CHAPTER 1

Introduction to Routing and Packet Forwarding

Objectives

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

- What features do routers and computers have in common?
- How do you configure Cisco devices and apply addresses?
- Can you describe the basic structure of a routing table?
- Can you describe, in detail, how a router determines the best path and then switches a packet?

Key Terms

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

IP 3

router 3

packets 3

RAM 4

ROM 4

Operating system 4

local-area networks (LAN) 5

wide-area networks (WAN) 5

Ethernet 5

Internet service provider (ISP) 5

best path 5

routing table 5

Point-to-Point Protocol (PPP) 5

serial 6

Frame Relay 6

Asynchronous Transfer Mode (ATM) 6

dynamic routing protocols 6

unified communications 6

media 7

ARP 9

MAC address 9

Flash 9

NVRAM 9

IPv6 10

IS-IS 10

static routing 10

RIP 10

EIGRP 10

continues

Today's networks have a significant impact on our lives, changing the way we live, work, and play. Today's networks and, in a larger context, the Internet allow people to communicate, collaborate, and interact in ways they never did before. We use the network in a variety of ways, including web applications, ***IP*** telephony, videoconferencing, interactive gaming, electronic commerce, education, and more.

At the center of the network is the ***router***. Routers are used to connect multiple networks. The router is responsible for the delivery of ***packets*** across different networks. The destination of the IP packet can be a web server in another country or an e-mail server on the local-area network. It is the router's responsibility to deliver those packets in a timely manner. The effectiveness of internetwork communications for a large part depends on the ability of the routers to forward packets in the most efficient way possible. Whether it is a packet sent between two LANs within a company's intranetwork or a packet sent thousands of miles away to a remote network in another country, it is the router that forwards the packet from network to network, from sending host to destination host.

Routers are even being added to satellites in space. These routers will have the ability to route IP traffic between satellites in space in much the same way that packets are moved on earth, therefore reducing delays and offering greater networking flexibility.

The services that a router provides go well beyond those of just packet forwarding. Because of the demands on today's network, the router also is used for

- Ensuring 24/7 (24 hours a day, 7 days a week) availability to help guarantee network reachability using alternate paths in case the primary path fails
- Providing integrated services of data, video, and voice over wired and wireless networks using quality of service (QoS) prioritization of IP packets to ensure that real-time traffic, such as voice and video or critical data, is not dropped or delayed
- Mitigating the impact of worms, viruses, and other attacks on the network by permitting or denying the forwarding of packets

All this is built around the router and its capability to forward packets from one network to the next, from the original source to the final destination. It is only because of the router's capability to route packets between networks that devices on different networks can communicate. This chapter introduces you to the router, its role in the networks, its main hardware and software components, and the routing process itself.

Inside the Router

A router is a computer and has many of the common hardware components found on other types of computers. A router also includes an operating system. Examining some of the basic hardware and software components will give you a better understanding of the routing and packet-forwarding process.

Routers Are Computers

A router is a computer, just like any other computer, including a PC. The first router, which was used for the Advanced Research Projects Agency Network (ARPANET), was the IMP (Interface Message Processor). The IMP was a Honeywell 516 minicomputer that brought the ARPANET to life on August 30, 1969.

The ARPANET was developed by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense. The ARPANET was the world's first operational packet-switching network and the predecessor of today's Internet.

Figure 1-1 shows the front side of a Cisco 1800 series Integrated Services Router, which is the recommended router for use with this course. Routers have many of the same hardware and software components that are found in other computers, including

- CPU
- ***RAM***
- ***ROM***
- ***Operating system***

Figure 1-1 Cisco 1841 Integrated Services Router

Routers Are at the Network Center

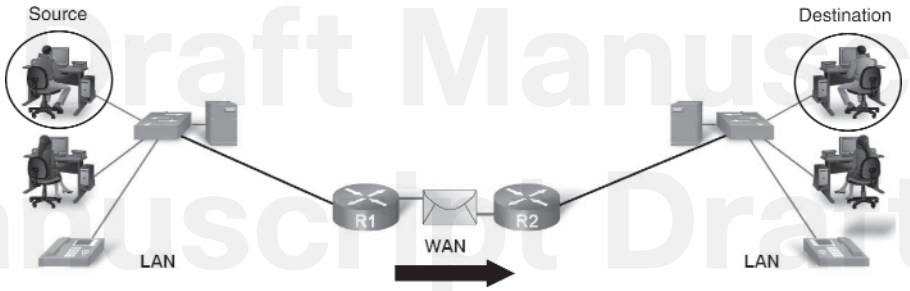
A typical user might be unaware of the presence of numerous routers in his or her own network or in the Internet. Users expect to be able to access web pages, send e-mails, and download music, whether the server they are accessing is on their own network or on another network halfway around the world. However, networking professionals know that it is the router that is responsible for forwarding packets from network to network, from the original source to the final destination.

A router connects multiple networks. This means that it has interfaces that belong to different IP networks. When a router receives an IP packet on one interface, it determines which interface to forward the packet on its way to its destination. The interface that the router uses to forward the packet can be the network of the final destination of the packet (the network with the destination IP address of this packet), or it can be a network connected to another router that is used to reach the destination network.

Each network that a router connects to typically requires a separate interface. These interfaces are used to connect a combination of both ***local-area networks (LAN)*** and ***wide-area networks (WAN)***. LANs are commonly ***Ethernet*** networks that contain devices such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area. For example, a WAN connection is commonly used to connect a LAN to the ***Internet service provider (ISP)*** network.

Figure 1-2 shows that Routers R1 and R2 are responsible for receiving the packet on one network and forwarding the packet out another network toward the packet's destination network.

Figure 1-2 What Is a Router?



Routers direct packets to their proper destination.
Routers connect different media.

Routers Determine the Best Path

The router's primary responsibility is to forward packets destined for local and remote networks by

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

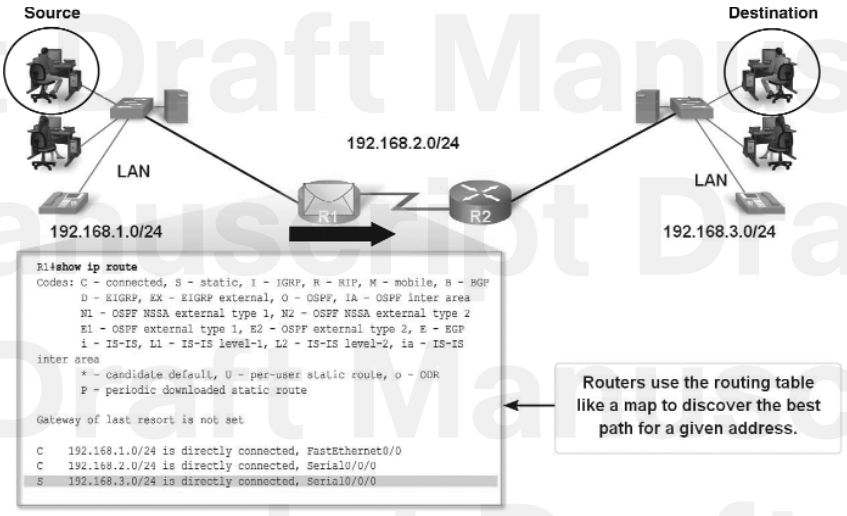
The router uses its ***routing table*** to determine the best path to forward the packet. When the router receives a packet, it examines the destination IP address and searches for the best match with a network address in the router's routing table. The routing table will include the interface to be used to forward the packet. When a match is found, the router encapsulates the IP packet into the data-link frame of the outgoing or exit interface, and the packet is then forwarded toward its destination.

A router will likely receive a packet encapsulated in one type of data-link frame, such as an Ethernet frame, and when forwarding the packet, encapsulate it in a different type of data-link frame, such as ***Point-to-Point Protocol (PPP)***. The data-link encapsulation depends on the type of interface on the router and the type of medium to which it connects. The different data-link technologies that a router connects to can include LAN technologies, such as

Ethernet, and WAN ***serial*** connections, such as a T1 connection using PPP, ***Frame Relay***, and ***Asynchronous Transfer Mode (ATM)***.

In Figure 1-3, notice that it is the router's responsibility to find the destination network in its routing table and forward the packet toward the destination. In the figure, R1 receives the packet encapsulated in an Ethernet frame. After decapsulating the packet, the router uses the destination IP address of the packet to search the routing table for a matching network address. R2 found the static route 192.168.3.0/24, which can be reached out its Serial 0/0/0 interface. R2 will encapsulate the packet in a frame format appropriate for the outbound interface and then forward the packet.

Figure 1-3 Routers Determine the Best Path



Static routes and ***dynamic routing protocols*** are used by routers to learn about remote networks and build their routing tables. This is the primary focus of the course. It will be discussed in detail in later chapters, along with the process routers use in searching their routing tables and forwarding the packets.

More Info

Visit websites such as http://www.howstuffworks.com, http://www.techweb.com/encyclopedia, and http://whatis.techtarget.com to see the definitions of a router and related terms.

Today's router is much more than just a packet-forwarding and network-interconnecting device. Modern routers incorporate many other features, such as security, QoS, and voice functionalities. Routers play an important role in the current trend toward ***unified communications***. To learn more about Cisco unified communications, see http://www.cisco.com/go/unifiedcommunications _solutions_unified_communications_home.html.

Packet Tracer Activity

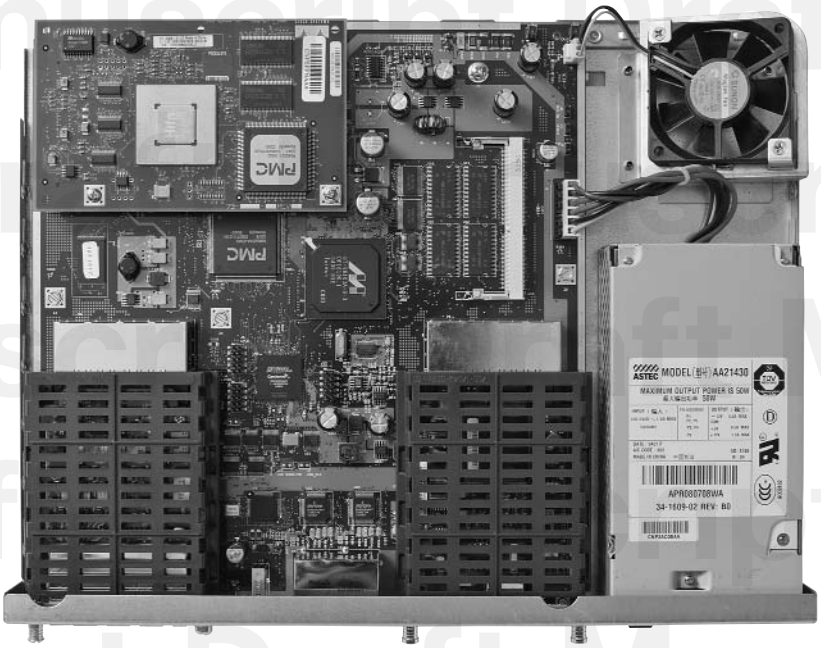
Corporate Network Simulation (1.1.1)

This Packet Tracer Activity shows a complex network of routers with many different technologies. Be sure to view the activity in simulation mode so that you can see the traffic traveling from multiple sources to multiple destinations over various types of ***media***. Detailed instructions are provided within the activity. Use file e2-111.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Router CPU and Memory

Although there are several different types and models of routers, every router has the same general hardware components. Depending on the model, those components are located in different places inside the router. Figure 1-4 shows the inside of an 1841 router. To see the internal router components, you must unscrew the metal cover and take it off the router. Usually you do not need to open the router unless you are upgrading memory.

Figure 1-4 Inside a Router



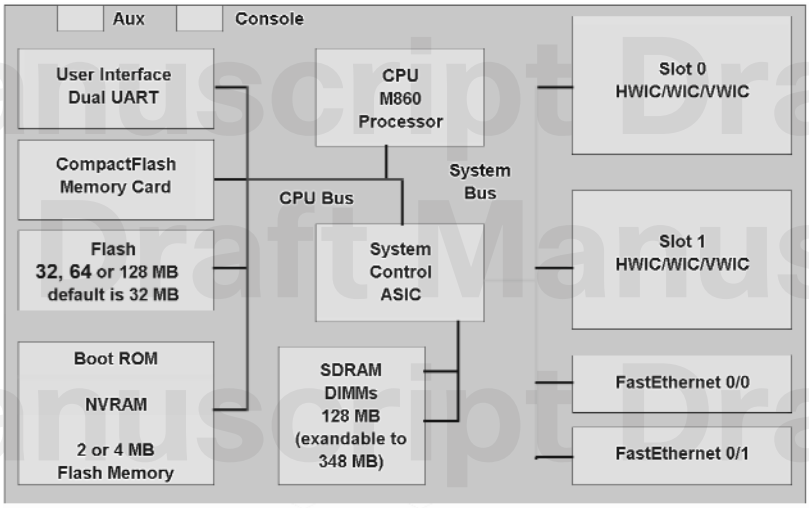
Similar to a PC, a router also includes

- Central processing unit (CPU)
- Random-access memory (RAM)
- Read-only memory (ROM)

- Flash memory
- NVRAM

Figure 1-5 is a schematic of the hardware components of an 1841 router.

Figure 1-5 Hardware Components of a Router



CPU

The CPU executes operating system instructions, such as system initialization, routing functions, and network interface control.

RAM

Similar to other computers, RAM stores the instructions and data needed to be executed by the CPU. RAM is used to store

- **Operating system:** Cisco IOS (Internetwork Operating System) is copied into RAM during bootup.
- **Running configuration file:** This is the configuration file that stores the configuration commands that the router's IOS is currently using. With few exceptions, all commands configured on the router are stored in the running configuration file known as the running-config.
- **IP routing table:** This is the file that stores information about directly connected and remote networks.

- ***ARP* cache:** This cache stores IP address–to–*MAC address* mappings, similar to the ARP cache on a PC. ARP cache would be used on routers that have Ethernet interfaces.
- **Packet buffering:** Packets are temporarily stored in a buffer when received on an interface or before they exit an interface.

