CHAPTER 2

NETWORK HARDWARE ESSENTIALS

After reading this chapter and completing the exercises, you will be able to:

Describe the basic operation of network repeaters and hubs

Explain the purpose of network switches

Summarize the operation of wireless access points

Describe the basic operation of network interface cards

Explain the function of routers

LANs, WANs, MANs, and internetworks are built with a variety of network hardware. Your understanding of how the most common network hardware works is crucial to your success in building reliable, high-performance networks.

This chapter begins by discussing the simplest of network devices: the hub, a device that's nearly obsolete but still might be found in older installations and special situations. Switches have supplanted hubs in networks large and small and are the main network building block today. Wireless networking can be found everywhere from small home networks to coffee shops and bookstores to large corporate networks. Wireless access points are the foundation of wireless networks, and you learn about their operation and basic configuration later in this chapter. Network interface cards have become such an essential component of computers that they're now built into most motherboards. Whether they're built in or installed as an expansion card, however, your understanding of NIC configuration options and properties will help

you build a better network. The last section of this chapter covers the most complex network devices: routers, the gateways to the Internet that make it possible for large companies to build vast internetworks and WANs.

Note

Because Ethernet is the dominant network technology used in LANs today, the network hardware components discussed in this chapter are Ethernet devices, unless otherwise stated.

Network hardware devices can be complex. This chapter serves as an introduction to the most common devices so that you have a basic understanding of their function when they're discussed with other topics in later chapters. The function of these devices is intertwined with network topologies and technologies (discussed in Chapter 3) and network protocols (discussed in Chapter 5). Chapter 8 includes a more thorough examination of the devices described in this chapter and discusses some specialized devices as well.

Table 2-1 summarizes what you need for the hands-on projects in this chapter.

Table 2-1 Hands-on project requirements

Hands-on project	Requirements	Time required	Notes
Hands-On Project 2-1: Using Wireshark with a Hub	Three computers, three patch cables, hub	20 minutes	
Hands-On Project 2-2: Using Wireshark with a Switch	Three computers, three patch cables, switch	20 minutes	
Hands-On Project 2-3: Examining Hub and Switch Indicator Lights and Uplink Ports	Three computers, four patch cables, two hubs, switch	30 minutes	
Hands-On Project 2-4: Connecting to a Wireless Access Point	Two computers with wireless NICs, wireless AP or router	15 minutes	
Hands-On Project 2-5: Communicating over a Router	Three computers, two switches, router, five patch cables	20 minutes	
Hands-On Project 2-6: Using Traceroute to See How Packets Travel through the Internet	Net-*XX*	10 minutes	Internet access

Network Repeaters and Hubs

Early networks didn't use interconnecting devices. Computers were connected in daisy-chain fashion by lengths of cable (see Figure 2-1). The problem with this arrangement was that you were limited by the total length of the cabling and the number of computers that could be connected.

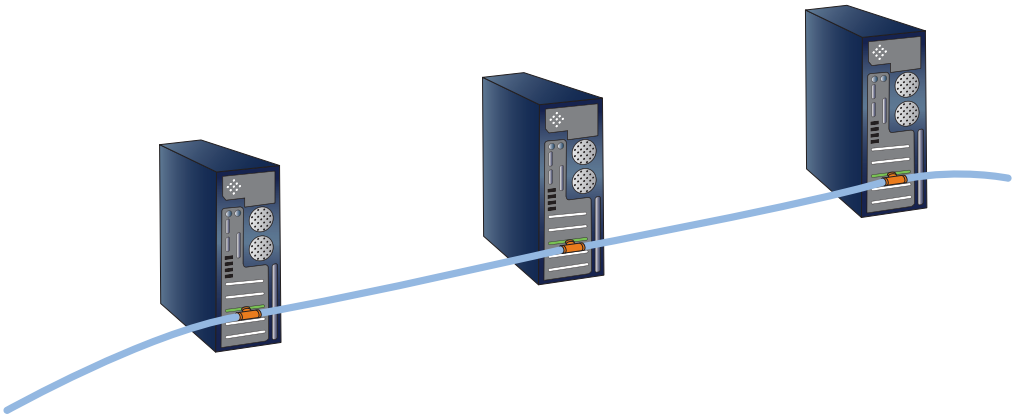

Figure 2-1 Older networks didn't use interconnecting devices

Some problems associated with the type of network shown in Figure 2-1 were solved with a device called a "repeater." A **repeater** has the rather straightforward job of receiving bit signals generated by NICs and other devices, strengthening them, and then repeating them to other parts of the network. Think of a repeater as a microphone for network signals. When people speak, their voices carry only so far until people in the back of the room can no longer hear what's being said. Network signals, too, carry only so far on their medium before receiving computers can no longer interpret them correctly. A repeater enables you to connect computers whose distance from one another would otherwise make communication impossible.

Note

Repeaters don't strengthen signals in the sense that the original signal is amplified; instead, a repeater takes a weakened signal and repeats it at its original strength.

A traditional repeater has two ports or connections that you can use to extend the distance your network can cover, as shown in Figure 2-2. Assuming the two groups of computers in this figure are separated by several hundred feet, the repeater is needed to allow them to communicate with one another.

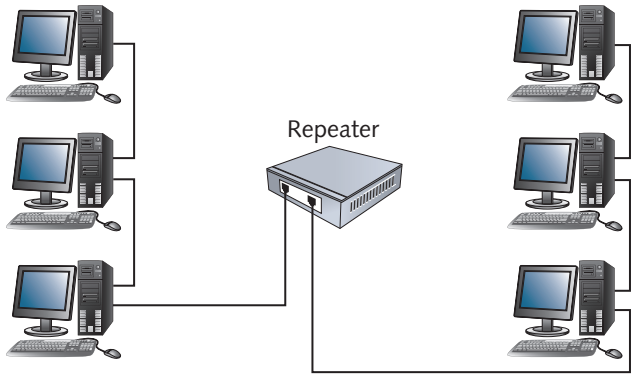

Figure 2-2 A repeater extends the distance a network can cover

Multiport Repeaters and Hubs

A multiport repeater is just a repeater with several ports to which you can connect cabling. Most multiport repeaters have at least four ports, and some have 24 or more. A multiport repeater is commonly called a **hub**, and although it performs the same function as a traditional repeater, it's used as a central connecting device for computers instead of merely a way to extend the network. So, instead of daisy-chaining computers together, all computers are connected to the central hub (see Figure 2-3). Because "hub" is the more common term and is much easier to write and say, a multiport repeater is often referred to as a "hub" in this book.

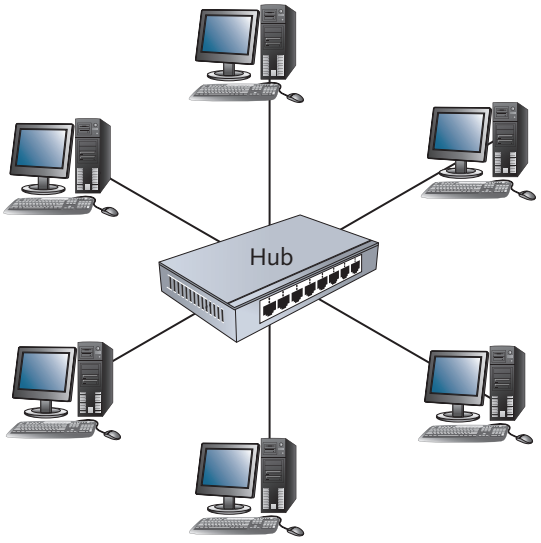

Figure 2-3 A multiport repeater or hub

A hub performs the same function as a repeater but with more outgoing ports to which bit signals are repeated, so its function is as follows:

- Receives bit signals generated from a connected computer on one of its ports
- Cleans the signal by filtering out electrical noise
- Regenerates the signal to full strength
- Transmits the regenerated signal to all other ports to which a network device is connected

Note

Like repeaters, hubs require power to operate, so they're sometimes referred to as "active hubs." However, this term isn't common because unpowered devices known as "passive hubs" aren't used for the same purposes.

Hubs and Network Bandwidth

Network bandwidth is the amount of data that can be transferred on a network during a specific interval. It's usually measured in bits per second; networks operate at speeds from 10 million bits per second (10 Mbps) up to 100 gigabits per second (Gbps). This bandwidth is determined by how fast network devices can send bits of data to the medium. A 10 Mbps hub, for example, transmits bits at the rate of 10 million per second. To put this rate into perspective, two computers connected to a 10 Mbps hub can copy 1 minute of MP3 music to each other in about 1.25 seconds, but a 100 Mbps hub can transfer the same amount of information in about one-eighth of a second.

One drawback of using a hub as the central connecting device on a network is that only one computer can transmit data at a time. On a busy network with dozens of computers transferring large files and accessing network applications and databases, this limitation is serious. This setup is called **bandwidth sharing** because all computers connected to the hub must share the amount of bandwidth the hub provides. For example, a network has 10 computers connected to a 10 Mbps hub, and all 10 computers are trying to send and receive files frequently. Because the computers must share the bandwidth, the average effective bandwidth for each computer is only 1 Mbps. Transferring that one minute of MP3 music in this example takes more than 12 seconds.

In the early days of networking, bandwidth sharing wasn't a big problem because the number and frequency of data transfers in a typical LAN were low and files tended to be small, making the actual effective bandwidth in the preceding example much higher than 1 Mbps. However, large multimedia data files are transferred often in LANs now, so the need for additional dedicated bandwidth is paramount. In fact, this need has become so critical that network administrators stopped including hubs in their network designs; finding a hub to buy from major computer parts retailers is difficult now.

Note

There are more details involved in the concept of bandwidth sharing and how computers transmit data to the medium. The details vary for different network technologies, such as Ethernet, token ring, and Wi-Fi, and are hammered out in Chapter 3.

Hub Indicator Lights

Most hubs have indicator lights for power, link status, network activity, and collisions. Each port has a link status indicator (link light) that glows (usually green) when a cable has been plugged in and a valid network connection, or link, has been made to a device on the other end of the cable. If a hub can operate at multiple speeds, there might be a separate indicator for each speed, or one indicator might vary in color for different connection speeds. For example, the link light might glow green for a 100 Mbps connection and amber for a 10 Mbps connection.

Another indicator light you're likely to find on a hub is for network activity. When the hub receives bit signals on any of its ports, this indicator flashes. Some hubs combine the link status indicator with the network activity indicator so that when the light is on solidly, a valid link is detected, and when the light is blinking, a valid link and network activity are detected.

A third type of indicator is for collisions. A collision occurs on a hub when two stations try to transmit at the same time, which isn't allowed on a hub-based network. When a collision occurs, the stations that were transmitting must retransmit their data. Collisions are discussed in more detail in Chapter 3.

Figure 2-4 shows a typical hub with indicator lights. This hub also has a series of indicator lights showing the utilization percentage for the network. In addition, the rightmost port has a button next to it for changing the port's configuration, depending on whether it's connected to a computer's NIC or another hub or switch. This port

Figure 2-4 A typical hub with indicator lights

Source: NETGEAR

is referred to as the **uplink port**. The term "uplink" is used when multiple hubs or switches are connected. When this button is pressed in, you can connect the hub to another hub or switch with a standard cable rather than a crossover cable. Cable types are discussed more in Chapter 4.

