state protocols? ?

A. RIPv1

B. RIPv2

C. OSPF

D. IS-IS

E. IGRP

10. Which of the following is a hybrid routing protocol? ?

A. RIPv2

B. EIGRP

C. IS-IS

D. IGRP

11. What does the acronym EIGRP stand for? ?

A. Enhanced Interior Gateway Routing Protocol

B. Enhanced Inside Gateway Redundancy Protocol

C. Enhanced Interior Group Reliability Protocol

D. Enhanced Interior Gateway Redundancy Protocol

12. What EGP protocol is used on the Internet? ?

A. GGP

B. EGP

C. BGP

D. IGP

13. What are the two categories of IGP protocols? (Choose two.)

A. Link state

B. Static

C. Distance vector

D. EGP

14. What two pieces of information does a router require to make a routing decision? (Choose two.)

A. Destination network (address)

B. Destination MAC address

C. Application layer protocol

D. Neighbor router

15. Where does a frame have to carry a packet to if it is destined for a remote network?

A. Default gateway

B. Neighbor host

C. Switch

D. Hub

16. Where along the IP routing process does a packet get changed?

A. Router

B. Host A

C. Destination device

D. Host B

17. When all routers in a network agree about the path from one point to another, the network is said to be what?

A. Dynamic

B. Static

C. Happy

D. Converged

18. What type of request must a client send if it does not know the destination MAC address?

A. ARP broadcast

B. Multicast

C. ICMP redirect

D. Reverse ARP

19. You need to perform maintenance on a router in your corporate office. It is important that the network does not go down. What can you do to accomplish your goal?

A. Configure BGP on the router.

B. Implement NAT on the router.

C. Configure on the router a static route that temporarily reroutes traffic through another office.

D. Implement convergence on the router.

20. When are you most likely to see a Request Timed Out message?

A. When an unknown error has occurred

B. When you have used the `arp -a` command incorrectly

C. When a known error has occurred

D. When you are using a hybrid routing protocol

Answers

1. C. Yep, you got it. RIP, RIPv2, and EIGRP are all examples of routing protocols; RIPv3 is nonexistent.
2. C. In dynamic routing, routers update each other about all the networks they know about and place this information into the routing table. This is possible because a protocol on one router communicates with the same protocol running on neighbor routers. If changes occur in the network, a dynamic routing protocol automatically informs all routers about the event.
3. D. Dynamic routing scales well in large networks and routes are automatically added into the routing table. Static routing is done by hand, one route at a time into each router.
4. B. Media Access Control (MAC) addresses are always local on the LAN and never go through and past a router.
5. C. Routing convergence is the time required by the routing protocols to update the routing tables (forwarding tables) on all routers in the network.
6. D. The `arp -a` command will show the ARP cache on your host.
7. D. Hope you answered D! A router will not send a broadcast looking for the remote network—the router will discard the packet.
8. C. RIPv1 and 2 and IGRP are all distance-vector (DV) protocols. Routers using a DV protocol send all or parts of their routing table in a routing-update message at a regular interval to each of their neighbor routers.
9. C, D. Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) are link-state (LS) routing protocols.
10. B. The only protocol you could select is Enhanced Interior Gateway Routing Protocol (EIGRP).
11. A. Interior Gateway Routing Protocol is a distance-vector (DV) interior gateway protocol.
12. C. Border Gateway Protocol (BGP) is the most popular choice for ISPs or really large corporations.
13. A, C. Distance-vector (DV) and link-state (LS) are the two routing protocols to remember.
14. A, D. A frame uses a local MAC address (router) to send a packet on the LAN. The frame will take the packet to either a host on the LAN or a router's interface if the packet is destined for a remote network, which would be sent to the neighbor router.
15. A. I hope you said A! Packets specifically have to be carried to a router in order to be routed through a network.
16. C. Remember that the frame changes at each hop but that the packet is never changed in any way until it reaches the destination device.
17. D. When the routing tables are complete because they include information about all networks in the internetwork, they are considered converged.
18. A. This is step 6 in the IP routing process. If the hardware address isn't in the ARP cache of the host, an ARP broadcast is sent out onto the local network to search for the hardware address.
19. C. The best answer would be to reroute traffic using a temporary static route until the maintenance is complete on the router.
20. A. You are most likely to see a Request Timed Out message when (if) a packet is lost on the way back to the originating host for an unknown error. Remember, if the error occurs because of a known issue, you are likely to see a Destination Unreachable message.