RAM is volatile memory and loses its contents when the router is powered down or restarted. For this reason, the router also contains permanent storage areas such as ROM, flash, and NVRAM.

ROM

ROM is a form of permanent storage. Cisco devices use ROM to store

- Bootstrap instructions
- Basic diagnostic software
- Scaled-down version of IOS

ROM uses firmware, which is software embedded inside the integrated circuit. Firmware, such as the bootup instructions, does not normally need to be modified or upgraded. Many of these features, including ROM monitor software, will be discussed in a later course. ROM does not lose its contents when the router loses power or is restarted.

Flash Memory

Flash memory is nonvolatile computer memory that can be electrically erased and reprogrammed. Flash is used as permanent storage for the operating system, Cisco IOS. In most models of Cisco routers, the IOS is permanently stored in flash memory and copied into RAM during the bootup process. Flash consists of single in-line memory modules (SIMM) or PC cards (PCMCIA cards), which can be upgraded to increase the amount of flash memory.

Flash memory does not lose its contents when the router loses power or is restarted.

NVRAM

NVRAM is nonvolatile random-access memory, which does not lose its information when the power is turned off. This is in contrast to the most common forms of RAM such as DRAM, which requires continual power to maintain its information. NVRAM is used by Cisco IOS Software as permanent storage for the startup configuration file (startup-config). All configuration changes are stored in the running-config file in RAM and, with few exceptions, are implemented immediately by the IOS. To save those changes in case the router is restarted or loses power, the running-config file must be copied to NVRAM, where it is stored as the startup-config file. NVRAM retains its contents even when the router is powered off.

ROM, RAM, NVRAM, and flash are discussed in the following sections, which introduce IOS and the bootup process. They are also discussed in more detail in a later course with regard to managing IOS.

For a networking professional, it is more important to understand the *function* of the main internal components of a router than the exact location of those components inside a particular model of router. Physical architecture differs among the models.

More Info

View the "Cisco 1800 Series Portfolio Multimedia Demo" at http://www.cisco.com/en/US/products/ps5875/index.html.

Internetwork Operating System (IOS)

The operating system software used in Cisco routers is known as Cisco Internetwork Operating System (IOS). Like any operating system on any other computer, Cisco IOS Software is responsible for managing the hardware and software resources of the router, including allocating memory, managing processes and security, and managing file systems. Cisco IOS is a multitasking operating system that is integrated with routing, switching, internetworking, and telecommunications functions.

Although the Cisco IOS might appear to be the same on many routers, there are many different IOS images. An IOS image is a file that contains the entire IOS for that router. Cisco creates many different IOS images, depending on the model and the features within the IOS. Typically, additional features require more flash and RAM to store and load the IOS. For example, some features can include the ability to run Internet Protocol version 6 (***IPv6***) or a routing protocol such as Intermediate System–to–Intermediate System (***IS-IS***).

As with other operating systems, Cisco IOS has its own user interface. Although some routers provide a GUI (graphical user interface), the CLI (command-line interface) is a much more common method of configuring Cisco routers and is used throughout this curriculum.

Upon bootup, the startup-config file in NVRAM is copied into RAM and stored as the running-config file. IOS executes the configuration commands in the running-config file. Any changes entered by the network administrator are stored in the running-config file and immediately implemented by the IOS. In this chapter, we will review some of the basic IOS commands used to configure a Cisco router. In later chapters, you will learn the commands used to configure, verify, and troubleshoot ***static routing*** and various routing protocols, such as Routing Information Protocol (***RIP***), Enhanced Interior Gateway Routing Protocol (***EIGRP***), and Open Shortest Path First (***OSPF***).

Note

Cisco IOS is discussed in more detail in a later course.

Router Bootup Process

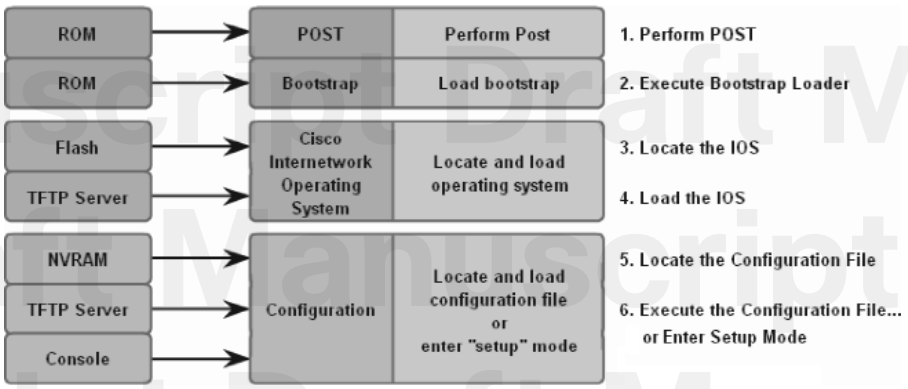
Like all computers, a router uses a systematic process to boot. This involves testing the hardware, loading the operating system software, and performing any saved configuration commands in the startup configuration file. Some of the details of this process have been excluded and are examined more completely in a later course.

Bootup Process

Figure 1-6 shows the six major phases in the bootup process:

1. POST: Testing the router hardware
2. Loading the bootstrap program
3. Locating Cisco IOS
4. Loading Cisco IOS
5. Locating the configuration file
6. Loading the startup configuration file or entering ***setup mode***

Figure 1-6 How a Router Boots Up



Step 1: Performing the POST

A ***power-on self test (POST)*** is a common process that occurs on most every computer during bootup. The POST process is used to test the router hardware. When the router is powered on, software on the ROM chip conducts the POST. During this self test, the router

executes diagnostics from ROM on several hardware components, including the CPU, RAM, and NVRAM. After the POST has been completed, the router executes the bootstrap program.

Step 2: Loading the Bootstrap Program

After the POST, the bootstrap program is copied from ROM into RAM. When the bootstrap program is in RAM, the CPU executes the instructions in the bootstrap program. The main task of the bootstrap program is to locate the Cisco IOS and load it into RAM.

At this point, if you have a console connection to the router, you will begin to see output on the screen.

Step 3: Locating Cisco IOS

The bootstrap program is responsible for locating the Cisco IOS and copying it into RAM. The IOS is typically stored in flash memory, but it can be stored in other places such as a TFTP (Trivial File Transfer Protocol) server.

If a full IOS image cannot be located, a scaled-down version of the IOS is copied from ROM into RAM. This version of IOS is used to help diagnose any problems and can be used to load a complete version of the IOS into RAM.

Note

A TFTP server is typically used as a backup server for IOS, but it can also be used as a central point for storing and loading the IOS. IOS management and using the TFTP server are discussed in a later course.

Step 4: Loading Cisco IOS

Some of the older Cisco routers ran the IOS directly from flash, but current models copy the IOS into RAM for execution by the CPU. When the IOS begins to load, you might see a string of pounds signs (#) while the image decompresses.

Step 5: Locating the Configuration File

After the IOS is loaded, the bootstrap program searches for the startup configuration file, known as the startup-config file, in NVRAM. This file has the previously saved configuration commands and parameters, including the following:

- Interface addresses
- Routing information

- Passwords
- Any other configurations saved by the network administrator

If the startup configuration file, startup-config, is located in NVRAM, it is then copied into RAM as the running configuration file, running-config.

Note

If the startup configuration file does not exist in NVRAM, the router can search for a TFTP server. If the router detects that it has an active link to another configured router, it will send a broadcast searching for a configuration file across the active link. This condition will cause the router to pause, but you will eventually see a console message like the following:

```
<router pauses here while it broadcasts for a configuration file across an
  active link>
%Error opening tftp://255.255.255.255/network-confg (Timed out)
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
```

Step 6: Loading the Startup Configuration File or Entering Setup Mode

If a startup configuration file is found in NVRAM, the IOS loads it into RAM as the running-config file and executes the commands in the file one line at a time. The running-config commands contain interface addresses, start routing processes, configure router passwords, and define other characteristics of the router.

If the startup configuration file cannot be located, the router will prompt the user to enter setup mode. Setup mode is a series of questions prompting the user for basic configuration information. Setup mode is not intended to enter complex router configurations, nor is it commonly used by network administrators. Setup mode will not be used in this course.

When booting a router that does not contain a startup configuration file, you will see the following question after the IOS has been loaded:

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

Setup mode will not be used in this course to configure the router. When prompted to enter setup mode, always answer **no**. If you answer **yes** and enter setup mode, you can press **Ctrl-C** at any time to terminate the setup process.

When setup mode is not used, IOS will create a default running-config file. The default running-config file is a basic configuration file that includes the router interfaces, management interfaces, and certain default information. The default running-config file does not contain any interface addresses, routing information, passwords, or other specific configuration information.

Command-Line Interface

Depending on the platform and IOS, the router might ask the following question before displaying the prompt:

```
Would you like to terminate autoinstall? [yes]: <Enter>

Press the Enter key to accept the default answer.

Router>
```

If a startup configuration file was found, the running configuration can include a host name, which means that the prompt will display the host name of the router.

After the prompt is displayed, the router is now running IOS with the current running configuration file. The network administrator can now begin using IOS commands on this router.

Note

The bootup process is discussed in more detail in a later course.

Verifying Router Bootup Process

The **show version** command can be used to help verify and troubleshoot some of the basic hardware and software components of the router. The **show version** command in Example 1-1 displays information about the version of Cisco IOS Software currently running on the router, the version of the bootstrap program, and information about the hardware configuration, including the amount of system memory.

Example 1-1 show version Command Output

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"
```

```
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

The output from the **show version** command includes information about the following:

- IOS version
- ROM bootstrap program
- Location of IOS
- CPU and amount of RAM
- Interfaces
- Amount of NVRAM
- Amount of flash
- Configuration register information

The sections that follow dissect these pieces of information in further detail.

IOS Version

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
```

This is the version of Cisco IOS Software in RAM and being used by the router.

ROM Bootstrap Program

```
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
```

This is the version of the system bootstrap software, stored in ROM, that was initially used to boot up the router.

Location of IOS

```
System image file is "flash:c2600-i-mz.122-28.bin"
```

This is the location from which the boostrap program located and loaded the Cisco IOS, along with the complete filename of the IOS image.

CPU and Amount of RAM

```
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
```

The first part of this line displays the type of CPU on this router. The last part of this line displays the amount of DRAM. Some series of routers like the 2600 use a fraction of DRAM as packet memory. Packet memory is used for buffering packets.

You must add both numbers to find out the total amount of DRAM on the router. In this example, the Cisco 2621 router has 60,416 KB (kilobytes) of free DRAM used for temporarily storing the Cisco IOS and other system processes. The other 5120 KB is dedicated to packet memory. Adding the two numbers gives you 60,416 KB + 5120 KB = 65,536 KB, or 64 megabytes (MB), of total DRAM.

It might be necessary to upgrade the amount of RAM when upgrading the IOS.

Interfaces

```
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
```

This section of the output displays the physical interfaces on the router. In this example, the Cisco 2621 router has two Fast Ethernet interfaces and two low-speed serial interfaces.

Amount of NVRAM

```
32K bytes of non-volatile configuration memory.
```

This is the amount of NVRAM on the router. NVRAM is used to store the startup-config file.

Amount of Flash

```
16384K bytes of processor board System flash (Read/Write)
```

This is the amount of flash memory on the router. Flash is used to permanently store the Cisco IOS. It might be necessary to upgrade the amount of flash when upgrading the IOS.

Configuration Register