Network hubs were the mainstay for connecting computers in a LAN for several years, but they've become obsolete. Because of their disadvantages, mainly bandwidth sharing, they're being replaced with switches, as discussed in the next section.

Network Switches

Certification

98-366 Understanding network hardware:

Understand switches

A network **switch**, like a hub, is used to interconnect multiple computers so that they can communicate with one another. A switch looks just like a hub, with several ports for plugging in network cables. However, instead of simply regenerating incoming bit signals and repeating them to all other ports, a switch actually reads data in the message, determines which port the destination device is connected to, and forwards the message to only that port. So, the first important difference between hubs and switches is that hubs work only with electrical signals and the bits these signals represent, whereas switches work with the actual information these bits represent. The unit of information that switches work with is called a frame.

Basic Switch Operation

Data is sent to the medium one frame at a time, and the beginning of each frame contains the destination computer's MAC address and the source computer's MAC address. When the frame reaches a switch, the switch reads both addresses. By reading the source MAC address, the switch keeps a record of which port the sending computer is on. This function is referred to as "learning" because the switch is learning to which port each MAC address in the network corresponds. By reading the destination MAC address, the switch can forward the frame to the port the destination computer is on. A switch maintains a **switching table** (see Figure 2-5) of MAC addresses that have been learned and their associated port numbers.

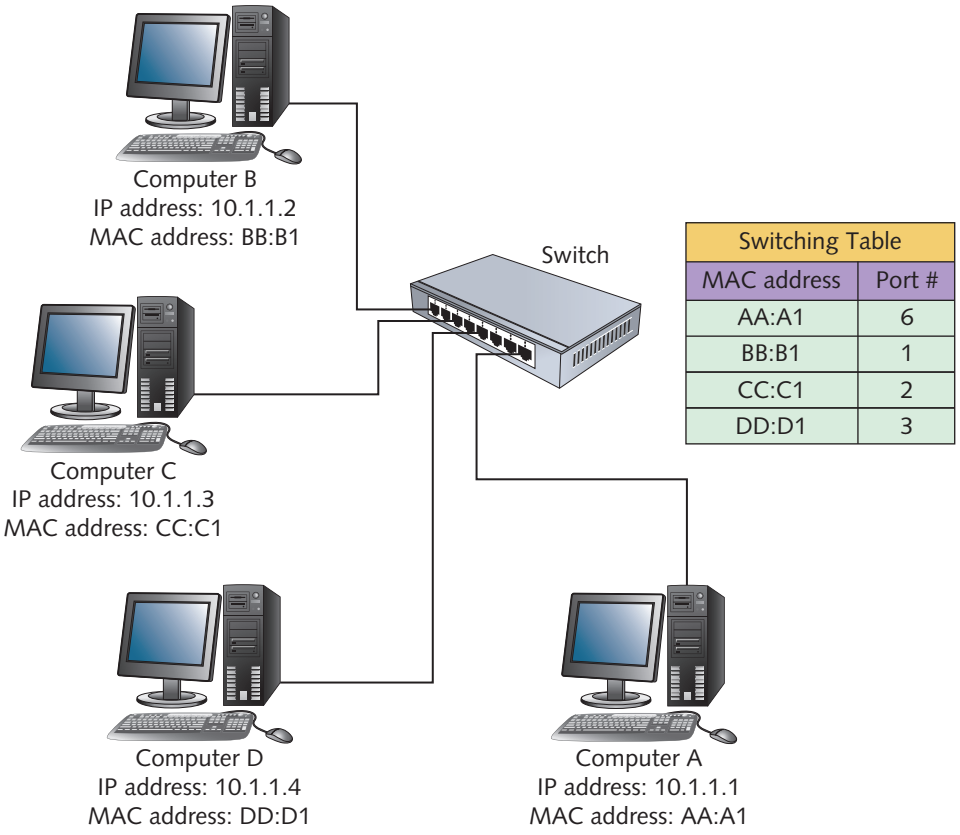

Figure 2-5 Switches maintain a switching table

Note

MAC addresses are 12 hexadecimal digits. Figure 2-5 uses shorter addresses only as an example.

A switch's operation can be summarized in these steps:

1. The switch receives a frame.
2. The switch reads the source and destination MAC addresses.
3. The switch looks up the destination MAC address in its switching table.
4. The switch forwards the frame to the port where the computer owning the MAC address is found.
5. The switching table is updated with the source MAC address and port information.

These steps raise some questions. For example, what happens if the switch doesn't find the destination MAC address in its switching table? In this case, the switch does the most reasonable thing: It forwards the frame to all ports. You can think of a switch as acting like a switchboard operator. When a call comes in for a person the operator knows, the operator can forward the call to the correct phone extension. If the call is for a person the operator doesn't know, the person can be paged via an intercom system.

You might also be wondering what happens if the source address is already in the switching table and how long each MAC address stays in the switching table. The answers to these questions are related. MAC addresses can't stay in the switching table forever because computers might be shut down or moved to other locations, and their MAC addresses can change. Leaving MAC addresses in the switching table for a long time is akin to having an out-of-date employee phone directory that still lists people who have left the company and others who have changed locations. To ensure that the switching table doesn't become out of date, a timestamp is included in each entry, and each entry can stay in the table for only a certain amount of time unless the timestamp is updated. So, when a switch first sees a source MAC address, it creates the switching table entry that includes the MAC address, the port from which the frame arrived, and a timestamp. If the same MAC address is seen again coming from the same port, the timestamp is updated. If the entry remains in the table beyond the maximum allowed time without being updated, it's deleted. (The maximum allowed time varies between switches, but it's often about 5 minutes.)

Switches and Network Bandwidth

Because a switch is capable of forwarding frames to only a single port instead of all ports, as a hub does, it can handle several computer conversations at one time, thereby allowing each device the full network bandwidth, or **dedicated bandwidth**, instead of requiring bandwidth sharing. In other words, if the switch in Figure 2-5 is a 100 Mbps switch, Computer A could communicate with Computer C at an uninterrupted 100 Mbps rate, and Computer B could communicate with Computer D at 100 Mbps simultaneously. Furthermore, each computer can receive data at 100 Mbps at the same time it's sending data at 100 Mbps, making each conversation between computers effectively 200 Mbps (100 Mbps in both directions). When a device can send data and receive data simultaneously, it's called **full-duplex mode**. When a device can send or receive, but not both at the same time, it's called **half-duplex mode**. Hubs operate only in half-duplex mode, but switches can operate in both half-duplex and full-duplex modes. To use another form of communication as an example, full-duplex mode is like talking on a telephone and half-duplex mode is like talking on a walkie-talkie. Chapter 3 describes these modes of communication in more detail.

The performance advantage of switches has made them the device of choice in networks of all sizes. Also, switches cost less than hubs, even though they're more complex. As mentioned, you might still find hubs in the workplace, but new installations don't specify them, and the tables have been turned—hubs are more expensive than switches because manufacturers simply aren't making them in large quantities.

Switch Indicator Lights

Like hubs, switches have indicator lights so that you can see the basic operating status of the ports with a quick glance. Aside from the requisite power indicator, switches have link status indicators and activity indicators. They might also have indicators to show whether a port is operating in full-duplex or half-duplex mode. Switches, like hubs, can be connected to one another so that your LAN can grow beyond the limitations of the number of ports on a single switch. Some switches also have a dedicated port for uplinking to another switch. **Uplinking** is making a connection between devices such as two switches, usually for the purpose of expanding a network. Switches are complex devices, and this section just introduces their basic operation. You can find a more detailed examination of switches in Chapter 8.

Hands-On Project 2-1: Using Wireshark with a Hub

Time Required: 20 minutes

Objective: Use the Wireshark protocol analyzer on a computer connected to other computers via a hub to see that all data is repeated to all stations.

Required Tools and Equipment: Three lab computers must be configured per the specification in the "Before You Begin" section of the book. In addition, three patch cables and a hub are required. Review the lab setup instructions in "Before You Begin" for more information on lab equipment.

Description: In this project, you run Wireshark on a group of computers connected via a hub. This project shows that a hub repeats all data to all stations so that Wireshark can capture packets generated by all stations. In the next project, you compare this behavior with that of a switch.

Note

This project requires at least three computers connected to a hub, with at least one computer running Wireshark. It's probably best done in groups. The steps in this project assume three computers are connected to the hub and labeled Computer1, Computer2, and Computer3. Wireshark must be installed on Computer1, but it can be installed on all computers. It's preferable that the computers aren't attached to the classroom network and don't have access to the Internet.

1. Connect three lab computers to a hub with patch cables. Make sure the device is a hub, not a switch.
2. Turn on the computers and log on as **NetAdmin**. Open an elevated command prompt window on each computer. (In Windows 10, right-click **Start** and click **Command Prompt (Admin) or Windows PowerShell (Admin)**.) Click **Yes** in the User Account Control window. On each computer, type `ipconfig` and press **Enter** to display its IP address

configuration. Write down these IPv4 addresses so that you know each computer's address:

- Computer1: _____
- Computer2: _____
- Computer3: _____

3. To verify connectivity, type **`ping IPaddress`** from each computer and press **Enter** (replacing *`IPaddress`* with another computer's IP address). Repeat this step until you have successfully pinged each computer from the other computers.

Note

If the pings aren't successful, you might need to turn off Windows Firewall. To do so, type **firewall** in the search box and click **Windows Defender Firewall**. In the Windows Defender Firewall window, click **Turn Windows Defender Firewall on or off**. Under Public network settings, click **Turn off Windows Defender Firewall**, and then click **OK**. Close the Windows Firewall window, and repeat Step 3.

4. On Computer1, start Wireshark. (If Wireshark isn't on your desktop, right-click **Start**, click **Run**, type **Wireshark** in the text box, and press **Enter**.)
5. By default, Wireshark captures all the packets your NIC sees. You want to limit the packets to only those created by the `ping` command, so click **Capture Options** on the left. In the Capture using this filter text box (see Figure 2-6), type **icmp**. You must use lowercase letters. (Internet Control Message Protocol [ICMP] packets are created by the `ping` command). Click the **Start capturing packets** toolbar icon, which looks like a blue shark fin on the far left of the menu bar.

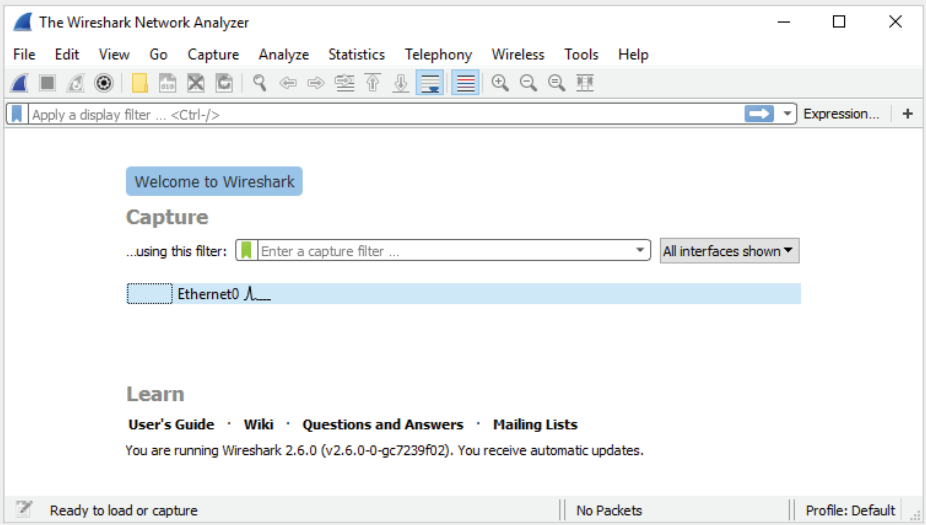

Figure 2-6 The Wireshark main window

Source: Wireshark

6. First, you ping from Computer2 to Computer1. On Computer2, type **`ping IPaddress`** at the command prompt and press **Enter** (replacing *`IPaddress`* with the IP address of Computer1).
7. On Computer1, click the **Stop the running live capture** toolbar icon (a red square button next to the shark fin) to stop the capture. You should see a window similar to Figure 2-7.

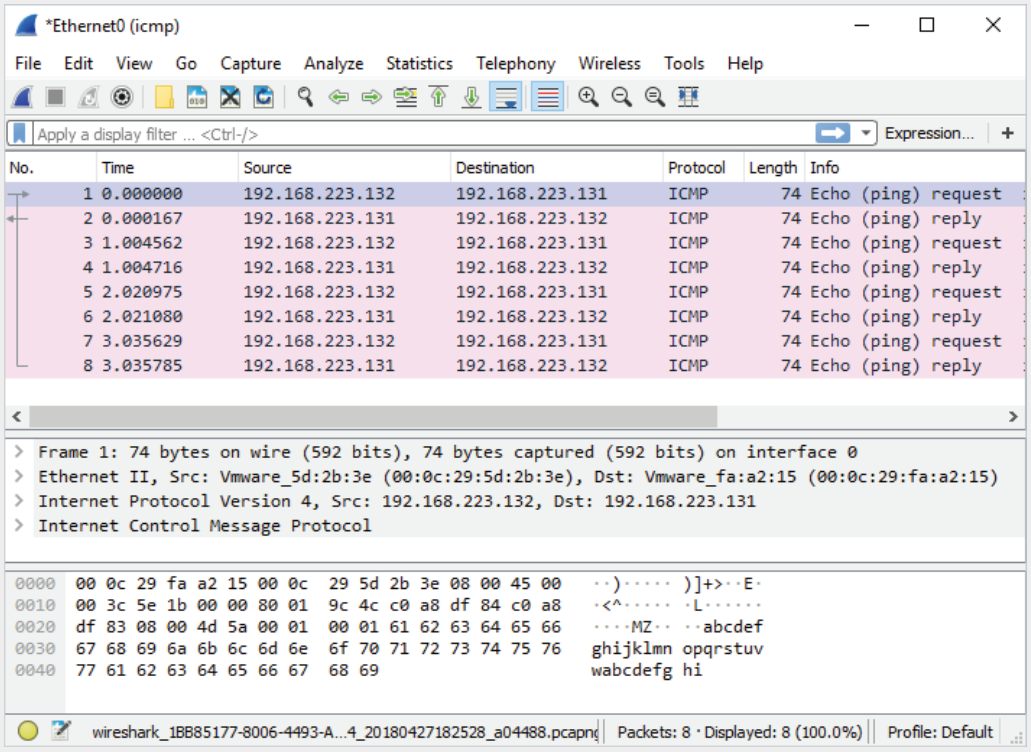

Figure 2-7 Ping packets captured on Computer1

Source: Wireshark

8. On Computer1, click the **Start capturing packets** toolbar icon. Click **Continue without Saving**.
9. Next, you ping from Computer2 to Computer3. On Computer2, type **`ping IPaddress`** at the command prompt and press **Enter** (replacing *`IPaddress`* with the IP address of Computer3). Wireshark running on Computer1 should have captured the ping packets. Stop the capture and exit Wireshark. Why are the packets sent between Computer2 and Computer3 captured by Computer1?

   _____

   _____
10. Close the command prompt window and shut down all computers.

Hands-On Project 2-2: Using Wireshark with a Switch

Time Required: 20 minutes

Objective: Use Wireshark on a computer connected to other computers via a switch to see that all data isn't repeated to all stations.

Required Tools and Equipment: The same requirements as Hands-On Project 2-1, replacing the hub with a switch

Description: In this project, you run Wireshark on a group of computers connected via a switch. This project shows that a switch only forwards data to the station to which the frame is addressed. In Hands-On Project 2-1, you configured Wireshark to capture only ICMP packets. In this project, you configure Wireshark to also capture Address Resolution Protocol (ARP) broadcast packets to show that switches forward broadcasts to all stations.

1. Connect the computers you used in Hands-On Project 2-1 to a switch instead of a hub, using the same patch cables you used previously.
2. Turn on the computers and log on as **NetAdmin**. Open an elevated command prompt window on each computer by right-clicking **Start** and clicking **Command Prompt (Admin)**. Click **Yes** in the User Account Control (UAC) message box. If the computers were shut down or restarted, their IP addresses might have changed. Type **`ipconfig`** and press **Enter** on each computer. Write down each computer's IP address again:
   - Computer1: _____
   - Computer2: _____
   - Computer3: _____
3. To make sure you have connectivity with the switch, type **`ping IPaddress`** from each computer and press **Enter** (replacing *`IPaddress`* with the IP address of another computer). Repeat this step until you have successfully pinged each computer from all other computers. Leave the command prompt window open.
4. At each computer, type **`arp -d`** and press **Enter**. As mentioned in Chapter 1, ARP manages the MAC addresses your computer has learned. This command deletes the entries created from the pings you did in Step 3 so that the computers have to learn the MAC addresses of other computers again. Leave the command prompt window open.
5. On Computer1, start Wireshark, and click **Capture Options**. In the Capture Filter text box, type **icmp** or **arp**. (You must use lowercase letters.) This capture filter tells Wireshark to capture only ICMP or ARP packets. Click **Start capturing packets**.
6. On Computer2 at the command prompt, type **`ping IPaddress`** and press **Enter** (replacing *`IPaddress`* with the IP address of Computer1).
7. On Computer1, click **Stop capturing packets**. You should see a window similar to Figure 2-8. Notice that the first ARP packet you see has the destination address "Broadcast." When you click this packet, the middle pane displays the MAC address ff:ff:ff:ff:ff:ff.

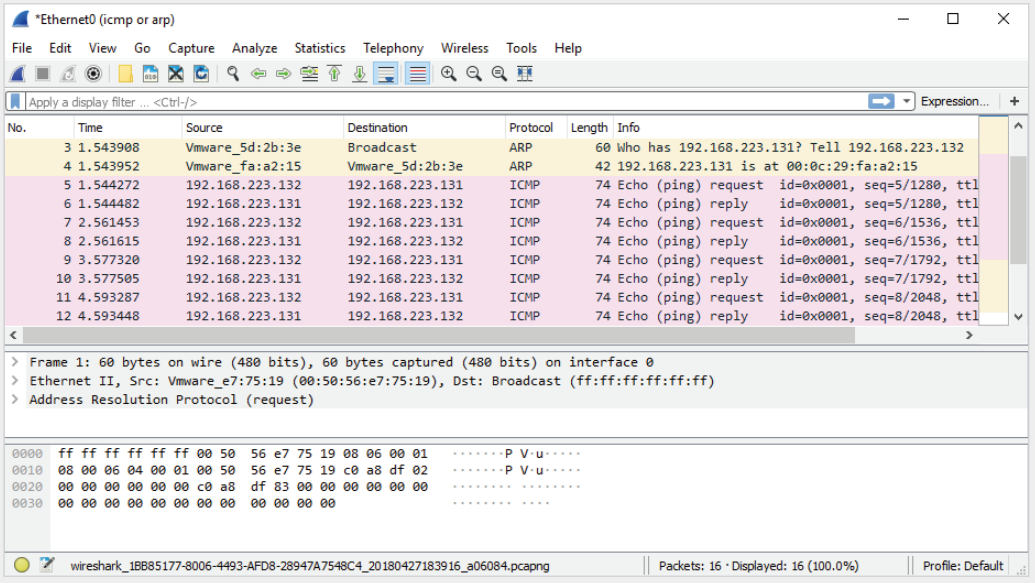

Figure 2-8 Ping and ARP packets

Source: Wireshark

8. On Computer1, click **Capture** on the Wireshark menu bar, then click **Start**. Next, click **Continue without Saving**.
9. On Computer2 at the command prompt, type **`ping IPaddress`** and press **Enter** (replacing *`IPaddress`* with the IP address of Computer3). Wireshark running on Computer1 should have captured only the ARP broadcast packet, not the actual ping ICMP packets, which are unicast packets (explained later in "NIC Basics"). Because the switch doesn't forward unicast packets except to the intended destination, Computer1 never received the ping packets between Computer2 and Computer3. Stop the capture in Wireshark. Why did Computer1 capture the ARP packets from Computer2 and Computer3 but not the ICMP packets?

   _____

10. What do you think the purpose of the ARP protocol is?

    _____

11. Close all open windows, and shut down the computers.

Hands-On Project 2-3: Examining Hub and Switch Indicator Lights and Uplink Ports

Time Required: 30 minutes

Objective: Examine the indicator lights of a hub and switch and understand the purpose of the uplink port.

Required Tools and Equipment: Three lab computers, four patch cables, one crossover cable, two hubs, and a switch

Description: In this project, you view the indicator lights of hubs and switches. Ideally, your hub has indicators for link status, activity, and collisions. In addition, if your hub has an uplink port, you test its function. Like the previous two projects, this project can be done in groups or as a class demonstration.

1. The computers should be shut down and one hub should be plugged in and turned on, if necessary. Connect all three computers to the hub with patch cables, but don't use the uplink port on the hub. Turn on the computers.
2. Examine the hub's indicator lights. A link status light should be glowing for each port to which a computer is connected. Next, examine the indicator lights on the NIC, which should also be glowing to indicate a good connection. See whether the hub's indicator lights vary for different connection speeds. Write the link status light's color and the connection speed, if available, in the following chart:

Computer	Link status light's color	Connection speed
Computer1		
Computer2		
Computer3		

3. Generate some traffic by using `ping` commands on each computer. At each computer, open a command prompt window and ping another computer by typing **`ping -n 20 IPaddress`** and pressing **Enter**. (For example, Computer1 can ping Computer2, Computer2 can ping Computer3, and Computer3 can ping Computer1.) Examine the activity indicator lights, which should blink as data is received. (On hubs that combine the activity indicator with the link status, network activity causes the link status indicator to blink.) The `-n 20` option in the `ping` command specifies sending 20 ICMP packets instead of just 4.
4. Next, if your hub has collision indicators, try to get them to glow. Note that the pings must be sent from each computer at the same time for a collision to occur. At each computer, type **`ping -n 20 -l 60000 IPaddress`** and press **Enter**. The `-l 60000` (lowercase "L") option makes each ping packet 60,000 bytes in length. Even with these large amounts of data being transferred, you might not see a collision. Remember that a collision occurs when two or more computers send data simultaneously, which isn't permitted when using a hub. However, if your hub and NICs are operating at 100 Mbps, data is transferred so quickly that producing a collision might be difficult.