```
Configuration register is 0x2102
```

The last line of the **show version** command displays the current configured value of the software configuration register in hexadecimal. If a second value is displayed in parentheses, this is the configuration register value that will be used during the next reload.

The configuration register has several uses, including password recovery. The factory default setting for the configuration register is 0x2102. This value indicates that the router will attempt to load a Cisco IOS Software image from flash memory and load the startup configuration file from NVRAM.

Note

The configuration register is discussed in more detail in a later course.

Packet Tracer Activity

Using Setup Mode (1.1.4)

Setup mode is available when a router is started for the first time to provide a basic configuration for the router. Packet Tracer supports only basic management setup. This limits you to configuring only a single interface that can connect to a management system to supply the remainder of the configuration. In this activity, R2 is an existing router already added to the network. You will clear any existing configuration and use setup mode to connect R2 to another router. Detailed instructions are provided within the activity. Use file e2-114.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

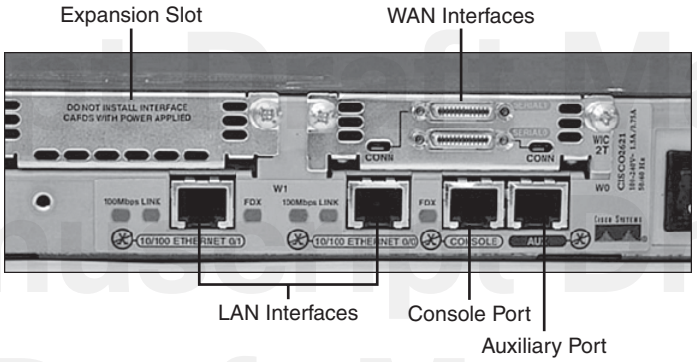
Router Ports and Interfaces

Although there are no "hard and fast" rules, the term *port*, when referring to a router, normally means one of the management ports used for administrative access. The term *interface* normally refers to interfaces that are capable of sending and receiving user traffic. However, these terms are often used interchangeably in the industry and even with IOS output.

Management Ports

Figure 1-7 shows the back side of a 2621 router. Routers have management ports, which are physical connectors used to manage the router. Management ports are not used for packet forwarding like Ethernet and serial interfaces. The most common of the management ports is the ***console port***. The console port is used to connect a terminal, or most likely a PC running terminal emulator software, to configure the router without the need for network access to that router. The console port must be used during initial configuration of the router.

Figure 1-7 Router Interfaces: Physical Representation



Each individual interface connects to a different network;
thus, each interface has an IP address/mask from that network.

Another management port is the auxiliary (AUX) port. Not all routers have auxiliary ports. At times, the auxiliary port can be used similarly to a console port but can also be used to attach a modem. Auxiliary ports will not be used in this curriculum.

Router Interfaces

The term *interface* on Cisco routers refers to a physical connector on the router whose main purpose is to receive and forward packets. Routers have multiple interfaces used to connect to multiple networks. It is common that the interfaces will connect to various types of networks, which means different types of media and connectors. Often a router will need to have different types of interfaces. For example, a router will most likely have Fast Ethernet interfaces for connections to different LANs and also have different types of WAN interfaces used to connect a variety of serial links, including T1, ***DSL***, and ***ISDN***. Figure 1-8 shows the Fast Ethernet and serial interfaces on the router.

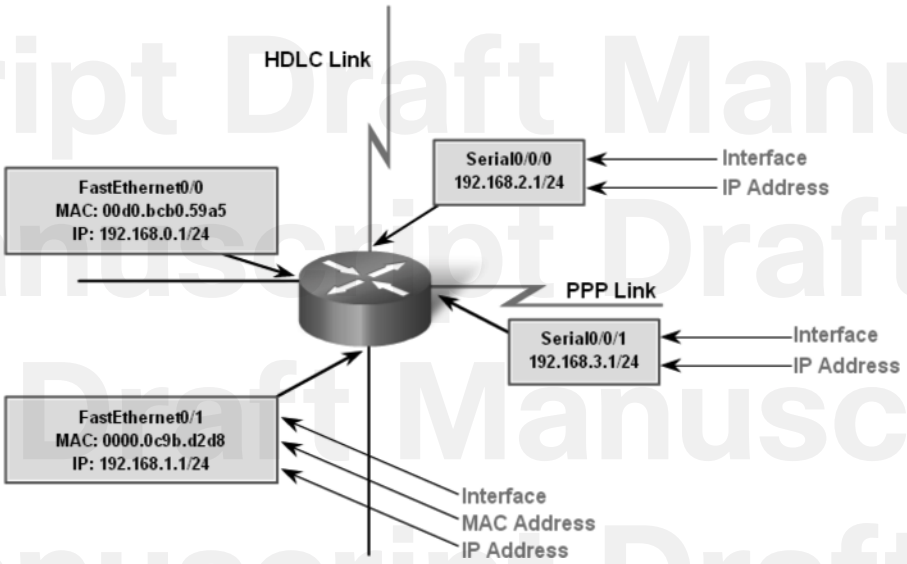
Like the interfaces on a PC, the ports and interfaces on a router are located on the outside of the router. This makes sense, because the appropriate network ***cable*** and connector will need to be connected to this interface.

Note

A single interface on a router can be used to connect to multiple networks; however, this is beyond the scope of this course and is discussed in a later course.

Like most networking devices, Cisco routers use light emitting diode (***LED***) indicators to provide status information. An interface LED indicates the activity of the corresponding interface. If an LED is off when the interface is active and the interface is correctly connected, this might be an indication of a problem with that interface. If an interface is extremely busy, its LED will always be on. Depending on the router, there might be other LEDs as well.

Figure 1-8 Router Interfaces: Logical Representation



More Info

For more information on reading LEDs on the 1841 series routers, see "Troubleshooting Cisco 1800 Series Routers (Modular)" at http://www.cisco.com/en/US/products/ps5853/products_installation_guide_chapter09186a00802c36b8.html.

Interfaces Belong to Different Networks

Every interface on the router belongs to a different network. In other words, each interface is a host on a different IP network, as shown previously in Figure 1-8. Each interface must be configured with an IP address and subnet mask of a different network. Cisco IOS will not allow two active interfaces on the same router to belong to the same network.

Router interfaces can be divided into two major groups:

- **LAN interfaces**, such as Ethernet and Fast Ethernet interfaces. As the name indicates, LAN interfaces are used to connect the router to the LAN, similar to how a PC's Ethernet network interface card (***NIC***) is used to connect the PC to the Ethernet LAN. Like a PC's Ethernet NIC, a router's Ethernet interface also has a Layer 2 MAC address and participates in the Ethernet LAN the same way as any other ***hosts*** on that LAN. For example, a router's Ethernet interface participates in the Address Resolution Protocol (ARP) process for that LAN. The router will maintain an ARP cache for that interface, send ARP requests when needed, and respond with ARP replies when required.

A router's Ethernet interface typically uses an RJ-45 jack that supports unshielded twisted-pair (UTP) cabling. When a router is connected to a switch, a straight-through cable is used. When two routers are connected directly through the Ethernet interfaces, or when a PC's NIC is connected directly to a router's Ethernet interface, a crossover cable is used.

- **WAN interfaces**, such as serial, ISDN, and Frame Relay interfaces. WAN interfaces are used to connect routers to external networks, usually over a larger geographical distance. The Layer 2 encapsulation can be different types including PPP, Frame Relay, and HDLC (High-Level Data Link Control). Similar to LAN interfaces, each WAN interface has its own IP address and subnet mask, making it a member of a specific network. Remember, MAC addresses are used only on Ethernet interfaces and are not on WAN interfaces. However, WAN interfaces use their own Layer 2 addresses depending on the technology. Layer 2 WAN encapsulation types and addresses are covered in a later course.

Example of Router Interfaces

The router in Figure 1-8 has four interfaces. Each interface has a Layer 3 IP address and subnet mask that configures it for a different network. The Ethernet interfaces also have Layer 2 Ethernet MAC addresses.

The WAN interfaces are using different Layer 2 encapsulations. Serial 0/0/0 is using HDLC and Serial 0/0/1 is using PPP. Both of these serial point-to-point protocols use a broadcast address for the Layer 2 destination address when encapsulating the IP packet into a data-link frame.

In the lab environment, you are restricted to how many LAN and WAN interfaces you can use to configure "hands-on" labs. With Packet Tracer, however, you have the flexibility to create more complex network designs.

Packet Tracer Activity

Cabling Devices (1.1.5.3)

To successfully complete this activity, you must select the proper cables to connect the various devices. Detailed instructions are provided within the activity. Use file e2-1153.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Packet Tracer Activity

Using Packet Tracer Device Tabs (1.1.5.4)

The configuration window in Packet Tracer for Cisco devices, such as routers and switches, consists of three tabs. The Physical tab is used to add and remove modules. The Config tab is used to configure Packet Tracer–specific settings and a limited number of other settings. The CLI tab is used to configure all the settings supported by Packet Tracer. The CLI tab simulates the command-line interface of a Cisco IOS device. In this activity, you will add a router to the lab topology, install a module, configure the router using the Config tab, and

complete the configuration using the CLI tab. Detailed instructions are provided within the activity. Use file e2-1154.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Routers and the Network Layer

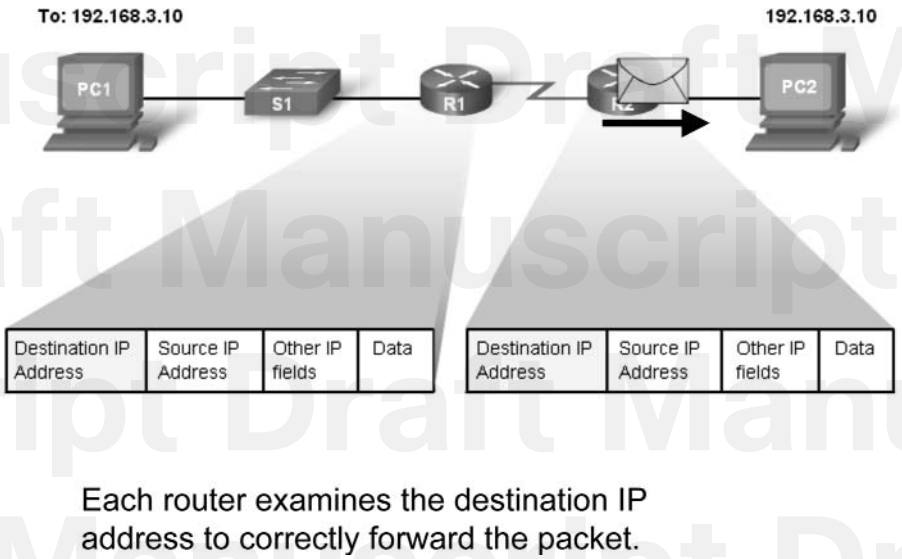
The key to understanding the role of a router in the network is to understand that a router is a Layer 3 device responsible for forwarding packets. However, a router also operates at Layers 1 and 2.

Routing Is Forwarding Packets

The main purpose of a router is to connect multiple networks and forward packets destined for its own networks or other networks. A router is considered a Layer 3 device because its primary forwarding decision is based on the information in the Layer 3 IP packet, specifically the destination IP address. This is known as routing.

When a router receives a packet, it examines the destination IP address. If the destination IP address does not belong to any of the router's directly connected networks, the router must forward this packet to another router. In Figure 1-9, R1 examines the packet's destination IP address and, after searching the routing table, forwards the packet onto R2. When R2 receives the packet, it also examines the packet's destination IP address and, after searching its routing table, forwards the packet out its directly connected Ethernet network to PC2.

Figure 1-9 Packet Forwarding



When each router receives a packet, it searches the routing table to find the best match between the destination IP address of the packet and one of the network addresses in the routing table. When a match is found, the packet is encapsulated in the Layer 2 data-link frame for that outgoing interface. The type of data-link encapsulation depends on the type of interface, such as Ethernet or HDLC.

Eventually the packet reaches a router, where the destination IP address of the packet belongs to the same network as one of the router's directly connected interfaces. In this example, Router R2 receives the packet from R1. R2 forwards the packet out its Ethernet interface, which belongs to the same network as the destination device, PC2.

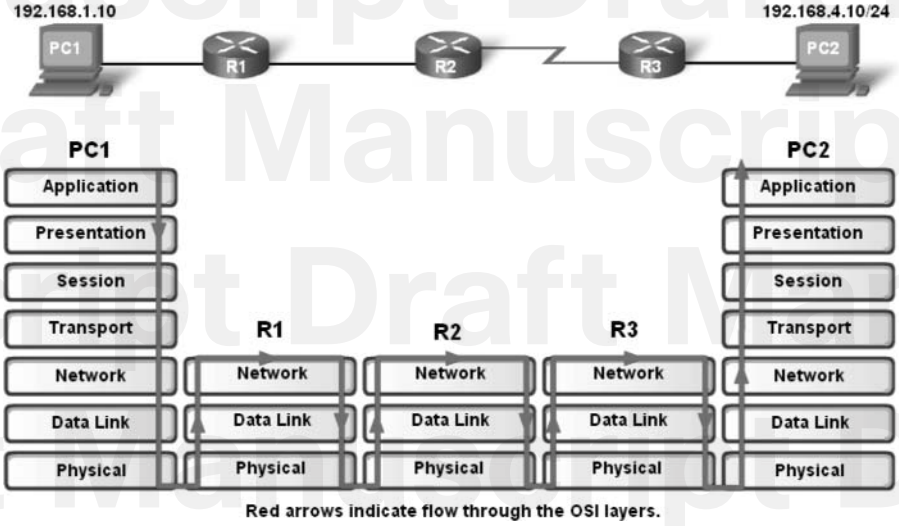
This sequence of events is explained in more detail later in this chapter.

Routers Operate at Layers 1, 2, and 3

A router makes its primary forwarding decision at Layer 3, but as you saw earlier, it also participates in Layer 1 and Layer 2 processes as well. After a router has examined the destination IP address of a packet and consulted its routing table to make its forwarding decision, it can then forward that packet out the appropriate interface toward its destination. The router will encapsulate the Layer 3 IP packet into the data portion of a Layer 2 data-link frame appropriate for the exit interface. This can be an Ethernet frame, an HDLC frame, or some other Layer 2 encapsulation, depending on the encapsulation used on that particular interface. The Layer 2 frame will then be encoded into the Layer 1 physical signals used to represent these bits over the physical link.

To understand this better, refer to Figure 1-10. Notice that PC1 operates at all seven layers, encapsulating the data and sending the frame out as a stream of encoded bits to R1, its default *gateway*.

Figure 1-10 Routers Operate at Layers 1, 2, and 3



R1 receives the stream of encoded bits on its interface. The bits are decoded and passed up to Layer 2, where R1 decapsulates the frame. The router examines the destination address of the data-link frame to determine whether it matches the receiving interface, including a broadcast or multicast address. If there is a match, the data portion of the frame, the IP packet, is then passed up to Layer 3, where R1 makes its routing decision. R1 then reencapsulates the packet into a new Layer 2 data-link frame and forwards it out the outbound interface as a stream of encoded bits. The new Layer 2 data-link address is associated with that of the interface of the next-hop router.

R2 then receives the stream of bits, and the process repeats itself. R2 decapsulates the frame and passes the data portion of the frame, the IP packet, to Layer 3, where R2 makes its routing decision. R2 then reencapsulates the packet into a new Layer 2 data-link frame and forwards it out the outbound interface as a stream of encoded bits.

This process is repeated once again by Router R3, where R3 forwards the IP packet, encapsulated inside a data-link frame and encoded as bits to PC2.

Each router in the path from source to destination performs this same process of decapsulation, searching the routing table, and then reencapsulation. This process is important to your understanding of how routers participate in networks. Therefore, we will revisit this discussion in more depth in a later section.

CLI Configuration and Addressing

The basic addressing and configuration of Cisco devices was covered in a previous course. However, we will spend some time reviewing these topics as well as preparing you for the hands-on lab experience in this course.

Implementing Basic Addressing Schemes

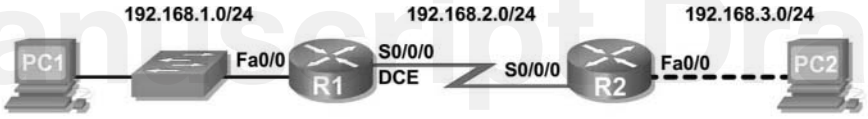
When designing a new network or mapping an existing network, it is important to document the network. As a starting point, the documentation should include a topology map of the network and an addressing table that lists the following information:

- Device names
- Interface
- IP address and subnet mask
- Default gateway address for end devices such as PCs

Populating an Address Table

Figure 1-11 shows the topology used for the rest of the chapter, with devices interconnected and configured with IP addresses. Below the network topology in the figure is a table used to document the network. The table is populated with the data documenting the network (devices, IP addresses, subnet masks, and interfaces).

Figure 1-11 Documenting an Addressing Scheme



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.1 68.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Packet Tracer Activity

Connecting and Identifying Devices (1.2.1)

Use the Packet Tracer Activity to connect the devices and configure the device names, and use the "Place Note" feature to add network address labels. Detailed instructions are provided within the activity. Use file e2-121.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer. Detailed instructions are provided within the activity.

Basic Router Configuration

When configuring a router, certain basic tasks are performed, including the following:

- Naming the router
- Setting passwords
- Configuring interfaces
- Configuring a banner
- Saving changes on a router
- Verifying basic configuration and router operations

You should already be familiar with these commands. However, this section will provide a brief review with the assumption that the router does not have a current startup-config file.

The first prompt is at user mode:

```
Router>
```

User mode will allow you to view the state of the router but will not allow you to modify its configuration. Don't confuse "user mode" with "users of the network." "User mode" is intended for the network technicians, operators, and engineers who have the responsibility to configure network devices.

The **enable** command is used to enter ***privileged EXEC mode***. This mode allows the user to make configuration changes on the router. The router prompt will change from a > to a # in this mode:

```
Router> enable
Router#
```

Host Name and Passwords

Table 1-1 shows the basic router configuration command syntax used to configure R1 in the following example. You can open Packet Tracer Activity 1.2.2 and follow along or wait until the end of this section to open it.

Table 1-1 Basic Router Configuration Command Syntax

Naming the router	`Router(config)# hostname name`

Setting passwords	`Router(config)# enable secret password`
	`Router(config)# line console 0`
	`Router(config-line)# password password`
	`Router(config-line)# login`
	`Router(config)# line vty 0 4`
	`Router(config-line)# password password`
	`Router(config-line)# login`

Configuring a message-of-the-day banner	`Router(config)# banner motd # message #`

Configuring an interface	`Router(config)# interface type number`
	`Router(config-if)# ip address address mask`
	`Router(config-if)# description description`
	`Router(config-if)# no shutdown`

Saving changes on a router	`Router# copy running-config startup-config`

Examining the output of **show** commands	`Router# show running-config`
	`Router# show ip route`
	`Router# show ip interface brief`
	`Router# show interfaces`

First, enter global configuration mode:

```
Router# config t
```

Next, apply a unique host name to the router:

```
Router(config)# hostname R1
```

Now, configure a password that is to be used to enter privileged EXEC mode. In our lab environment, we will use the password **class**. However, in production environments, routers should have strong passwords. See the links at the end of this section for more information on creating and using strong passwords.

```
R1(config)# enable secret class
```

Next, configure the console and *Telnet* lines with the password **cisco**. Once again, the password **cisco** is used only in our lab environment. The **login** command enables password checking on the line. If you do not enter the **login** command on the console line, the user will be granted access to the line without entering a password. The console commands follow:

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
```

The Telnet lines use similar commands:

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

Configuring a Banner

From global configuration mode, configure the message-of-the-day (MOTD) banner. A delimiting character such as a # is used at the beginning and at the end of the message. The delimiter allows you to configure a multiline banner as shown here:

```
R1(config)# banner motd #

Enter TEXT message.  End with the character '#'.
**************************************
WARNING!! Unauthorized Access Prohibited!!
**************************************
#
```

Configuring an appropriate banner is part of a good security plan. At a minimum, a banner should warn against unauthorized access. A good security policy would prohibit configuring a banner that "welcomes" an unauthorized user.

Router Interface Configuration

You will now configure the individual router interfaces with IP addresses and other information. First, enter interface configuration mode by specifying the interface type and number. Next, configure the IP address and subnet mask:

```
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
```

It is good practice to configure a description on each interface to help document the network information. The description text is limited to 240 characters. On production networks, a description can be helpful in troubleshooting by providing information about the type of network the interface is connected to and whether any other routers are on that network. If the interface connects to an ISP or service carrier, it is helpful to enter the third party's connection and contact information. For example:

```
Router(config-if)# description Circuit#VBN32696-123 (help desk:1-800-555-1234)
```

In lab environments, enter a simple description that will help in troubleshooting situations. For example:

```
R1(config-if)# description Link to R2
```

After configuring the IP address and description, the interface must be activated with the **no shutdown** command. This is similar to powering on the interface. The interface must also be connected to another device (a hub, a switch, another router, and so on) for the physical layer to be active.

```
R1(config-if)# no shutdown
```

Note

When cabling a point-to-point serial link in our lab environment, one end of the cable is marked DTE and the other end is marked DCE. The router that has the DCE end of the cable connected to its serial interface will need the additional **clock rate** command configured on that serial interface, as follows:

```
R1(config-if)# clock rate 64000
```

This step is only necessary in a lab environment and will be explained in more detail in Chapter 2, "Static Routing."

Repeat the interface configuration commands on all other interfaces that need to be configured. In our example topology, the Fast Ethernet interface needs to be configured:

```
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# description R1 LAN
R1(config-if)# no shutdown
```

Each Interface Belongs to a Different Network

At this point, note that each interface must belong to a different network. Although IOS allows you to configure an IP address from the same network on two different interfaces, the router will not activate the second interface.

For example, what if you attempt to configure the FastEthernet 0/1 interface on R1 with an IP address on the 192.168.1.0/24 network? FastEthernet 0/0 has already been assigned an address on that same network. If you attempt to configure another interface, FastEthernet 0/1, with an IP address that belongs to the same network, you will get the following message:

```
R1(config)# interface FastEthernet0/1
R1(config-if)# ip address 192.168.1.2 255.255.255.0
192.168.1.0 overlaps with FastEthernet0/0
```

If there is an attempt to enable the interface with the **no shutdown** command, the following message will appear:

```
R1(config-if)# no shutdown

192.168.1.0 overlaps with FastEthernet0/0
FastEthernet0/1: incorrect IP address assignment
```

In Example 1-2, notice that the **show ip interface brief** command output displays the second interface configured for the 192.168.1.0/24 network, FastEthernet 0/1, is still down.

Example 1-2 show ip interface brief Command Output

```
R1# show ip interface brief

Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  192.168.1.1    YES manual up                    up
Serial0/0        192.168.2.1    YES manual up                    up
FastEthernet0/1  192.168.1.2    YES manual administratively down down
Serial0/1        unassigned     YES unset  administratively down down
```

More Info

For discussions about using strong passwords, see the following articles:

- "Strong passwords: How to create and use them" at http://www.microsoft.com/athome/security/privacy/password.mspx
- "Simple formula for strong passwords" at http://www.sans.org/reading_room/whitepapers/authentication/1636.php

Verifying Basic Router Configuration

All the previous basic router configuration commands entered were immediately stored in the running configuration file of R1. The running-config file is stored in RAM and is the configuration file used by IOS. Verify the commands entered by displaying the running configuration with the **show running-config** command, as shown in Example 1-3.

Example 1-3 show running-config Command Output

```
R1# show running-config

!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
****************************************
WARNING!! Unauthorized Access Prohibited!!
****************************************
^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

Now that the basic configuration commands have been entered, it is important to save the running-config file to nonvolatile memory, the router's NVRAM. In case of a power outage or an accidental reload, the router will be able to boot with the current configuration. After

the router's configuration has been completed and tested, it is important to save the running-config file to the startup-config file as the permanent configuration file:

```
R1# copy running-config startup-config
```

After applying and saving the basic configuration, several commands will help you verify that you have correctly configured the router. All of these commands are discussed in detail in later chapters. For now, begin to become familiar with the output.

The **show running-config** command displays the current running configuration that is stored in RAM. With a few exceptions, any configuration commands that were used will be entered into the running-config file and implemented immediately by IOS.

The **show startup-config** command, demonstrated in Example 1-4, displays the startup configuration file stored in NVRAM. This is the configuration that the router will use on the next reboot. This configuration does not change unless the current running configuration is saved to NVRAM with the **copy running-config startup-config** command.

Example 1-4 show startup-config Command Output

```
R1# show startup-config

Using 728 bytes
!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
****************************************
WARNING!! Unauthorized Access Prohibited!!
****************************************
^C
line con 0
 password cisco
 login
```

```
line vty 0 4
 password cisco
 login
!
end
```

When comparing the output from the **show running-config** and **show startup-config** commands, notice that the startup configuration and the running configuration are identical. They are identical because the running configuration has not changed since the last time it was saved. Also notice that the **show startup-config** command displays how many bytes of NVRAM the saved configuration is using: 728 bytes in Example 1-4.

The **show ip route** command, demonstrated in Example 1-5, displays the routing table that IOS is currently using to choose the best path to its destination networks. At this point, R1 only has routes for its directly connected networks, its own interfaces.

Example 1-5 show ip route Command Output

```
R1# show ip route

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

Gateway of last resort is not set

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

The **show interfaces** command, demonstrated in Example 1-6, displays all the interface configuration parameters and statistics. Some of this information will be discussed in later chapters and in later courses.

Example 1-6 `show interfaces` Command Output

```
R1# show interfaces

<some interfaces not shown>
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0007.eca7.1511 (bia 00e0.f7e4.e47e)
  Description: R1 LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

The **show ip interface brief** command, demonstrated in Example 1-7, displays abbreviated interface configuration information, including IP address and interface status. This command is a useful tool for troubleshooting and is quick way to determine the status of all router interfaces.

Example 1-7 show ip interface brief Command Output

```
R1# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0              192.168.2.1     YES manual up                    up
Serial0/1              unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Packet Tracer Activity

Configure and Verify R1 (1.2.2)

In this activity, all devices on the network are configured with the exception of R1. You will configure R1 and then verify the configuration. Detailed instructions are provided within the activity. Use file e2-122.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Building the Routing Table

The primary function of a router is to forward packets toward their destination network, the destination IP address of the packet. To do this, a router needs to search the routing information stored in its routing table. In the following sections, you will learn how a router builds the routing table. Then, you will learn the three basic routing principles.

Introducing the Routing Table

A routing table is a data file in RAM that is used to store route information about directly connected and remote networks. The routing table contains network/next-hop associations that tell a router that a particular destination can be optimally reached by sending the packet to a particular router representing the "next hop" on the way to the final destination. The ***next-hop*** association can also be the outgoing or exit interface to the final destination.

The network/exit interface association can represent the destination network address of the IP packet. This would be one of the router's directly connected networks.

A directly connected network is a network that is directly attached to one of the router interfaces. When a router's interface is configured with an IP address and subnet mask, the interface becomes a host on that attached network. The network address and subnet mask of the interface, along with the interface type and number, are entered into the routing table as a directly connected network. When a router forwards a packet to a host such as a web server, that host is on the same network as a router's directly connected network.

A remote network is a network that is not directly connected to the router. In other words, a remote network is a network that can only be reached by sending the packet to another router. Remote networks are added to the routing table using a dynamic routing protocol or by configuring static routes. Dynamic routes are routes to remote networks that were learned automatically by the router, using a dynamic routing protocol. Static routes are routes to networks that a network administrator manually configured.

Note

The routing table—with its directly connected networks, static routes, and dynamic routes—will be introduced in the following sections and discussed in even greater detail throughout this course.

The following analogies can help clarify the concept of connected, static, and dynamic routes:

- **Directly connected routes:** To visit a ***neighbor***, you only have to go down the street on which you already live. This path is similar to a directly connected route because the "destination" is available directly through your "connected interface"—the street.
- **Static routes:** A train uses the same railroad tracks every time for a specified route. This path is similar to a static route because the path to the destination is always the same.
- **Dynamic routes:** When driving a car, you can "dynamically" choose a different path based on traffic, weather, or other conditions. This path is similar to a dynamic route because you can choose a new path at many different points on your way to the destination.

show ip route Command

You can use the **show ip route** command to display the routing table for a router, as demonstrated in Example 1-8.

Example 1-8 Connected Routes in the Routing Table

```
R1# show ip route

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

Gateway of last resort is not set

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

At this point, no static routes have been configured nor any dynamic routing protocols enabled. Therefore, the routing table for R1 only shows the router's directly connected networks. For each network listed in the routing table, the following information is included:

- **C:** The information in this column denotes the source of the route information, directly connected network, static route, or a dynamic routing protocol. The **C** represents a directly connected route.
- **192.168.1.0/24:** This is the network address and subnet mask of the directly connected or remote network. In this example, both entries in the routing table, 192.168.1./24 and 192.168.2.0/24, are directly connected networks.
- **FastEthernet 0/0:** The information at the end of the route entry represents the exit interface and/or the IP address of the next-hop router. In this example, both FastEthernet 0/0 and Serial 0/0/0 are the exit interfaces used to reach these networks.

When the routing table includes a route entry for a remote network, additional information is included, such as the routing ***metric*** and the ***administrative distance***. Routing metrics, administrative distance, and the **show ip route** command are explained in more detail in later chapters.

PCs also have a routing table. In Example 1-9, you can see the **route print** command output. The command reveals the configured or acquired default gateway and connected, loopback, multicast, and broadcast networks.

Example 1-9 route print Command Output in Windows

```
C:\> route print

===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 11 25 af 40 9b ...... Intel(R) PRO/1000 MT Mobile Connection
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.1      10
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0      192.168.1.1     192.168.1.1      10
     192.168.1.10    255.255.255.0        127.0.0.1     192.168.1.1      10
        224.0.0.0        240.0.0.0      192.168.1.10    192.168.1.10      10
  255.255.255.255  255.255.255.255      192.168.1.10    192.168.1.10       1
Default Gateway:     192.168.1.1
===========================================================================
Persistent Routes:
  None
```

The output from the **route print** command will not be analyzed during this course. It is shown here to emphasize the point that all IP-configured devices should have a routing table. The **route –n** command is a similar command used with Linux operating systems.

Directly Connected Networks

When a router's interface is configured with an IP address and subnet mask, that interface becomes a host on that network. When the FastEthernet 0/0 interface on R1 is configured with the IP address 192.168.1.1 and the subnet mask 255.255.255.0, the FastEthernet 0/0 interface is now a member of the 192.168.1.0/24 network. Hosts that are attached to the same LAN, like PC1, are also configured with an IP address that belongs to the 192.168.1.0/24 network.

When a PC is configured with a host IP address and subnet mask, the PC uses the subnet mask to determine what network it now belongs to. This is done by the operating system

performing an AND operation using the host IP address and subnet mask. A router uses the same logic when an interface is configured.

A PC is normally configured with a single host IP address because it only has a single network interface, usually an Ethernet NIC. Routers have multiple interfaces; therefore, each interface must be a member of a different network. In Example 1-10, R1 is a member of two different networks: 192.168.1.0/24 and 192.168.2.0/24. Although not shown in the example, R2 is also a member of two networks: 192.168.2.0/24 and 192.168.3.0/24.

Example 1-10 Connected Routes in the Routing Table for R1

```
R1# show ip route

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

Gateway of last resort is not set

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

After the router's interface is configured and the interface is activated with the **no shutdown** command, the interface must receive a carrier signal from another device (another router, switch, hub, and so on) before the interface state is considered as "up." After the interface is up, the network of that interface is added to the routing table as a directly connected network.