5. Leave the first hub powered on, and power on the second hub. With a regular patch cable, connect the first hub to the second hub, but don't use the uplink port. In most cases, you won't see the link lights glow at the ports where the two devices are connected. To fix this problem, plug one end of the patch cable into the uplink port on one hub (not on both hubs) and set the switch to the uplink position. You should now have connectivity between the hubs, and the link lights should be on.
6. If your hubs don't have an uplink port, you can connect two hubs with a crossover cable. To do this, first disconnect the two hubs. Then, using a crossover cable from your instructor, connect each end of the cable to regular ports (not uplink ports) on the two hubs. The link lights should glow. (You learn more about patch cables and crossover cables in Chapter 4.)
7. List any other indicator lights you find on the hub and what these lights tell you:

   _____

   _____

   _____
8. Disconnect the computers from the hubs and put the hubs away. Connect the computers to the switch, and then power on the switch.
9. Along with link status lights, most switches have lights on each port to indicate whether the port is operating in full-duplex or half-duplex mode. If your switch has these indicators, find them and try to determine in which mode your NIC and switch are communicating. Most NICs and switches support full-duplex communication, and this mode is chosen automatically.
10. List any other indicator lights you find on the switch and what these lights tell you:

    _____

    _____
11. Close all open windows, and shut down the computers.

Wireless Access Points

Certification

98-366 Understanding network infrastructures:

Understand local area networks

Understand wireless networking

As you probably know, not all networks require a cable tethering the computer to a switch or hub. Wireless networks have become ubiquitous in college and corporate campuses and in many public locations, such as airports and libraries. At the heart of a wireless LAN is the wireless **access point (AP)**. An AP is a lot like a hub, in that all computers send signals through it to communicate with other computers. The obvious difference is that signals don't travel through a physical medium; they travel through the airwaves as radio signals.

Most wireless networks in small businesses and homes use a device typically called a wireless router that combines the functions of an AP, a switch, and a router (see Figure 2-9). Wireless routers can usually be identified by the two or more antennae on the device. These devices are usually used with a cable or DSL modem to provide wireless access to the Internet. Large businesses use dedicated APs to give users wireless access to the corporate network as well as the Internet.

Figure 2-9 A wireless router combines an access point, a switch, and a router

Source: Cisco Systems, Inc.

Wireless networks rarely stand by themselves. They're almost always connected to a wired network at some point. APs typically have one or more connectors for connecting to a wired Ethernet network.

Basic AP Operation

An AP is much like a wired hub, in that all stations hear all network data transmitted by all other wireless devices in the network. All communication goes to the AP, which then retransmits or repeats the transmission to the destination station. However, unlike hubs, communication between two stations requires an extra step. The destination device sends an acknowledgment back to the sending device to indicate that the frame was received. When the sending device receives the acknowledgment, it knows that no error or collision has occurred.

Some wireless configurations require additional handshaking between two communicating devices. Before a computer can transmit data to the AP, it must first send a short **request to send (RTS)** message to let the AP know it intends to transmit data. If no other stations are trying to send data, the AP responds with a **clear to send (CTS)** message letting the requesting station (and all other stations on the network) know that it can send data. The RTS and CTS messages are sent in addition to the acknowledgment the receiving computer sends. Imagine if you had to communicate in this fashion while speaking. Before each sentence you wanted to speak, you would have to ask a moderator

whether you could speak, and the moderator would have to answer affirmatively. Then, after each sentence, the moderator would have to acknowledge that you were heard before you could speak the next sentence. Conveying any real information would take much longer because so much time would be wasted on the overhead required by the communication rules. Fortunately, most wireless networks don't use the RTS/CTS configuration, but it's available as an option on some APs and wireless NICs.

Wireless APs and Network Bandwidth

All the extra chatter required to send data in a wireless network slows communication quite a bit. In fact, the effective bandwidth (that is, the bandwidth used for actual data transmission) is about half the physical bandwidth. Keep in mind, too, that wireless network bandwidth is shared, as with a hub.

Most APs operate at anywhere from 11 Mbps to several Gbps. A common operating speed is 54 Mbps. So, a wireless AP operating at 54 Mbps shares this 54 Mbps with all computers in the wireless network. Therefore, if 10 stations are connected to an 54 Mbps wireless network, each station has about 5.4 Mbps of effective bandwidth; with all the extra network traffic (acknowledgments and possible RTS/CTS messages), however, you must halve this amount, leaving only about 2.7 Mbps of effective bandwidth. That's why developers are constantly striving to get more bandwidth out of wireless networks. In recent years, the performance of basic 11 Mbps wireless networks has increased to several hundred Mbps, and speeds of 1, 2, and more Gbps are becoming common.

Note

Wireless networking is a big subject to tackle; you learn more about wireless networking standards and technologies in Chapter 3.

Network Interface Cards

Certification

98-366 Understanding network infrastructures:

Understand local area networks

As a networking professional, you must understand what a network interface card does and how it works as well as what's involved in configuring a NIC for special network situations in which the default configuration is inadequate. Although most NICs are built into a computer's motherboard, they occasionally fail or additional NICs are needed for your application, so you should know how to install a new NIC, too. The following sections discuss the basic operation of a NIC along with its device driver, its most common features, and some configuration options.

NIC Basics

Attaching a computer to a network requires a **network interface card (NIC)** to create and mediate the connection between the computer and the networking medium. The networking medium might be copper wire, fiber-optic cable, or the airwaves, but in all cases, data is represented as bit signals that the NIC transmits or receives.

For incoming data, the NIC must be able to interpret the signals used for the network medium, which are electrical for copper wire, light for fiber-optic cable, or radio waves for wireless networks. These signals are then converted to bits and assembled into frames. For outgoing data, the NIC converts frame data into bits and transmits these bits to the medium in the correct signal format. The following list summarizes the tasks a NIC and its driver perform:

- Provide a connection from the computer to the network medium.
- For incoming messages, receive bit signals and assemble them into frames, verify the frame's destination address and the error-checking code, remove the frame header and trailer, and transfer the packet to the network protocol.
- For outgoing messages, receive packets from the network protocol and create frames by adding source and destination MAC addresses and the error-checking code.
- Convert the frame data into bit signals in a format suitable for the network medium and transmit the signals.

Note

The error-checking code in the frame trailer is called the cyclical redundancy check (CRC).

Figure 2-10 shows a NIC handling incoming data, and Figure 2-11 shows a NIC handling outgoing data.

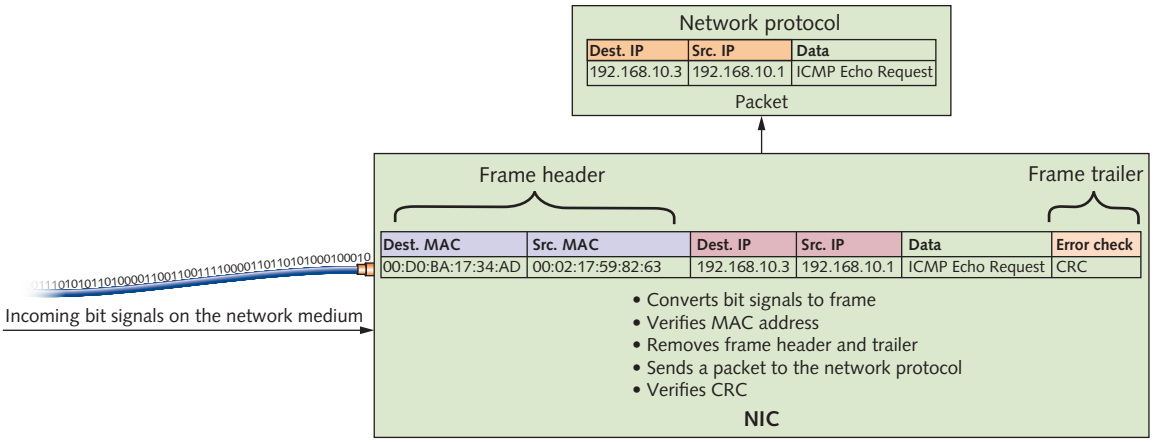

Figure 2-10 A NIC handles incoming data from the network medium

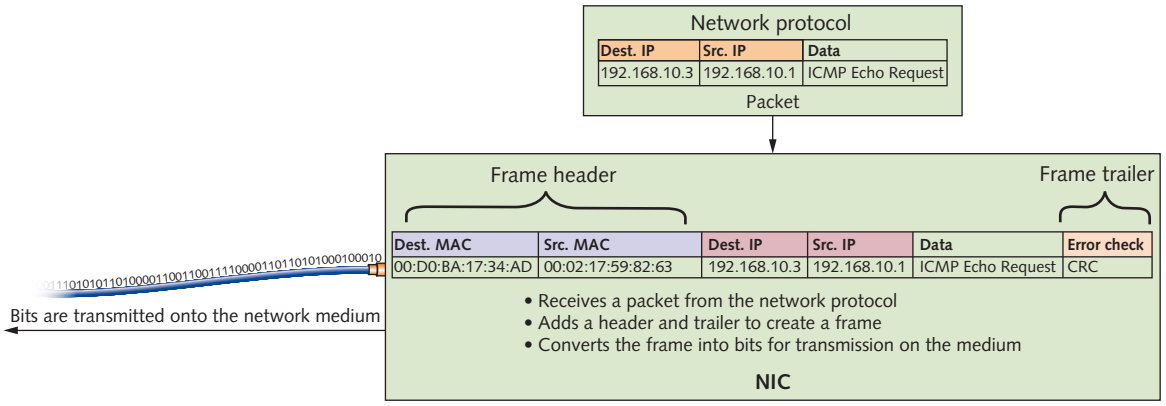

Figure 2-11 A NIC handles outgoing data to be sent to the network medium

NICs and MAC Addresses

Aside from the tasks described previously, a NIC has the important function of giving a computer a MAC address, which is an integral part of each NIC. NIC manufacturers ensure that every NIC has a unique address because networks don't function correctly if duplicate MAC addresses exist. The MAC address is stored in nonvolatile memory on the NIC. Because the address is said to be burned into memory, it's sometimes referred to as the "burned-in address" (BIA). The MAC address is composed of two 24-bit numbers:

- A 24-bit manufacturer ID called an organizationally unique identifier (OUI)
- A 24-bit serial number assigned by the manufacturer

The 48-bit MAC address is expressed in hexadecimal notation, usually as six two-digit alphanumeric characters separated by dashes or colons, such as 04-40-31-5B-1A-C4. The first three two-digit groups represent the OUI, and the last three are the unique serial number. A hexadecimal number is based on powers of 16. There are 16 symbols to represent each hexadecimal number: 0 to 9, A, B, C, D, E, and F. The symbol A represents the decimal value 10, and F represents the decimal value 15.

Tip

You can find a NIC's manufacturer by its MAC address. Go to *http://standards.ieee.org/regauth/oui/index.shtml* and enter the first three numbers (six digits) of a MAC address, separated by dashes.