Before any static or dynamic routing is configured on a router, the router only knows about its own directly connected networks. These are the only networks that are displayed in the routing table until static or dynamic routing is configured. Directly connected networks are of prime importance for routing decisions. Static and dynamic routes cannot exist in the routing table without a router's own directly connected networks. The router cannot send packets out an interface if that interface is not enabled with an IP address and subnet mask, just as a PC cannot send IP packets out its Ethernet interface if that interface is not configured with an IP address and subnet mask.

Note

The process of configuring router interfaces and adding the network address to the routing table is discussed in the following chapter.

Packet Tracer Activity

Directly Connected Routes (1.3.2)

This activity focuses on the routing table and how it is built. A router builds routing tables by first adding the networks for the IP addresses configured on its own interfaces. These networks are the directly connected networks for the router. The focus of this activity is two routers, R1 and R2, and the networks supported through the configuration of the router interfaces. Initially, all interfaces have been configured with correct addressing, but the interfaces are shut down. Detailed instructions are provided within the activity. Use file e2-132.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Static Routing

Remote networks are added to the routing table by configuring static routes or enabling a dynamic routing protocol. When the IOS routing process learns about a remote network and the interface it will use to reach that network, it adds that route to the routing table as long as the exit interface is enabled.

A static route includes the network address and subnet mask of the remote network, along with the IP address of the next-hop router or exit interface. Static routes are denoted with the code S in the routing table, as shown in Example 1-11. Static routes are examined in detail in the next chapter.

Example 1-11 Static Route in the Routing Table for R1

```
R1# show ip route

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

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

When to Use Static Routes

Static routes should be used in the following cases:

- **A network consists of only a few routers.** Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing can add more administrative overhead.
- **A network is connected to the Internet only through a single ISP.** There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.
- **A large network is configured in a hub-and-spoke topology.** A ***hub-and-spoke*** topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using a dynamic routing protocol would be unnecessary because each branch only has one path to a given destination: through the central location.

Typically, most routers' routing tables contain a combination of static routes and dynamic routes. But, as stated earlier, the routing table must first contain the directly connected networks used to access these remote networks before any static or dynamic routing can be used.

Packet Tracer Activity

Static Routing (1.3.3)

Routers can learn of remote networks through static or dynamic routing. This activity focuses on how remote networks are added to the routing table using static routes. Detailed instructions are provided within the activity. Use file e2-133.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Dynamic Routing

Remote networks can also be added to the routing table by using a dynamic routing protocol. In Example 1-12, R1 has automatically learned about the 192.168.4.0/24 network from R2 through the dynamic routing protocol RIP (Routing Information Protocol). RIP was one of the first IP routing protocols and will be fully discussed in later chapters.

Example 1-12 Dynamic Route in the Routing Table for R1

```
R1# show ip route

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

continues

continued

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:20, Serial0/0/0
```

Note

In Example 1-12, R1's routing table shows that R1 has learned about two remote networks, one route dynamically using RIP and a static route that was manually configured. This is an example of how routing tables can contain routes learned dynamically and configured statically and is not necessarily representative of the best configuration for this network.

Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including the following:

- Network discovery
- Updating and maintaining routing tables

Automatic Network Discovery

Network discovery is a routing protocol's capability to share information about the networks it knows about with other routers that are also using the same routing protocol. Instead of configuring static routes to remote networks on every router, a dynamic routing protocol allows the routers to automatically learn about these networks from other routers. These networks and the best path to each network are added to the router's routing table and denoted as a network learned by a specific dynamic routing protocol.

Maintaining Routing Tables

After the initial network discovery, dynamic routing protocols will also update and maintain the networks in their routing tables. Dynamic routing protocols not only make a best-path determination to various networks but also determine a new best path if the initial path

becomes unusable (or if the topology changes). For these reasons, dynamic routing protocols have an advantage over static routes. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator.

IP Routing Protocols

There are several dynamic routing protocols for IP. Here are some of the more common dynamic routing protocols for routing IP packets:

- RIP (Routing Information Protocol)
- ***IGRP*** (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System–to–Intermediate System)
- ***BGP*** (Border Gateway Protocol)

Note

RIP (versions 1 and 2), EIGRP, and OSPF are covered in this course. EIGRP and OSPF are also covered in more detail in CCNP, along with IS-IS and BGP. IGRP is a legacy routing protocol and has been replaced by EIGRP. Both IGRP and EIGRP are Cisco-proprietary routing protocols, whereas all other routing protocols listed are nonproprietary protocols based on open standards.

Remember, in most cases, routers contain a combination of static routes and dynamic routes in the routing tables. Dynamic routing protocols will be discussed in more detail in Chapter 3, "Introduction to Dynamic Routing Protocols."

Packet Tracer Activity

Dynamic Routing (1.3.4)

Use the Packet Tracer Activity to learn how IOS installs and removes dynamic routes. Detailed instructions are provided within the activity. Use file e2-134.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Routing Table Principles

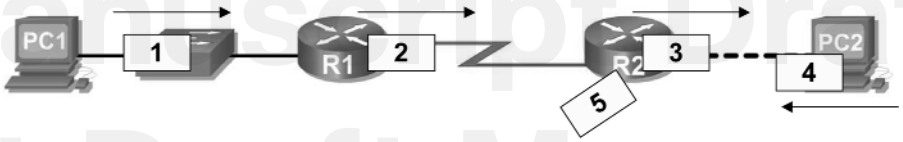
At times in this course, we will refer to three principles regarding routing tables that will help you understand, configure, and troubleshoot routing issues. These principles, listed as follows, are from Alex Zinin's book, *Cisco IP Routing*[1]:

- Every router makes its decision alone, based on the information it has in its own routing table.

- The fact that one router has certain information in its routing table does not mean that other routers have the same information.
- Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.

What is the effect of these principles? Consider the example in Figure 1-12.

Figure 1-12 Routing Principle Example



1. PC1 Sends ping to PC2.
2. R1 has a route to PC2's network.
3. R2 is directly connected to PC2's network.
4. PC2 sends reply ping to PC1.
5. R2 does NOT have a route to PC1's network so it drops the packet

After making its routing decision, R1 forwards the packet destined for PC2 to R2. R1 only knows about the information in its own routing table, which indicates that Router R2 is the next-hop router. R1 does not know whether R2 actually has a route to the destination network.

It is the network administrator's responsibility to make sure that all routers within their control have complete and accurate routing information so that packets can be forwarded between any two networks. This can be done using static routes, a dynamic routing protocol, or a combination of both.

Because R2 is directly connected to the destination network, it was able to forward the packet to PC2. However, the packet from PC2 to PC1 was dropped by R2. Although R2 had information in its routing table about the destination network of PC1's original ping request, that does not mean it has the information for the return path to PC1's network.

Asymmetric Routing

Because routers do not necessarily have the same information in their routing tables, packets can traverse the network in one direction, using one path, and return through another path. This is called ***asymmetric routing***. Asymmetric routing is more common in the Internet, which uses the BGP routing protocol, than it is in most internal networks.

This example implies that when designing and troubleshooting a network, the network administrator should check the following:

- Is there a path from source to destination available in both directions?
- Is the path taken in both directions the same path? (Asymmetrical routing is not uncommon but sometimes can pose additional issues.)

Packet Tracer Activity

Routing Table Principles (1.3.5)

Use this activity to investigate a "black hole" routing scenario and then make configuration changes to correct the problem. Detailed instructions are provided within the activity. Use file e2-135.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Path Determination and Switching Functions

The following sections focus on exactly what happens to data as it moves from source to destination. First, these sections review the packet and frame field specifications, and then discuss in detail how the frame fields change from hop to hop, whereas the packet fields remain unchanged.

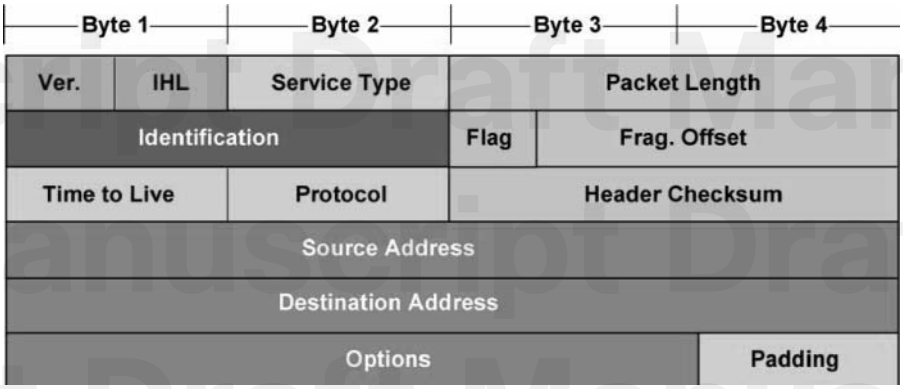
Packet Fields and Frame Fields

As previously discussed, routers make their primary forwarding decision by examining the destination IP address of a packet. Before sending that packet out the proper exit interface, the IP packet needs to be encapsulated into a Layer 2 data-link frame. In later sections, you will follow an IP packet from source to destination, examining the encapsulation and decapsulation process at each router. But first, you need to review the format of a Layer 3 IP packet and a Layer 2 Ethernet frame.

Internet Protocol (IP) Packet Format

The Internet Protocol specified in RFC 791 defines the IP packet format. As shown in Figure 1-13, the IP packet header has specific fields that contain information about the packet and about the sending and receiving hosts.

Figure 1-13 Field Specifications for the IP Header



The following list describes the fields in the IP header. You should already be familiar with destination IP address, source IP address, version, and ***Time to Live (TTL)*** fields. The other fields are important but are outside the scope of this course.

- **Version:** Version number (4 bits); predominant version is IP version 4 (IPv4).
- **IHL:** IP header length in 32-bit words (4 bits).
- **Service Type:** How the datagram should be handled (8 bits); the first 3 bits are precedence bits. (This use has been superseded by Differentiated Services Code Point [DSCP], which uses the first 6 bits [last 2 reserved].)
- **Packet Length:** Packet length (header + data) (16 bits).
- **Identification:** Unique IP datagram value (16 bits).
- **Flag:** Controls fragmenting (3 bits).
- **Frag. Offset:** Supports fragmentation of ***datagrams*** to allow differing maximum transmission units (MTU) in the Internet (13 bits).
- **Time to Live: (TTL)** Identifies how many routers can be traversed by the datagram before being dropped (8 bits).
- **Protocol:** Upper-layer protocol sending the datagram (8 bits).
- **Header Checksum:** Integrity check on the header (16 bits).
- **Source Address:** 32-bit source IP address (32 bits).
- **Destination Address:** 32-bit destination IP address (32 bits).
- **Options:** IP options for network testing, debugging, security, and others (multiple of 32 bits).

MAC Layer Frame Format

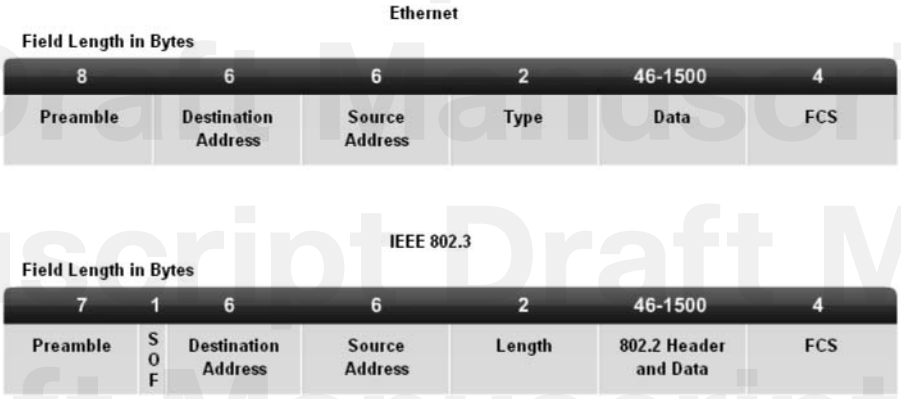
The Layer 2 data-link frame usually contains header information with a data-link source and destination address, trailer information, and the actual transmitted data. The data-link source address is the Layer 2 address of the interface that sent the data-link frame. The data-link destination address is the Layer 2 address of the interface of the destination device. Both the source and destination data-link interfaces are on the same network. As a packet is forwarded from router to router, the Layer 3 source and destination IP addresses will not change; however, the Layer 2 source and destination data-link addresses will change. This process will be examined more closely in later sections.

Note

When ***NAT*** (Network Address Translation) is used, the destination IP address does change, but this process is of no concern to IP and is a process performed within a company's network. Routing with NAT is discussed in a later course.

The Layer 3 IP packet is encapsulated in the Layer 2 data-link frame associated with that interface. In this example, we will show the Layer 2 Ethernet frame. Figure 1-14 shows the two compatible versions of Ethernet.

Figure 1-14 Field Specification for Ethernet Frames



The following list describes the fields in an Ethernet frame:

- **Preamble:** Seven bytes of alternating 1s and 0s, used to synchronize signals
- **Start of Frame (SOF) delimiter:** 1 byte signaling the beginning of the frame
- **Destination Address:** 6-byte MAC address of the sending device on the local segment
- **Source Address:** 6-byte MAC address of the receiving device on the local segment

- **Type/Length:** 2 bytes specifying either the type of upper-layer protocol (Ethernet II frame format) or the length of the data field (IEEE 802.3 frame format)
- **Data and Pad:** 46 to 1500 bytes of data; 0s used to pad any data packet less than 46 bytes
- **Frame Check Sequence (FCS):** 4 bytes used for a cyclic redundancy check to make sure that the frame is not corrupted

Best Path and Metrics

A router determines the best path by evaluating metrics.

Best Path

A router's best-path determination involves evaluating multiple paths to the same destination network and selecting the optimum or "shortest" path to reach that network. Whenever there are multiple paths to reach the same network, this means that each path uses a different exit interface on that router to reach that network. The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. Some routing protocols, such as RIP, use simple hop count, which is the number of routers between a router and the destination network. Other routing protocols, such as OSPF, determine the shortest path examining the bandwidth of the links, therefore using links with the fastest bandwidth from a router to the destination network.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. A metric is the quantitative value used to measure the distance to a given route. The best path to a network is the path with the lowest metric. For example, a router will prefer a path that is five hops away over a path that is ten hops away.

The primary objective of the routing protocol is to determine the best paths for each route to include in the routing table. The routing algorithm generates a value, a metric for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path. Some routing protocols can base route selection on multiple metrics, combining them into a single metric. The smaller the value of the metric, the better the path.

Comparing Hop Count and Bandwidth Metrics

Two metrics that are used by some dynamic routing protocols are

- **Hop count:** This is the number of routers that a packet must travel through before reaching its destination. Each router is equal to one hop. A hop count of 4 indicates that a packet must pass through four routers to reach its destination. If multiple paths are available to a destination, the routing protocol, such as RIP, picks the path with the least number of hops.

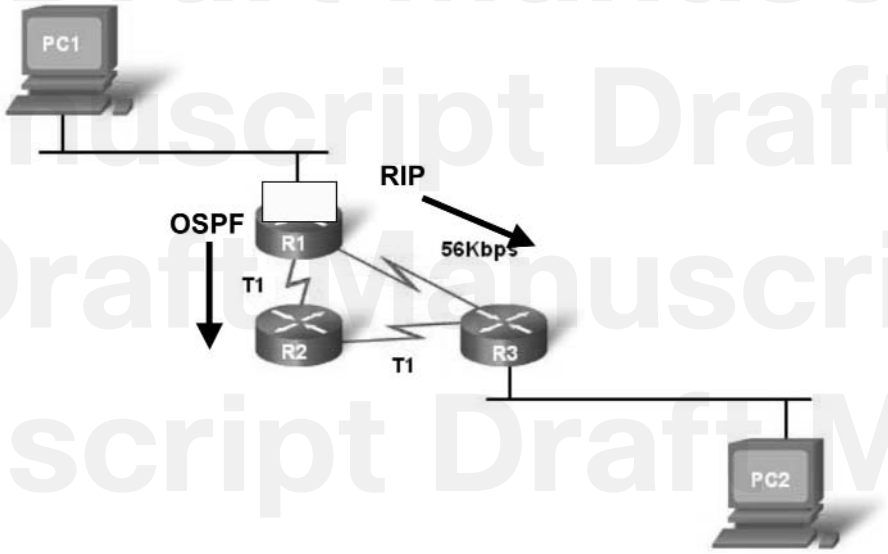
- **Bandwidth:** Bandwidth is the data capacity of a link, sometimes referred to as the "speed" of the link. For example, the Cisco implementation of the OSPF routing protocol uses bandwidth as its metric. The best path to a network is determined by the path that has an accumulation of links with the highest bandwidth values, that is, the fastest links. Chapter 11, "OSPF," explains the use of bandwidth in OSPF.

Note

"Speed" is technically not an accurate description because all bits travel at the same speed over the same physical medium. Bandwidth is more accurately defined as the number of bits that can be transmitted over that link per second.

When hop count is used as the metric, the resulting path can sometimes be suboptimal. For example, consider the network shown in Figure 1-15.

Figure 1-15 Hop Count Versus Bandwidth as a Metric



If RIP is the routing protocol used by the three routers, R1 will choose the suboptimal route through R3 to reach PC2 because this path has fewer hops. Bandwidth is not considered. However, if OSPF is used as the routing protocol, R1 will choose the route based on bandwidth. Packets will be able to reach their destination sooner using the two, faster T1 links as compared to the single, slower 56-kbps link.

Packet Tracer Activity

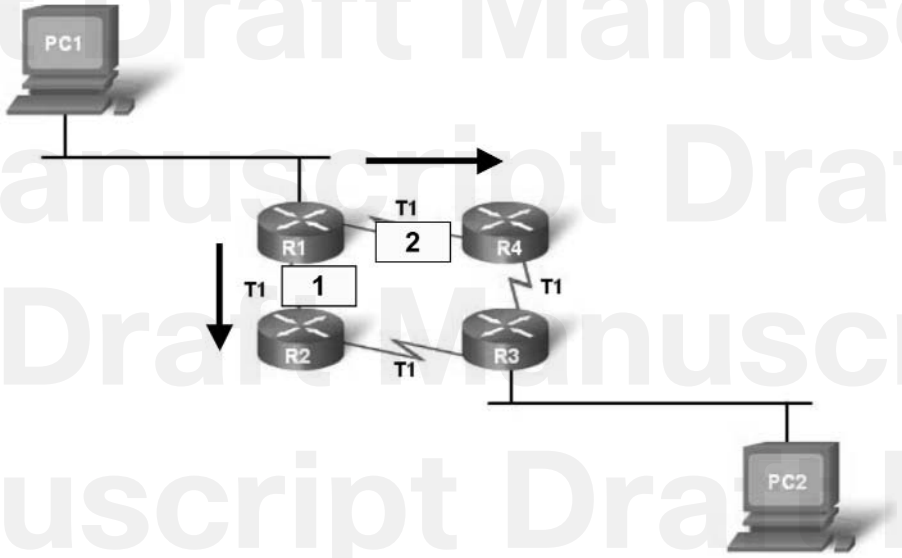
Determine Best Path Using Routing Tables (1.4.2)

Use the Packet Tracer Activity to investigate the contents of the IP and frame headers. Detailed instructions are provided within the activity. Use file e2-142.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Equal-Cost Load Balancing

You might be wondering what happens if a routing table has two or more paths with the same metric to the same destination network. When a router has multiple paths to a destination network and the value of that metric (hop count, bandwidth, and so on) is the same, this is known as an ***equal-cost metric***, and the router will perform ***equal-cost load balancing***, as shown in Figure 1-16. Because both paths to the destination have the same metric, R1 will send the first packet to R2 and the second packet to R4. The routing table will contain the single destination network but will have multiple exit interfaces, one for each equal-cost path. The router will forward packets using the multiple exit interfaces as listed in the routing table.

Figure 1-16 Equal-Cost Load Balancing



If configured correctly, load balancing can increase the effectiveness and performance of the network. Equal-cost load balancing can be configured to use both dynamic routing protocols and static routes. Equal-cost load balancing is discussed in more detail in Chapter 8, "The Routing Table: A Closer Look."

Equal-Cost Paths Versus Unequal-Cost Paths

Just in case you are wondering, a router can send packets over multiple networks even when the metric is not the same if it is using a routing protocol that has this capability. This is known as ***unequal-cost load balancing***. EIGRP (as well as IGRP) are the only routing