The NIC as Gatekeeper

When a frame arrives at a NIC, the NIC doesn't simply read the frame and send a packet to the network protocol. It examines incoming network frames and checks the frame's destination MAC address to see whether it matches the NIC's built-in

MAC address. The NIC acts as a gatekeeper and permits inbound communications to pass through the interface only if the destination MAC address meets one of these criteria:

- The destination MAC address in the frame matches the NIC's built-in MAC address.
- The destination MAC address in the frame is the broadcast address.
- The NIC is operating in promiscuous mode.

A frame with a destination MAC address composed of all binary 1s or FF-FF-FF-FF-FF-FF in hexadecimal is a **broadcast frame**. Broadcast frames are intended to be processed by all computers on the network. Destination MAC addresses intended for a single computer are called **unicast frames**. Most NICs can operate in what's called **promiscuous mode**—essentially, this mode turns off the gatekeeper functions and enables the NIC to process all frames it sees. This mode is used by software called a protocol analyzer or packet sniffer (such as the Wireshark program you used in Hands-On Project 2-2) that captures frames and displays their contents for the purposes of troubleshooting and learning.

Note

A third type of MAC address, called a "multicast address," is intended to be processed by a group of computers running a particular application or service. These MAC addresses are identified by a value of 1 in the rightmost bit of the first two digits, such as 01-22-33-44-55-66.

NIC Indicator Lights

Like hubs and switches, NICs have indicator lights to show status information. Although the details vary across NIC models, NICs usually have a link status indicator and an activity indicator. The link status light is usually green when the NIC has a valid connection between the network medium and another device, such as a hub or switch. NICs usually also have an indicator light that flashes when the NIC detects network activity. As with hubs and switches, the link light and activity indicators are sometimes combined.

Some NICs that support multiple speeds, such as 100 Mbps and 1000 Mbps, have a separate link light for each speed so that you can determine at what speed the NIC is connected to the hub or switch. In other cases, the link light indicates the connection speed by using different colors, such as amber for 100 Mbps and green for 1000 Mbps. There's no standard for NIC indicator lights, so you should consult the NIC's documentation to determine their purposes.

Selecting a NIC

The average user might never have to install a NIC because most NICs are built into the motherboard. However, onboard interfaces can fail or prove inadequate for how the computer is to be used. For example, the built-in NIC might operate at only 1 Gbps, and you want the interface to operate at 10 Gbps, or there might be only one built-in NIC, and you want two or more NICs for a server. In these cases, you need to select a NIC with the correct bus interface to connect to your computer.

The NIC connects to the motherboard via the bus; when a NIC receives data, the data must be transferred to the bus and then to the CPU so that it can be processed. The bus speed determines how fast data can be transferred between components. When data is to be transmitted to the network, it goes from the CPU through the bus and to the NIC before being sent to the network medium.

Several bus types are in common use on PC motherboards. Chapter 8 delves into specifics of the bus architectures commonly used for NICs, but for now, you just need to know that PCI Express (PCIe) is the one you're most likely to encounter when installing an internal NIC. To make installation easier, you might want to choose a NIC that connects to your computer via an external USB connector.

What's most important in selecting a NIC to install is that you choose one your system supports, both in bus type and availability of device drivers for your computer's OS. The NIC's specifications tell you the bus type, and the packaging or manufacturer's Web site lists the OSs for which device drivers are available.

A close second in importance is selecting a NIC that's suitable for the role your computer will play in the network. If the computer is a typical desktop system, a standard $10 PCIe NIC that operates at speeds of 100/1000 Mbps is probably enough. For servers or high-performance workstations, consider a NIC that has onboard memory and multiple ports and connects at 10 Gbps.

NIC Drivers

Installing a driver for a NIC is usually easy. Most OSs ship with drivers for a wide range of NIC manufacturers and models. Also, most NICs include drivers for the most common OSs, including current Windows and Linux versions. In most cases, you simply need to shut down your computer, install the NIC, and restart the computer. If the OS has a suitable driver available, it's installed automatically. If not, you're usually prompted to insert media containing the driver files or download them from the manufacturer's Web site.

After the drivers are installed, the NIC is usually ready to function without further configuration. In Windows 10, you can verify that the NIC is installed in the Network & Internet Status window, which you access by right-clicking Start and clicking Network Connections (see Figure 2-12).

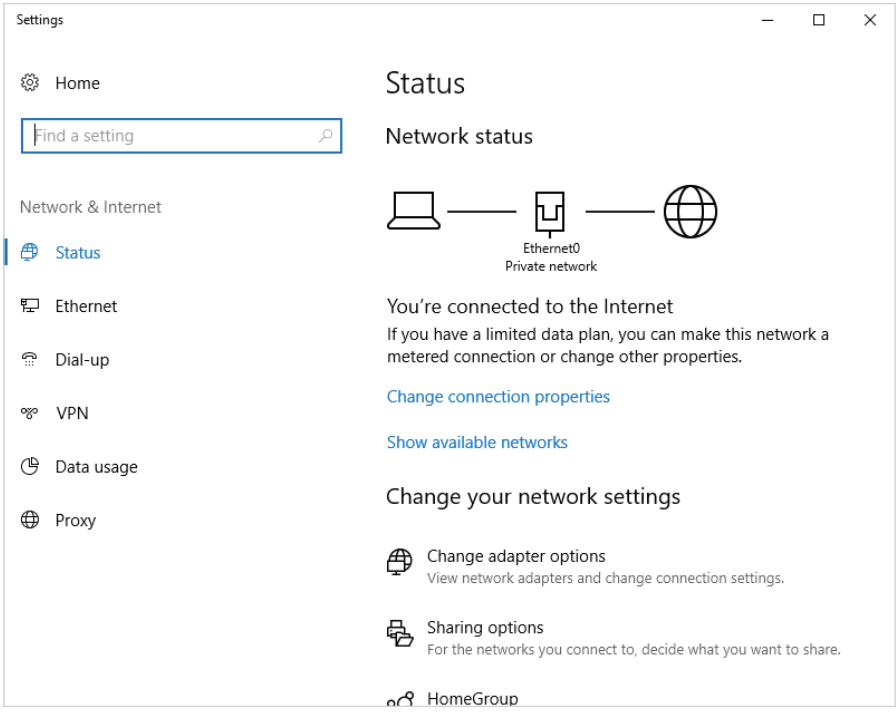

Figure 2-12 The Network & Internet Status window in Windows 10

In Windows, each NIC is assigned a connection name. The first NIC in the system is assigned the name Ethernet0. If you have a second NIC, it's assigned Ethernet1, and so forth, but you can change the name to be more descriptive. To view a connection's properties, click Change adapter options to open the Network Connections window, then right-click the connection and click Properties to open the dialog box shown in Figure 2-13. The "Connect using" text box shows the type of NIC that's installed. To change the NIC's settings and its driver, click the Configure button. Common NIC configuration options are discussed in Chapter 8.

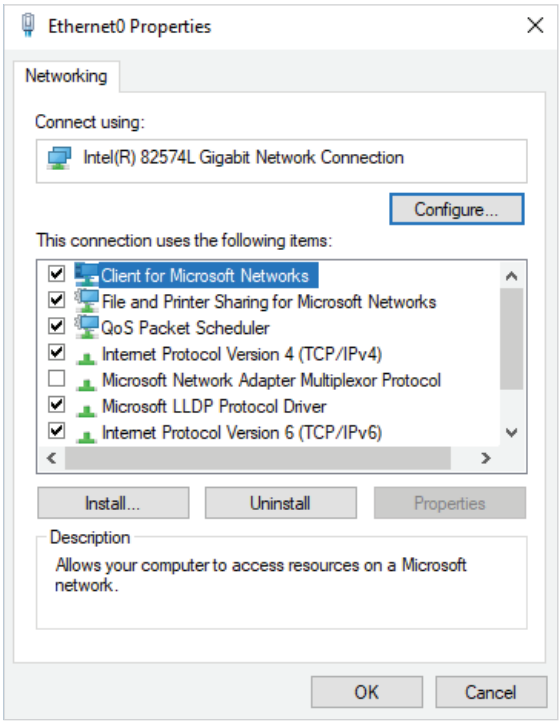

Figure 2-13 The Ethernet0 Properties dialog box

Wireless NICs

The selection process for a wireless NIC differs somewhat from selecting a wired NIC. Wireless NICs are most often built into laptops and other portable computers, but you still might want to install one on a desktop computer, particularly in a small business that uses wireless networking exclusively.

Wireless NICs must be chosen according to the type of wireless AP you have installed. Most are described in terms such as Wireless-n or 802.11ac or perhaps 802.11a/b/g/n. The letters a, b, g, n, and ac refer to the wireless networking standard the device supports. These standards support increasing speeds and features in this order from slowest to fastest: b, g, a, n, and ac. Wireless-b, or 802.11b, is among the earliest wireless standards and supports up to 11 Mbps transfer rates. 802.11a and 802.11g came next and support up to 54 Mbps transfer rates. 802.11n supports speeds from 54 Mbps to more than 600 Mbps. The newest standard, 802.11ac, supports speeds faster than 1 Gbps and will eventually support almost 7 Gbps. Chapter 3 covers these standards in more detail.

Unlike a wired NIC, a wireless NIC often requires a few more steps before a successful connection can be made. Figure 2-14 shows the Wi-Fi connections window, which lists all wireless networks in the range of your wireless NIC. You can click the network ID and

Figure 2-14 Connecting to a wireless network

then click the Connect button to connect to a wireless network. You also have the option to connect automatically whenever the network is in range of your computer. The name assigned to a wireless network, called the **service set identifier (SSID)**, is configured on the AP. You might also be prompted for a security key or a username and password, depending on the network's security configuration. When security is enabled on a wireless LAN (WLAN), communication is encrypted so that unauthorized parties can't connect or easily interpret the data traveling through airwaves. The security key serves as a decryption key, allowing a client to access the wireless network. You learn more about wireless networks and how to configure them in Chapter 3.

Hands-On Project 2-4: Connecting to a Wireless Access Point

Time Required: 15 minutes
Objective: Install a wireless NIC and connect to an access point.
Required Tools and Equipment: You need two lab computers with 802.11 wireless NICs installed. USB wireless NICs work well, as they don't require opening the computer case. Laptops with built-in wireless NICs will also do. You also need one wireless AP or wireless router configured with the SSID "NetEss." The 802.11 standard supported doesn't matter as long as the AP is compatible with the NICs. The computers shouldn't be connected to a hub or switch.
Description: In this project, you connect to a wireless AP and test the connection by pinging another computer connected to the same AP.

1. Start your computer and log on as an administrator. If the wireless NIC isn't installed yet, install it according to your instructor's instructions.
2. After the wireless NIC has been installed, click the network connection icon in the notification area to display a list of available wireless networks (shown previously in Figure 2-14).
3. Click the **NetEss** wireless network. A message is displayed, stating that information sent over the network might be visible to others because it's not secured with encryption. You will secure the network later, so click the **Connect** button.
4. After a short time, you might see the Set Network Location window. The network location can be Home, Work, or Public and is used to set up firewall rules for the connection. If you see this window, click the **Work** network, and then click **Close**.
5. You're now connected to the NetEss wireless network. To test the connection, get the IP address of another computer connected to the wireless network and ping the address. Alternatively, you can ping the router, which should be at the address 192.168.1.1. Ask your instructor for the correct address if pinging 192.168.1.1 doesn't work.
6. Close all open windows, and shut down all computers.