protocols that can be configured for unequal-cost load balancing. Unequal-cost load balancing in EIGRP is not discussed in any of the CCNA-related courses, but is covered in the CCNP-related courses.

Packet Tracer Activity

Equal-Cost Load Balancing (1.4.3)

Use the Packet Tracer Activity to explore a routing table that is using equal-cost load balancing. Detailed instructions are provided within the activity. Use file e2-143.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

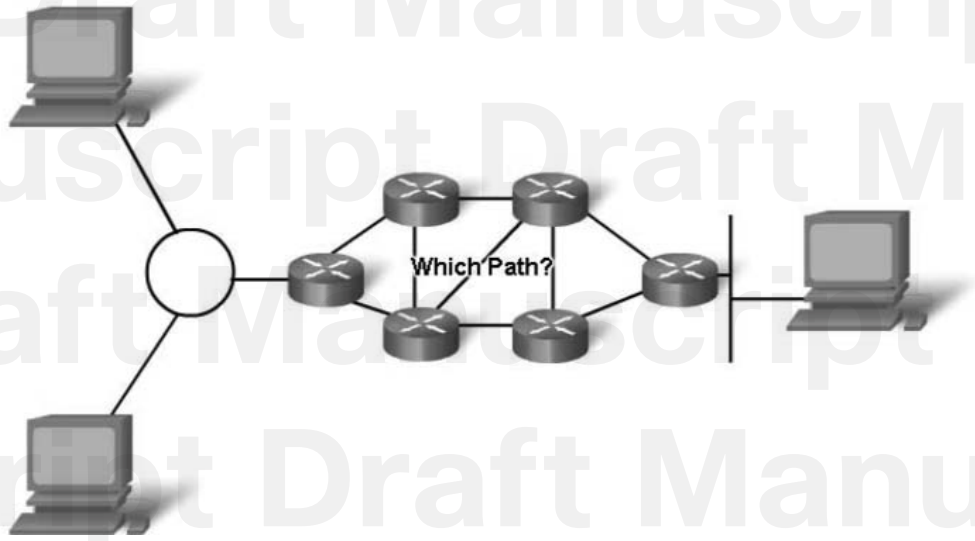
Path Determination

Packet forwarding involves two functions:

- Path determination function
- Switching function

The path determination function is the process of how the router determines which path to use when forwarding a packet, as illustrated in Figure 1-17. To determine the best path, the router searches its routing table for a network address that matches the packet's destination IP address.

Figure 1-17 Routers Determine the Best Path to the Destination



One of three path determinations results from this search:

- **Directly connected network:** If the destination IP address of the packet belongs to a device on a network that is directly connected to one of the router's interfaces, that packet is forwarded directly to that device. This means that the destination IP address of the packet is a host address on the same network as this router's interface.
- **Remote network:** If the destination IP address of the packet belongs to a remote network, the packet is forwarded to another router. Remote networks can only be reached by forwarding packets to another router.
- **No route determined:** If the destination IP address of the packet does not belong to either a connected or remote network, and the router does not have a default route, the packet is discarded. The router sends an Internet Control Message Protocol (ICMP) Unreachable message to the source IP address of the packet.

In the first two results, the router reencapsulates the IP packet into the Layer 2 data-link frame format of the exit interface. The type of Layer 2 encapsulation is determined by the type of interface. For example, if the exit interface is Fast Ethernet, the packet is encapsulated in an Ethernet frame. If the exit interface is a serial interface configured for PPP, the IP packet is encapsulated in a PPP frame.

The following section demonstrates this process.

More Info

For more information on how a router using Cisco IOS performs route lookup, see the Cisco Press book *Inside Cisco IOS Software Architecture*, by Vijay Bolapragada, Curtis Murphy, and Russ White.

Switching Function

After the router has determined the exit interface using the path determination function, the router needs to encapsulate the packet into the data-link frame of the outgoing interface.

The switching function is the process used by a router to accept a packet on one interface and forward it out another interface. A key responsibility of the switching function is to encapsulate packets in the appropriate data-link frame type for the outgoing data link.

What does a router do with a packet received from one network and destined for another network? The router performs the following three major steps:

1. Decapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer
2. Examines the destination IP address of the IP packet to find the best path in the routing table
3. Encapsulates Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface

As the Layer 3 IP packet is forwarded from one router to the next, the IP packet remains unchanged, with the exception of the TTL (Time to Live) field. When a router receives an IP packet, it decrements the TTL by 1. If the resulting TTL value is 0, the router discards the packet. The TTL is used to prevent IP packets from traveling endlessly over networks because of a routing loop or other misfunction in the network. Routing loops are discussed in a later chapter.

As the IP packet is decapsulated from one Layer 2 frame and encapsulated into a new Layer 2 frame, the data-link destination address and source address will change as the packet is forwarded from one router to the next. The Layer 2 data-link source address represents the Layer 2 address of the outbound interface. The Layer 2 destination address represents the Layer 2 address of the next-hop router. If the next hop is the final destination device, it will be the Layer 2 address of that device.

The packet might be encapsulated in a different type of Layer 2 frame than the one in which it was received. For example, the packet might be received by the router on a Fast Ethernet interface, encapsulated in an Ethernet frame, and forwarded out a serial interface, encapsulated in a PPP frame.

Remember, as a packet travels from the source device to the final destination device, the Layer 3 IP addresses do not change. However, the Layer 2 data-link addresses change at every hop as the packet is decapsulated and reencapsulated in a new frame by each router.

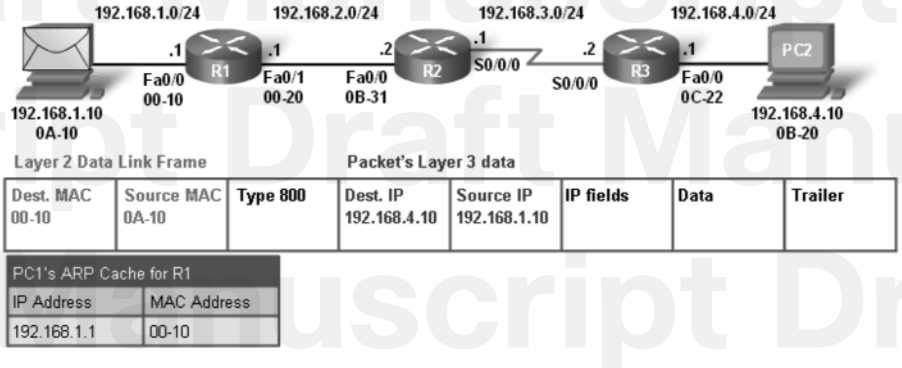
Path Determination and Switching Function Details

Can you describe the exact details of what happens to a packet at Layer 2 and Layer 3 as it travels from source to destination? If not, study Figures 1-18 through 1-23 along with the following discussion until you can describe the process on your own.

Step 1: PC1 Has a Packet to Be Sent to PC2

Refer to Figure 1-18. PC1 encapsulates the IP packet into an Ethernet frame with the destination MAC address of R1's FastEthernet 0/0 interface.

Figure 1-18 Day in the Life of a Packet: Step 1



How does PC1 know to forward the packet to R1 and not directly to PC2? PC1 has determined that the IP source and IP destination addresses are on different networks.

PC1 knows what network it belongs to by doing an AND operation on its own IP address and subnet mask, which results in its network address. PC1 does this same AND operation using the packet's destination IP address and PC1's subnet mask. If the result is the same as its own network, PC1 knows that the destination IP address is on its own network, and it does not need to forward the packet to the default gateway, the router. If the AND operation results in a different network address, PC1 knows that the destination IP address is not on its own network, and it must forward this packet to the default gateway, the router.

Note

If an AND operation with the packet's destination IP address and PC1's subnet mask results in a different network address than what PC1 has determined to be its own network address, this address does not necessarily reflect the actual remote network address. PC1 only knows that if the destination IP address is on its own network, the masks would be the same and the network addresses would be the same. The mask of the remote network can very well be a different mask. If the destination IP address results in a different network address, PC1 doesn't know the actual remote network address, only that it is not on its own network.

How does PC1 determine the MAC address of the default gateway, router R1? PC1 checks its ARP table for the IP address of the default gateway and its associated MAC address.

What if this entry does not exist in the ARP table? PC1 sends an ARP request, and Router R1 sends back an ARP reply.

Step 2: Router R1 Receives the Ethernet Frame

Router R1 examines the destination MAC address, which matches the MAC address of the receiving interface, FastEthernet 0/0. R1 will therefore copy the frame into its buffer.

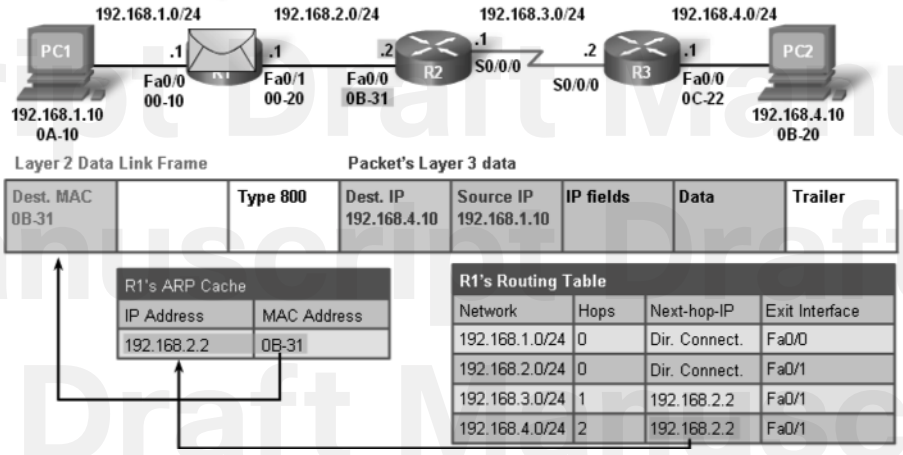
R1 sees that the Ethernet Type field is 0x800, which means that the Ethernet frame contains an IP packet in the data portion of the frame.

R1 decapsulates the Ethernet frame.

Because the destination IP address of the packet does not match any of R1's directly connected networks, the router consults its routing table to route this packet. As shown in Figure 1-19, R1 searches the routing table for a network address and subnet mask that would include this packet's destination IP address as a host address on that network.

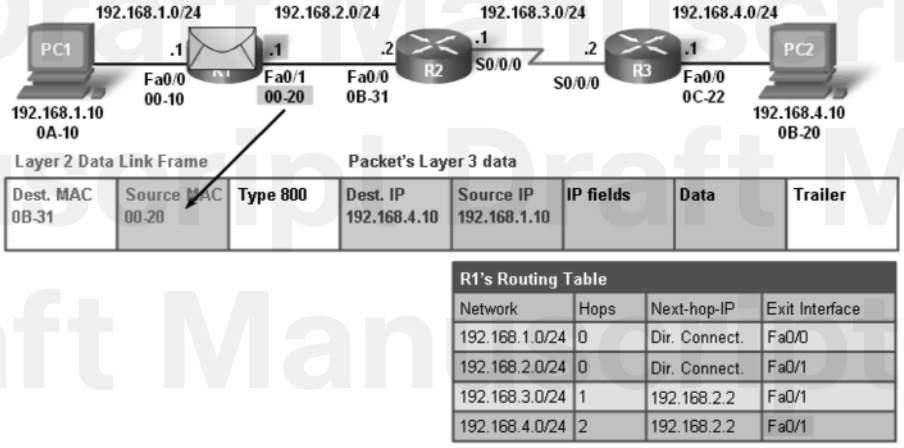
In this example, the routing table has a route for the 192.168.4.0/24 network. The destination IP address of the packet is 192.168.4.10, which is a host IP address on that network. R1's route to the 192.168.4.0/24 network has a next-hop IP address of 192.168.2.2 and an exit interface of FastEthernet 0/1. This means that the IP packet will be encapsulated in a new Ethernet frame, with the destination MAC address being that of the next-hop router's IP address. Because the exit interface is on an Ethernet network, R1 must resolve the next-hop IP address with a destination MAC address.

Figure 1-19 Day in the Life of a Packet: Step 2a



Refer to Figure 1-20. R1 looks up the next-hop IP address of 192.168.2.2 in its ARP cache for its FastEthernet 0/1 interface. If the entry is not in the ARP cache, R1 sends an ARP request out its FastEthernet 0/1 interface. R2 would then send back an ARP reply. R1 then updates its ARP cache with an entry for 192.168.2.2 and the associated MAC address.

Figure 1-20 Day in the Life of a Packet: Step 2b



The IP packet is now encapsulated into a new Ethernet frame and forwarded out R1's FastEthernet 0/1 interface.

Step 3: Packet Arrives at Router R2

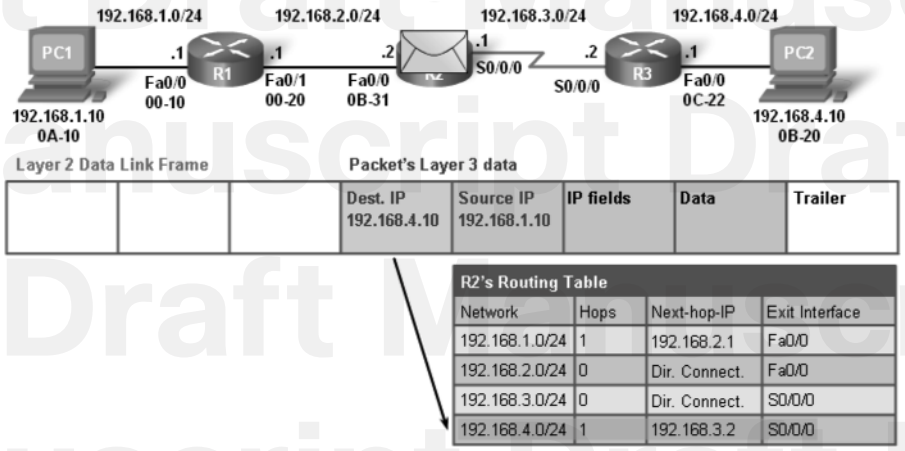
Router R2 examines the destination MAC address, which matches the MAC address of the receiving interface, FastEthernet 0/0. R1 will therefore copy the frame into its buffer.

R2 sees that the Ethernet Type field is 0x800, which means that the Ethernet frame contains an IP packet in the data portion of the frame.

R2 decapsulates the Ethernet frame.

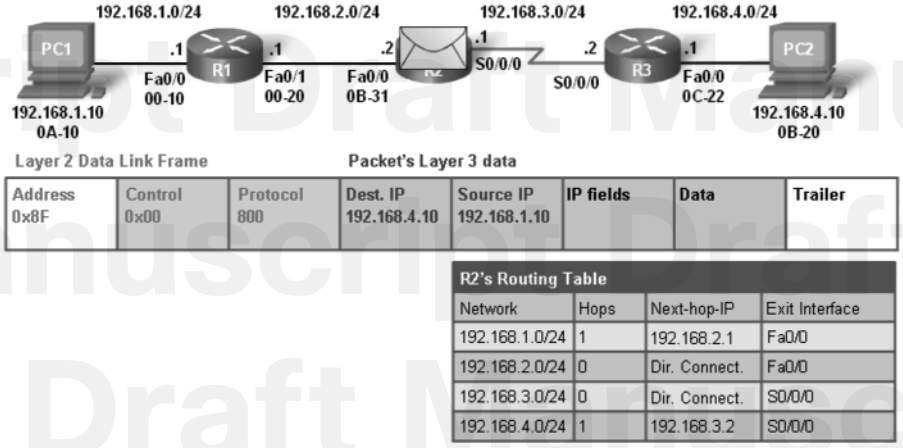
Because the destination IP address of the packet does not match any of R2's interface addresses, the router consults its routing table to route this packet. As shown in Figure 1-21, R2 searches the routing table for the packet's destination IP address using the same process as discussed in R1.

Figure 1-21 Day in the Life of a Packet: Step 3a



R2's routing table has a route to the 192.168.4.0/24 route, with a next-hop IP address of 192.168.3.2 and an exit interface of Serial 0/0/0. Because the exit interface is not an Ethernet network, R2 does not have to resolve the next-hop IP address with a destination MAC address. When the interface is a point-to-point serial connection, R2 encapsulates the IP packet into the proper data-link frame format used by the exit interface (HDLC, PPP, and so on). The Layer 2 encapsulation shown in Figure 1-22 is HDLC. Therefore, the data-link destination address is set to 0x8F. Remember, there are no MAC addresses on serial interfaces.

Figure 1-22 Day in the Life of a Packet: Step 3b



The IP packet is now encapsulated into a new data-link frame, PPP, and sent out the Serial 0/0/0 exit interface.

Step 4: Packet Arrives at R3

R3 receives and copies the data-link HDLC frame into its buffer.

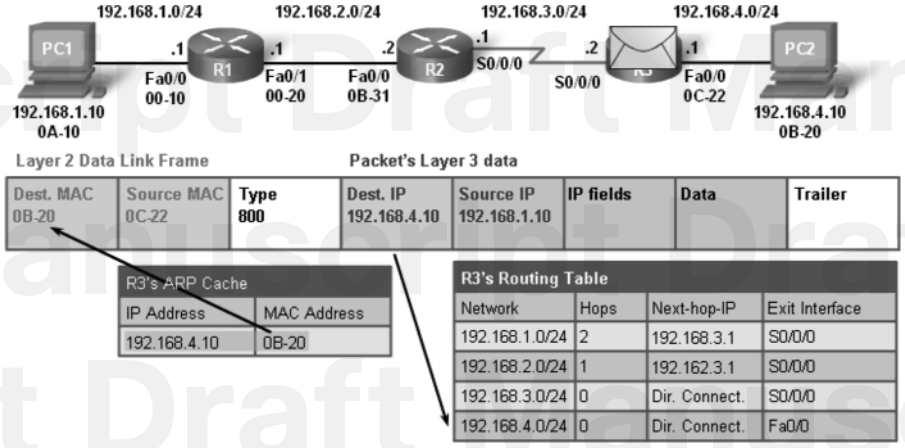
R3 decapsulates the data-link HDLC frame.

Refer to Figure 1-23. R3 searches the routing table for the destination IP address of the packet. The search of the routing table results in a network that is one of R3's directly connected networks. This means that the packet can be sent directly to the destination device and does not need to be sent to another router. Because the exit interface is a directly connected Ethernet network, R3 needs to resolve the destination IP address of the packet with a destination MAC address.

R3 searches for the packet's destination IP address of 192.168.4.10 in its ARP cache. If the entry is not in the ARP cache, R3 sends an ARP request out its FastEthernet 0/0 interface. PC2 sends back an ARP reply with its MAC address. R3 updates its ARP cache with an entry for 192.168.4.10 and the MAC address returned in the ARP reply.

The IP packet is encapsulated into a new data-link Ethernet frame and sent out R3's FastEthernet 0/0 interface.

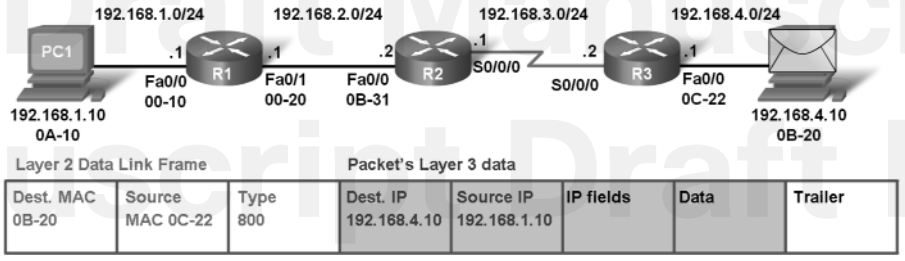
Figure 1-23 Day in the Life of a Packet: Step 4



Step 5: Ethernet Frame with Encapsulated IP Packet Arrives at PC2

Refer to Figure 1-24. PC2 examines the destination MAC address, which matches the MAC address of the receiving interface, that is, its own Ethernet NIC. PC2 will therefore copy the rest of the frame.

Figure 1-24 Day in the Life of a Packet: Step 5



PC2 sees that the Ethernet Type field is 0x800, which means that the Ethernet frame contains an IP packet in the data portion of the frame.

PC2 decapsulates the Ethernet frame and passes the IP packet to its operating system's IP process.

Path Determination and Switching Function Summary

We have just examined the encapsulation and decapsulation process of a packet as it is forwarded from router to router, from the originating source device to the final destination

device. We have also introduced the routing table lookup process, which will be discussed more thoroughly in a later chapter. You have seen that routers are not just involved in Layer 3 routing decisions, but also participate in Layer 2 processes, including encapsulation, and on Ethernet networks, ARP. Router interfaces also participate in Layer 1 used to transmit and receive the bits over the physical medium. Layer 1 is used to convert the bit stream into a physical signal, which then is transmitted over the cable or wireless medium.

Routing tables contain both directly connected networks and remote networks. It is because routers contain addresses for remote networks in their routing tables that routers know how and where to send packets destined for other networks, including the Internet. In the following chapters, you will learn how the routers build and maintain these routing tables, either by the use of manually entered static routes or through the use of a dynamic routing protocol.

More Info

For more information about how routers using Cisco IOS forward packets and the packet-switching mechanisms that exist, refer to the Cisco Press book *Inside Cisco IOS Software Architecture*, by Vijay Bolapragada, Curtis Murphy, Russ White.

Summary

This chapter introduced the router. Routers are computers and include many of the same hardware and software components found in a typical PC, such as CPU, RAM, ROM, and an operating system.

The main purpose of a router is to connect multiple networks and forward packets from one network to the next. This means that a router typically has multiple interfaces. Each interface is a member or host on a different IP network.

The router has a routing table, which is a list of networks known by the router. The routing table includes network addresses for its own interfaces, which are the directly connected networks, as well as network addresses for remote networks. A remote network is a network that can only be reached by forwarding the packet to another router.

Remote networks are added to the routing table in two ways: either by the network administrator manually configuring static routes or by implementing a dynamic routing protocol. Static routes do not have as much overhead as dynamic routing protocols; however, static routes can require more maintenance if the topology is constantly changing or is unstable.

Dynamic routing protocols automatically adjust to changes with no intervention from the network administrator. Dynamic routing protocols require more CPU processing and also use a certain amount of link capacity for routing updates and messages. In many cases, a routing table will contain both static and dynamic routes.