Routers

Certification

98-366 Understanding network hardware:

Understand routers

Routers are the most complex devices discussed in this chapter. Hubs and switches connect computers to the LAN; routers connect LANs to one another. Routers typically have two or more network ports to which switches or hubs are connected to form an internetwork. Figure 2-15 is a diagram of an internetwork, with two LANs connected via a router. Each LAN in this example uses switches to connect workstations and a router port to the LAN. LAN 2 has two switches that are connected.

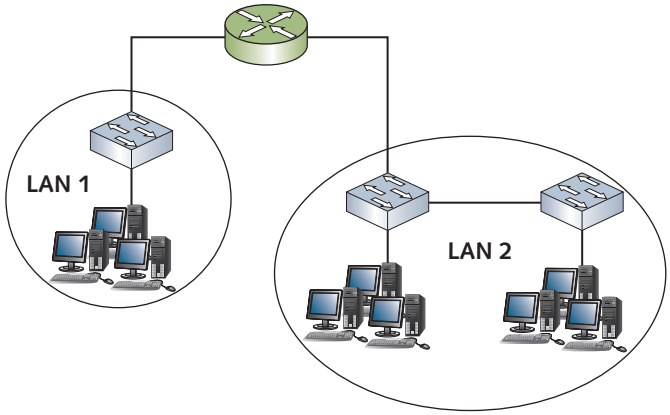

Figure 2-15 Two LANs connected by a router to make an internetwork

A **router** enables multiple LANs to communicate with one another by forwarding packets from one LAN to another. They also forward packets from one router to another when LANs are separated by multiple routers. The Internet is built on a vast collection of LANs, all interconnected via routers. Figure 2-16 shows a small business network connected to its Internet service provider (ISP), followed by connections to several other Internet routers and ultimately to a Web server on the cengage.com network.

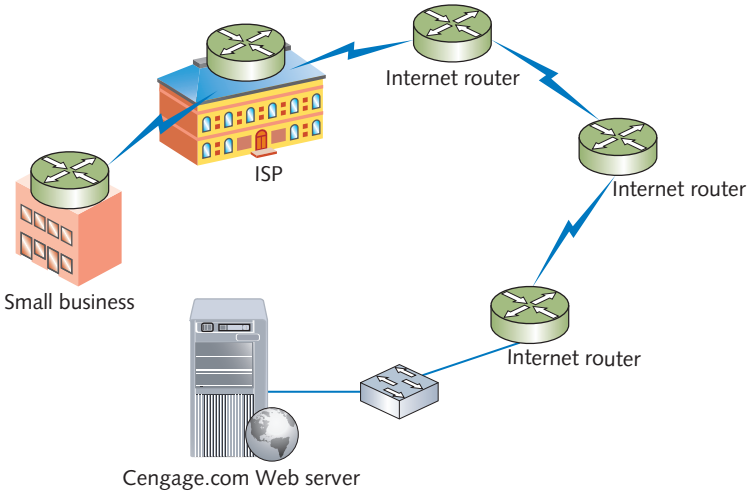

Figure 2-16 Routers interconnect LANs to form the Internet

Note

Recall from Chapter 1 that a cloud is usually shown in network diagrams to represent the complex web of routers and devices that make up the Internet.

On the surface, it might seem as though switches and routers perform a similar function, but in reality, they have very different jobs to do and how they work with network data differs substantially. The following points summarize the key properties and features of a router versus a switch:

- Routers connect LANs, switches connect computers.
- Routers work with logical (IP) addresses, switches work with physical (MAC) addresses.
- Routers work with packets, switches work with frames.
- Routers don't forward broadcast packets, switches do.
- Routers use routing tables, switches use switching tables.

The following sections discuss how and why routers are used to connect LANs and how routers use routing tables.

Routers Connect LANs

Switches are the devices of choice to connect computers to create a LAN. However, if you look at a LAN as a group of people with similar interests getting together to converse and share information, there's a point at which the group can become too large for effective communication. For example, in most group discussions, several conversations often occur at once, but periodically, someone wants to speak to the entire group. For small groups with tightly coupled interests, this method works well, but as the group gets larger, the frequency of group announcements can affect the flow of communication adversely. This is particularly true when only a small subset of the group is interested in the announcement, yet the whole group must stop to listen. In this case, communication can be enhanced by dividing the large group into smaller groups of similar interests in different locations. By doing so, group announcements are contained to a smaller group and need not interrupt other groups' conversations. You can look at these announcements as network broadcast frames that switches (and hubs) are obliged to forward to all connected stations.

Breaking a large group into smaller groups works well until a member of one group must communicate with a member of another group. A messenger could be used to get a message from one group to another and would normally forward only messages directed to a person in another group, not announcements to the entire group. This messenger is analogous to a router in an internetwork. Like the messenger, the router doesn't forward announcements (broadcasts); it forwards only messages destined for a particular address.

Examine Figure 2-17, which shows a large LAN with all workstations and servers connected via switches. All these switches are interconnected through the switch the servers are on. This arrangement works fine if the number of workstations on each switch doesn't exceed about 20, making a total of about 60 workstations. However, if each switch has as many as 50 stations connected (making 150 total workstations), announcement messages (broadcasts) will probably start affecting communication efficiency. Remember that each time a computer sends a broadcast frame, the switch forwards it out all connected ports so that all computers eventually receive the broadcast. One deleterious effect of broadcast frames is that when a computer receives a broadcast, a CPU interrupt occurs, causing the computer to stop what it's doing to

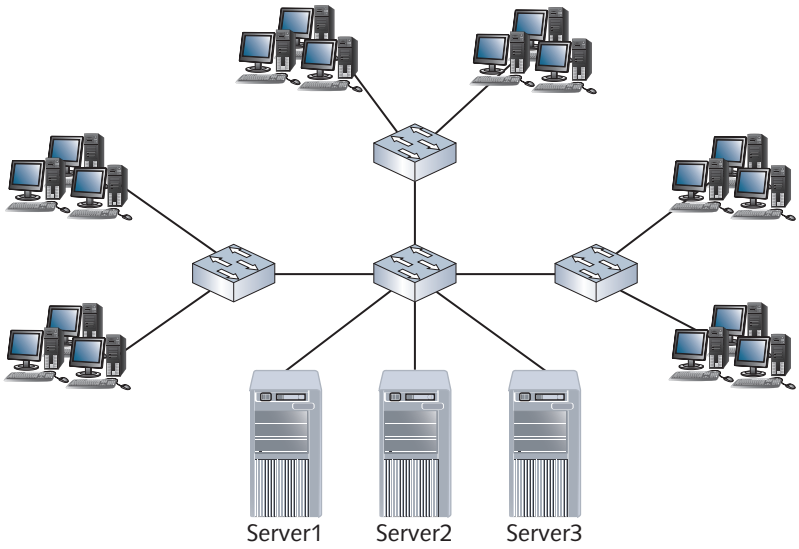

Figure 2-17 A large LAN connected by switches

service the interrupt. If enough interrupts occur in a short period because of many broadcast frames, the computer's overall performance can suffer as a result of the CPU having to service the interrupt and process the broadcast.

Now look at Figure 2-18, in which the network has been redesigned for efficiency. Workstations have been organized so that each department's users are

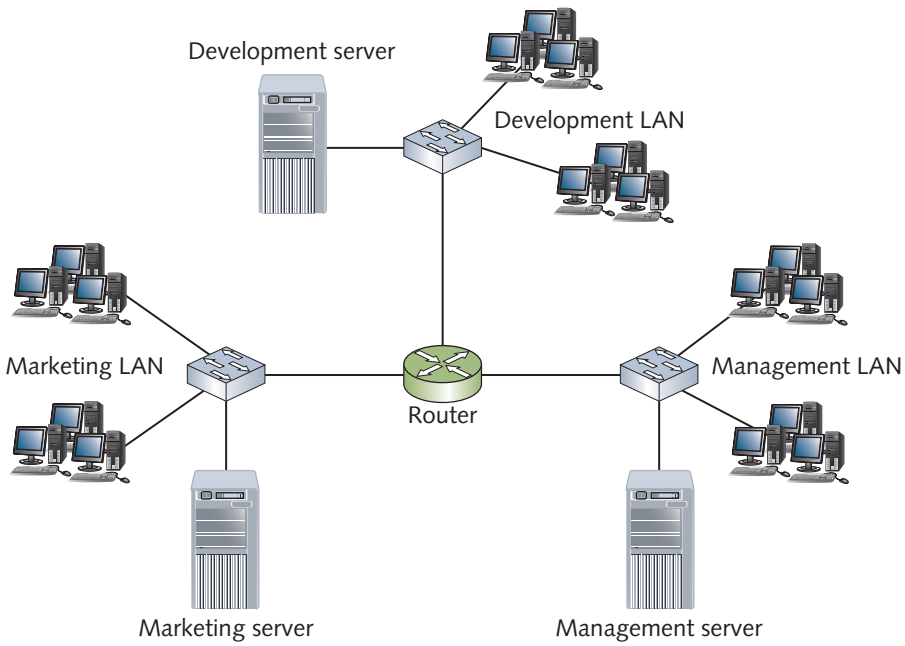

Figure 2-18 Three smaller LANs connected by a router

grouped together, and servers have been configured so that each department's frequently accessed documents and applications reside on the departmental server. In this arrangement, the switches for each LAN allow all computers in the LAN to communicate with one another and forward important broadcast frames so that all computers receive the announcement, but broadcasts aren't forwarded to other LANs because the router doesn't forward broadcast frames. However, the router does allow communication between LANs so that if a computer on the Management LAN needs to access data on the Marketing server, it can do so.

Routers Create Broadcast Domains

The scope of devices to which broadcast frames are forwarded is called a **broadcast domain**. Because routers don't forward broadcasts, router interfaces are the delimiter for broadcast domains. In other words, each router interface in a network creates another broadcast domain. Figure 2-19 shows the same network as Figure 2-18, with

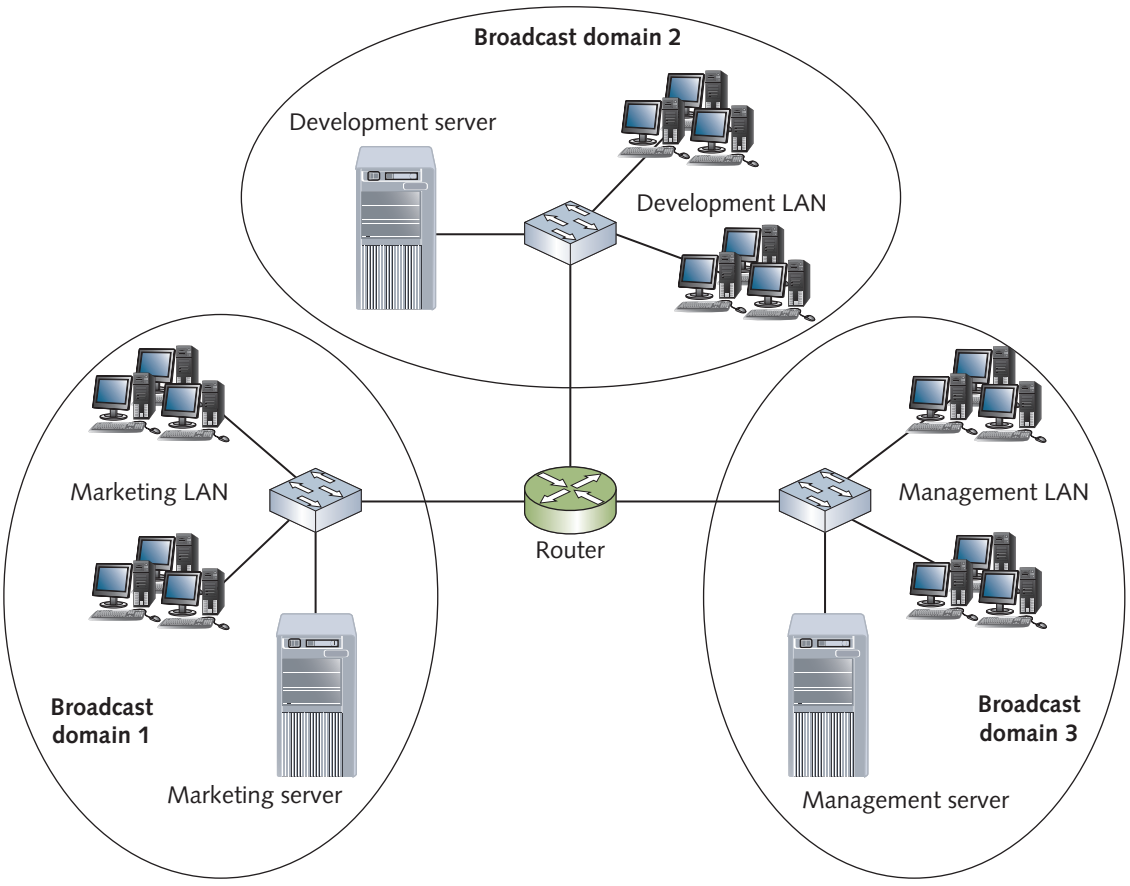

Figure 2-19 Each router interface creates a broadcast domain

circles around each broadcast domain. (Note that Figure 2-17, with no routers at all, is a single broadcast domain.) Chapter 8 describes broadcast domains and how to create them with advanced switch features.

Routers Work with IP Addresses and Routing Tables

Switches, as you know, maintain a switching table of MAC address/switch port pairs to determine where to forward frames in a LAN. Routers maintain routing tables composed of IP network address and interface pairs to determine where to forward packets in an internetwork.

Routers have two or more interfaces, with each interface connected to a different network. When a router receives a packet on one interface, it looks at the destination IP address in the packet to determine to which network the packet is addressed. Then it forwards the packet out of the interface that its routing table indicates is the best way to get the packet to its destination. Figure 2-20 shows the same internetwork as Figure 2-19, with each LAN assigned a network number, and an example of what the routing table might look like. The router's three interfaces are labeled EthA, EthB, and EthC.

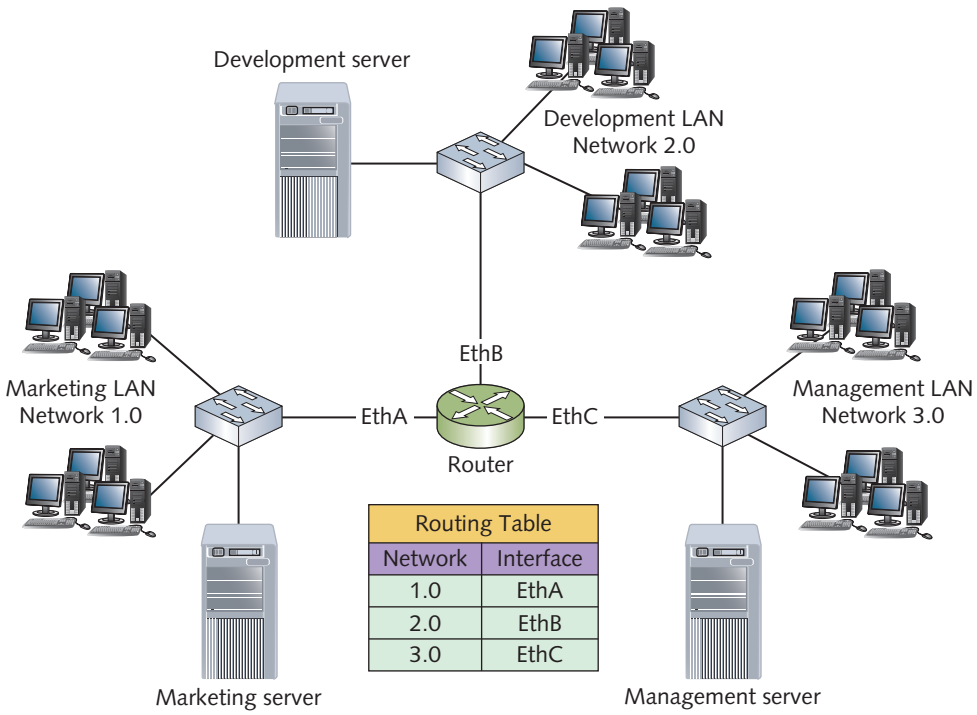

Figure 2-20 An internetwork with a routing table

When the router receives a packet from a computer in Network 1.0 that has a destination address of a computer in Network 3.0, the router looks in its routing table and discovers that Network 3.0 can be found via the EthC interface. The router then forwards the packet out its EthC interface to reach the intended computer.

This routing table has been simplified for demonstration purposes; routing tables have more information than simply the network number and interface name. In addition, network numbers are derived from IP addresses and contain more numbers than shown. Chapter 8 has additional details about how routers work, and Chapter 6 discusses IP addresses and network addresses in more depth.

You might wonder what happens when a router isn't connected to the network to which the packet is addressed. Figure 2-21 illustrates this situation and shows what the routing table would look like on each router between the source and destination networks. In this example, if a computer on Network 1.0 sends a packet to a computer on Network 5.0, router R1 receives the packet and looks up Network 5.0 in its routing table. According to its routing table, it forwards the packet out its WAN A interface. Router R2 receives the packet and forwards it out the router's WAN B interface, as specified by its routing table, and finally, router R3 receives the packet and forwards it out the EthA interface to the destination computer.

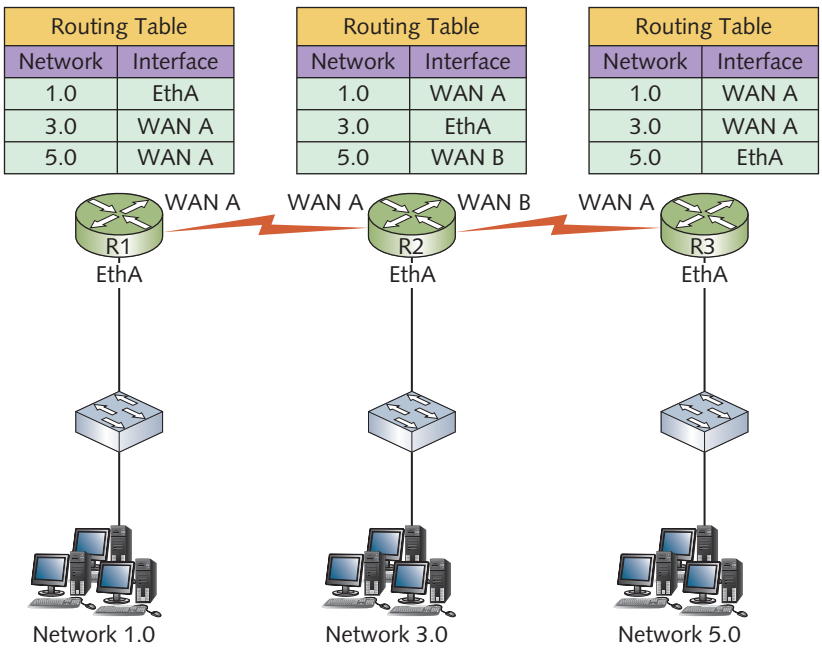

Figure 2-21 Packets are forwarded through multiple routers

Default Routes

Routers on a corporate network might have a routing table entry for every network in the organization, but what about routers connected to the Internet? The Internet is composed of millions of networks, and routers on the Internet are responsible for getting packets from any network to any other network. Although it might be technically possible for routers to have a record of every network in the Internet, having such large routing tables isn't practical. To solve this dilemma, routers can have a special routing table entry called a **default route**, which tells a router where to send a packet with a destination network that can't be found in its routing table. The default route leads to another router and perhaps another router and so on, until the packet reaches a router that has the network address in its routing table.

Network Unreachable

Most routers are configured with a default route, but not always. If a router receives a packet with a destination network address that isn't in its routing table and no default route is configured, the router simply discards the packet. The router may also send a message to the sending station informing it that the network is unreachable. By doing so, the sender is made aware that the destination network doesn't exist or the routers must be configured differently to access the destination network.

Default Gateway

Just as a router must know where to forward a packet it receives, a workstation must know when to send a packet to the router instead of simply addressing the packet and sending it to the local LAN. When a workstation has a packet ready to send, it compares its own IP address with the destination IP address in the packet. If the two addresses are on the same network, the workstation gets the destination computer's MAC address and sends the frame to the local LAN to be delivered to the destination. If the two addresses are on separate networks, the workstation must instead get the router's MAC address and send the frame to the router, which then tries to get the packet to the destination network. In this case, the workstation must know the address of a router. The **default gateway** in a computer's IP address settings must be set to the address of a router to which the computer can send all packets destined for other networks. If the default gateway doesn't have a valid address of a router, the computer can communicate only with computers on the same LAN. In Chapter 5, you learn more about how a computer determines its network address.

This chapter has explained the basic operation of the most common network hardware components. There's more to learn about all these components, but before you delve deeper into network hardware, examining other aspects of networking is helpful. The next several chapters discuss network topologies and technologies, network media, protocols, and networking standards, among other topics. In Chapter 8, we'll delve deeper into network devices like switches and routers.

Hands-On Project 2-5: Communicating over a Router

Time Required: 20 minutes
Objective: Configure workstations to communicate with one another through a router.
Required Tools and Equipment: Three lab computers, two switches, a router, and five patch cables
Description: This project requires some setup by your instructor. You should verify with your instructor that it's complete before starting this project. In this project, you configure workstations to communicate with one another through a router. The router is configured to support two networks: 192.168.1.0 and 192.168.2.0. Computer1 and Computer2 are configured to operate in the 192.168.1.0 network, and Computer3 is configured to work in the 192.168.2.0 network. Figure 2-22 shows the network setup, in which all three computers are connected to the same switch. Cable the network as shown. The router should already be configured.