Routers make their primary forwarding decision at Layer 3, the network layer. However, router interfaces participate in Layers 1, 2, and 3. Layer 3 IP packets are encapsulated into a Layer 2 data-link frame and encoded into bits at Layer 1. Router interfaces participate in Layer 2 processes associated with their encapsulation. For example, an Ethernet interface on a router participates in the ARP process like other hosts on that LAN.

In the next chapter, we will examine the configuration of static routes and introduce the IP routing table.

Labs

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

Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1)

Complete this lab if you need a solid review of device cabling, establishing a console connection, and command-line interface (CLI) basics. If you are comfortable with these skills, you can substitute Lab 1-2: Basic Router Configuration (1.5.2) for this lab.

Lab 1-2: Basic Router Configuration (1.5.2)

Complete this lab if you have solid skills in device cabling, establishing a console connection, and command-line interface (CLI) basics. If you need a review of these skills, you can substitute Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1) for this lab.

Lab 1-3: Challenge Router Configuration (1.5.3)

This lab challenges your subnetting and configuration skills. Given an address space and network requirements, you are expected to design and implement an addressing scheme in a two-router topology.

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

Check Your Understanding

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

1. Which of the following matches a router component with its function?

   A. Flash: Permanently stores the bootstrap program
   B. ROM: Permanently stores the startup configuration file
   C. NVRAM: Permanently stores the operating system image
   D. RAM: Stores the routing tables and ARP cache

2. Which two commands can a technician use to determine whether router serial ports have IP addresses that are assigned to them?

   A. **show interfaces**
   B. **show interfaces ip brief**
   C. **show controllers all**
   D. **show ip config**
   E. **show ip interface brief**

3. Which of the following commands will set the privileged mode password to "quiz"?

   A. R1(config)# **enable secret quiz**
   B. R1(config)# **password secret quiz**
   C. R1(config)# **enable password secret quiz**
   D. R1(config)# **enable secret password quiz**

4. Which routing principle is correct?

   A. If one router has certain information in its routing table, all adjacent routers have the same information.
   B. Routing information about a path from one network to another implies routing information about the reverse, or return, path.
   C. Every router makes its routing decisions alone, based on the information it has in its own routing table.
   D. Every router makes its routing decisions based on the information it has in its own routing table and its neighbor routing tables.

5. What two tasks do dynamic routing protocols perform?

   A. Discover hosts
   B. Update and maintain routing tables
   C. Propagate host default gateways
   D. Network discovery
   E. Assign IP addressing

6. A network engineer is configuring a new router. The interfaces have been configured with IP addresses and activated. But no routing protocols or static routes have been configured yet. What routes are present in the routing table?

   A. Default routes.
   B. Broadcast routes.
   C. Direct connections.
   D. No routes; the routing table is empty.

7. What two statements are correct regarding how a router forwards packets?

   A. If the packet is destined for a remote network, the router forwards the packet out all interfaces that might be a next hop to that network.
   B. If the packet is destined for a directly connected network, the router forwards the packet out the exit interface indicated by the routing table.

C. If the packet is destined for a remote network, the router forwards the packet based on the information in the router host table.

D. If the packet is destined for a remote network, the router sends the packet to the next-hop IP in the routing table.

E. If the packet is destined for a directly connected network, the router forwards the packet based on the destination MAC address.

F. If the packet is destined for a directly connected network, the router forwards the packet to the switch on the next-hop VLAN.

8. Which statement is true regarding metrics used by routing protocols?

A. A metric is the quantitative value a routing protocol uses to measure a given route.

B. A metric is a Cisco-proprietary means to convert distances to a standard unit.

C. Metrics represent a composite value of the amount of packet loss occurring for all routing protocols.

D. Metrics are used by the router to determine whether a packet has an error and should be dropped.

9. The network administrator configured the **ip route 0.0.0.0 0.0.0.0 serial 0/0/0** command on the router. How will this command appear in the routing table, assuming that the Serial 0/0/0 interface is up?

A. D 0.0.0.0/0 is directly connected, Serial0/0/0

B. S* 0.0.0.0/0 is directly connected, Serial0/0/0

C. S* 0.0.0.0/0 [1/0] via 192.168.2.2

D. C 0.0.0.0/0 [1/0] via 192.168.2.2

10. Describe the internal and external router hardware components and outline the purpose of each.

11. Describe the router bootup process from power on to final configuration.

12. What important features does a router add to the network?

13. Describe the steps necessary to apply a basic configuration to a router.

14. Describe the importance of the routing table. What purposes does it serve?

15. What are the three basic ways a router learns about networks?

16. What fields in the IP header were the most relevant to the information presented in this chapter?

17. Describe the encapsulation/decapsulation process as a packet travels from source to destination.

Challenge Questions and Activities

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

1. When you think about the difference between the hardware and software of a PC and a router, what do you see as the strengths and weaknesses of each device? Which device do you think is the more powerful and why?
2. As you study, learn, and use the command-line interface on a Cisco router, do you see a time when you cannot need to use the CLI to configure routers and switches? What does your vision of network configuration tasks look like without the CLI?
3. If you could design your own routing protocol algorithm to route packets, what would its main features be? How would your protocol decide on the best route? Remember, a computer is going to implement your idea; therefore, be specific.
4. Although the Internet Protocol is now considered the only protocol to use for Layer 3 addressing, this was not always the case. Investigate and report on some other Layer 3 protocols that serve the same purpose. What features do they share in common with IP? How are they different?

To Learn More

Create a topology similar to that presented in Figure 1-18 earlier in the chapter, with several routers and a LAN at each end. On one LAN, add a client host, and on the other end, add a web server. On each LAN, include a switch between the computer and the router. Assume that each router has a route to each of the LANs, similar to that shown in Figure 1-18.

What happens when the host requests a web page from the web server? Look at all the processes and protocols involved, starting with the user entering a URL such as http://www.cisco.com. This includes protocols learned in *Network Fundamentals, CCNA Exploration* as well as information learned in this chapter.

See whether you can determine each of the processes that happen, starting with the client needing to resolve www.cisco.com to an IP address, which results in the client having to do an ARP request for the DNS server. What are all the protocols and processes involved, starting with the DNS request, in getting the first packet with http information from the web server?

- How is DNS involved?
- How is ARP involved?
- What effect does TCP have between the client and the server? Is the first packet the web server receives from the client the request for the web page?

- What do the switches do when they receive an Ethernet frame? How do they update their MAC address tables, and how do they determine how to forward the frame?
- What do the routers do when they receive an IP packet?
- What is the decapsulation and encapsulation process of each frame received and forwarded by the router?
- Are any ARP processes required by the web server and its default gateway (its router)?

End Notes

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

Check Your Understanding and Challenge Questions Answer Key

Check Your Understanding

1. D. The routing table and ARP cache are both stored in RAM. These tables are not saved after the router is powered off. The bootstrap program is stored in ROM, the startup configuration file is stored in NVRAM, and the operating system image is stored in flash. These files are permanently stored in these locations after the router is powered off.

2. A, E. The **show interfaces** and **show ip interface brief** commands include the interfaces and their IP addresses in the output. The other choices are not valid commands.

3. A. The correct command to configure a privileged mode password is **enable secret** *password*.

4. C. The three routing table principles, as described by Alex Zinin in his book *Cisco IP Routing*, are as follows:
   - Every router makes its decision alone, based on the information it has in its own routing table.
   - The fact that one router has certain information in its routing table does not mean that other routers have the same information.
   - Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.

5. B, D. One task that routing protocols are responsible for is discovering networks and adding those networks to the routing table. After those routes are added to the routing table, the routing protocol is responsible for updating and maintaining the routes in the routing table. Routing protocols are not responsible for discovering hosts, propagating a default gateway for hosts, or assigning IP addresses.

6. C. At this point, only the router's directly connected networks are in the routing table. Remote networks can only be added by configuring static routes and/or by using a dynamic routing protocol.

7. B, D. All packets that are forwarded by the router must be resolved to an exit interface in the routing table. If a route only has a next-hop IP address, that next-hop address must eventually be resolved to another route in the routing table that does include an exit interface, such as a directly connected network.

8. A. A metric is used by routing protocols as a quantitative value used to measure the distance to a remote network.

9. B. S* 0.0.0.0/0 is directly connected, Serial0/0/0

10. Router hardware components are described as follows:
    - Central processing unit (CPU): Executes operating system instructions, such as system initialization, routing functions, and network interface control.
    - Random-access memory (RAM): Stores the routing table and other data structures that the router needs when forwarding packets.
    - Read-only memory (ROM): Holds basic diagnostic software used when the router is powered on.
    - Nonvolatile RAM (NVRAM): Stores the startup configuration, including IP addresses, routing protocol, and other related information. NVRAM is a portion of the boot ROM chip.
    - Flash memory: Stores the operating system (Cisco IOS) and other files.
    - LAN interfaces, such as Ethernet and Fast Ethernet interfaces.
    - WAN interfaces, such as serial, ISDN, and Frame Relay interfaces.

11. Test router hardware:
    1. Perform POST.
    2. Execute bootstrap loader.

    Locate and load the Cisco IOS Software:

    3. Locate the IOS.
    4. Load the IOS.

    Locate and load the startup configuration file or enter setup mode:

    5. Locate the configuration file.
    6. Execute the configuration file.
    7. Enter setup mode.

12. A router adds the following features:
    - Determines the best path to send packets
    - Forwards packets toward their destination

13. The steps to apply a basic configuration are as follows:
    1. Name the router.
    2. Set passwords.
    3. Configure interfaces.
    4. Configure a banner.
    5. Save changes on a router.
    6. Verify basic configuration and router operations.

14. A routing table provides the router with the necessary information to carry out its primary function: forwarding packets toward the destination network.

15. A router learns about networks in the following ways:
    - Connected routes
    - Static routes
    - Dynamic routes

16. The most relevant fields are as follows:
    - Version: Version of IP currently used (IPv4)
    - Time to Live (TTL): Number of routers a packet can traverse before being dropped
    - Source IP address: 32-bit source IP address
    - Destination IP address: 32-bit destination IP address

17. The source encapsulates data in a packet with source and destination IP addresses. It then encapsulates the packet into a frame with source and destination MAC addresses and sends the frame out as bits on the wire. The frame is received by the source's gateway—a router—and is decapsulated. If the destination MAC address is the router, the router will search the routing table for an outgoing interface to the destination, encapsulate the packet in the appropriate frame format for the outgoing interface with new source and destination Layer 2 addresses, and forward the frame out the interface. This process is repeated at each router along the path until the packet reaches the destination. From source to destination, the Layer 2 addresses change at each hop. However, the Layer 3 source and destination IP addresses do not change.

Challenge Questions and Activities

1. Your answer should revolve around the understanding that a router is a single-purpose device and a computer is a multipurpose device. The router's main purpose is to forward packets across different Layer 3 networks. A typical PC will most likely have several purposes, including word processing, gaming, and Internet access.

2. Answers will vary. Currently, CLI is the preferred configuration method on Cisco routers, and for many operations, it is the only method. Some of the more complex security operations can be configured on some Cisco routers using the Cisco Security Device Manager (SDM). SDM is a web-based device-management tool for Cisco routers that can improve the productivity of network managers, simplify router deployments, and help troubleshoot complex network and VPN (Virtual Private Network) connectivity issues. For the foreseeable future, it will be important for a network administer to be comfortable with using the Cisco CLI.

3. Answers will vary. Your description should include a step-by-step process. To see pseudocode for current routing algorithms, search the web for Bellman-Ford and Dijkstra algorithms.

4. A hierarchical structure is common to all Layer 3 addressing protocols. Each one identifies a network portion and a host portion. How each does this is different. For example, Novell's Internet Packet Exchange uses an 80-bit address. The first 32 bits are designated network bits and are determined by the administrator. The remaining 48 bits are the same as the MAC address of the host.