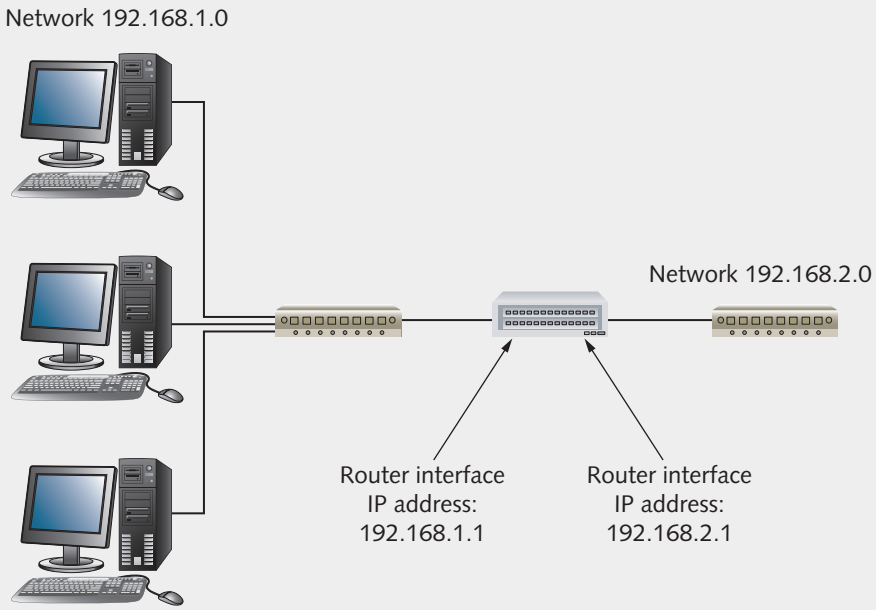

Figure 2-22 Network setup for Hands-On Project 2-5

1. Start all three computers. To configure the IP address of each computer, right-click **Start**, click **Run**, type **ncpa.cpl**, and press **Enter** to open the **Network Connections** control panel. Right-click **Ethernet0** and click **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Use the following IP address**. For now, just set the IP address and subnet mask, using the following values:
   - Computer1: IP address **192.168.1.11**, subnet mask **255.255.255.0**
   - Computer2: IP address **192.168.1.12**, subnet mask **255.255.255.0**
   - Computer3: IP address **192.168.2.21**, subnet mask **255.255.255.0**

2. After you have entered these values, click **OK** twice and close all windows.
3. To test your configuration, open a command prompt window on Computer1 and Computer2, and ping each other's IP address. The ping should be successful. If it's not, verify that the IP address settings are correct by typing `ipconfig`, pressing **Enter**, and comparing the values with the ones listed in Step 1. From both computers, type `ping 192.168.1.1` and press **Enter** to verify that they can communicate with the router.
4. On Computer1, ping Computer3 by typing `ping 192.168.2.21` and pressing **Enter**. You should get a message that the ping failed or timed out. The reason is that the two computers are configured to be on different networks. In this case, Computer1 is configured to be on network 192.168.1.0, and Computer2 is configured to be on network 192.168.2.0. When two computers are configured to be on separate networks, their connection to each other must be separated by a router. Move Computer3 to the other network by plugging the cable from Computer3 into the other switch so that your network configuration now looks like Figure 2-23.

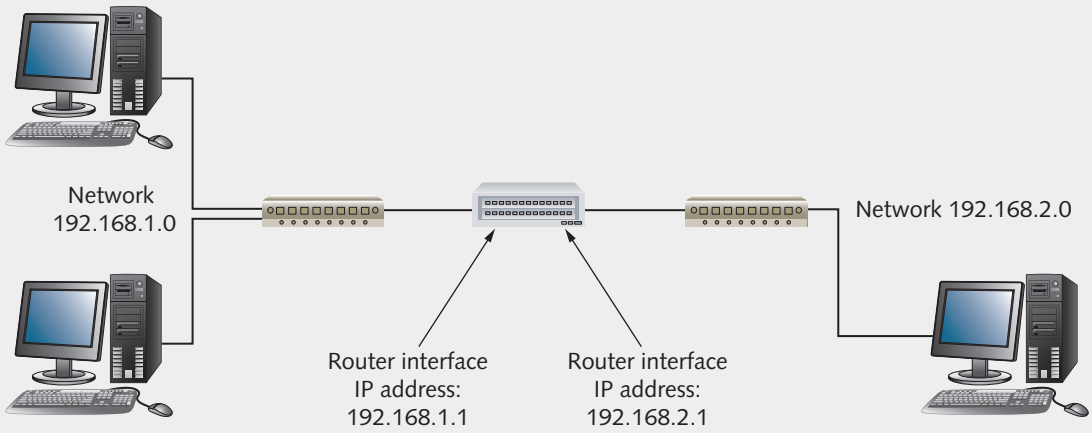

Figure 2-23 Corrected network setup

5. Try the ping again from Computer1 to Computer3. Again, you get an error because one piece of the IP address configuration has been omitted. When a computer needs to send a packet to a device on another network, it must know the address of the router to which to send the packet. This address is called the "default gateway." To set the default gateway for all three computers, follow the instructions in Step 1 to get to the IP settings. In the "Default gateway" text box, enter the following values:
   - Computer1: **192.168.1.1**
   - Computer2: **192.168.1.1**
   - Computer3: **192.168.2.1**

6. After you have finished configuring the default gateway for all three computers, you should be able to ping from Computer1 to Computer3 and from Computer2 to Computer3 and vice versa. Try it now, and write down your results:

_____

_____

7. Next, try another command that shows the route your packet travels to get to the other computer. From Computer1 and Computer2, type `tracert 192.168.2.21` and press **Enter**. From Computer3, type `tracert 192.168.1.11` and press **Enter**. You'll see a few lines of output showing that the packet had to travel through the router to get to its destination. This command is used again in the next project.
8. Close all open windows on all three computers.

Hands-On Project 2-6: Using Traceroute to See How Packets Travel through the Internet

Time Required: 10 minutes
Objective: Use the traceroute program to see the routers that packets must travel through to get from your computer to a destination on the Internet.
Required Tools and Equipment: Net-*XX* and Internet access
Description: The importance of routers is clear when you need to access servers on the Internet. The traceroute program (tracert.exe) lists each router your packets must travel through between your computer and an Internet server.

1. Log on to your computer as **NetAdmin**, if necessary, and open a command prompt window.
2. Type `tracert www.yahoo.com` and press **Enter**. You should see output that's similar to Figure 2-24, but the details will vary, depending on your location. In this output, there are five columns of information. The first column is just a count of how many routers the packet traversed. The second, third, and fourth columns show the amount of time in milliseconds (ms) the router took to respond. Three packets are sent, so three times are listed. The last column is the router's IP address or name and IP address.
3. You can garner some information about the geography of the path your packet took by looking at the router's name. For example, in Figure 2-24, the domain name of the first router is yc-cnt.edu, which is a router at Yavapai College in Prescott, Arizona, where this book has been written. Other routers have the domain name yahoo.com, which tells you that the router is on Yahoo's network. You get the idea. However, looking up router names can sometimes make the trace run slowly. To do the same trace without looking up names, type `tracert -d www.yahoo.com` and press **Enter**. This time, you should see only the IP address of each router.

```
C:\Users\gtomsho>tracert www.yahoo.com

Tracing route to atsv2-fp-shed.wg1.b.yahoo.com [98.137.246.8]
over a maximum of 30 hops:

  1     6 ms    <1 ms    <1 ms  cntrouter.yc-cnt.edu [172.31.1.250]
  2    63 ms    68 ms    83 ms  172.16.0.1
  3     1 ms     1 ms    <1 ms  198.60.126.30
  4     1 ms     1 ms     1 ms  198.60.121.20
  5     6 ms    10 ms    14 ms  206.207.5.1
  6     6 ms     6 ms     6 ms  206.207.226.130
  7    15 ms     5 ms     6 ms  et-8-0-0.1020.rtsw.phoe.net.internet2.edu [198.71.47.195]
  8    14 ms    14 ms    15 ms  lsan0.tr-cps.internet2.edu [206.223.123.199]
  9    15 ms    15 ms    15 ms  exchange-cust1.la1.equinix.net [206.223.123.16]
 10    14 ms    15 ms    14 ms  UNKNOWN-216-115-102-X.yahoo.com [216.115.102.184]
 11    24 ms    33 ms    21 ms  et-8-1-1.pat1.sjc.yahoo.com [216.115.107.150]
 12    39 ms    38 ms    39 ms  ae-3.pat2.swp.yahoo.com [216.115.96.57]
 13    44 ms    44 ms    44 ms  ae-5.pat1.gqb.yahoo.com [216.115.101.111]
 14    43 ms    42 ms    42 ms  et-19-1-0.msr2.gq1.yahoo.com [66.196.67.111]
 15    42 ms    42 ms    42 ms  et-19-1-0.clr1-a-gdc.gq1.yahoo.com [67.195.37.95]
 16    42 ms    42 ms    42 ms  et-16-6.bas2-2-flk.gq1.yahoo.com [98.137.120.14]
 17    44 ms    44 ms    43 ms  media-router-fp2.prod1.media.vip.gq1.yahoo.com [98.137.246.8]

Trace complete.

C:\Users\gtomsho>
```

Figure 2-24 Output of the `tracert` command

4. Try using traceroute and various Web sites to determine the path packets take to other destinations. Try **books.tomsho.com**, and for a destination on the East Coast, try **www.cengage.com.** For a destination in Germany, try **www.kontron.de.** If the trace repeatedly times out (as indicated by a * symbol in the output), press **Ctrl**+**C** to stop the trace.
5. Close the command prompt window and shut down your computer, unless you're continuing to the critical thinking activities at the end of the chapter.

Chapter Summary

- Network repeaters and hubs take incoming bit signals and repeat them at their original strength out all connected ports. A hub is just a multiport repeater. Hubs are a central connecting device for multiple computers, but because hubs allow only one device to communicate at a time, the bandwidth of each port must be shared between all connected computers.
- Network switches interconnect multiple computers, just as hubs do. However, instead of simply regenerating incoming bit signals and repeating them to all other ports, a switch reads the destination MAC address in the frame, determines which port the destination device is connected to, and forwards the frame to only that port.

- Switches use switching tables to determine which MAC address can be found on which port. Switches can operate in full-duplex mode, allowing connected devices to both transmit and receive data simultaneously. Hubs operate only in half-duplex mode.
- Access points are central devices in wireless networks and perform similar functions to hubs. An AP requires devices to use an RTS signal when they want to transmit data, and the AP responds with a CTS signal when it's okay to transmit. This extra network traffic reduces the effective bandwidth of wireless networks.
- Network interface cards create and mediate the connection between the computer and the network medium. A computer's MAC address is defined on the NIC as a burned-in address. The NIC reads each frame arriving on the network medium and determines whether the frame's destination address matches its MAC address. If it matches or is a broadcast frame, the NIC processes the frame; otherwise, it's discarded.
- Wireless NICs perform the same function as wired NICs. Wireless NICs must be selected to match the wireless standard supported on the AP. When a wireless client connects to an AP, it uses the SSID to identify the wireless network's name.
- Routers connect LANs to one another and forward packets from one LAN to another, according to the destination IP address specified in the packet. Routers use routing tables to determine where to forward packets.
- Unlike hubs and switches, routers don't forward broadcast frames. Each interface on a router is the delimiter for a broadcast domain. When a router receives a unicast frame, it reads the destination IP address and compares it with the list of networks in its routing table. If a match is found, the router forwards the packet to the destination network or to another router that gets the packet to its destination. If no match is found, the router discards the frame. If a router has a default route defined, it forwards any packets that don't match networks in its routing table to the default route.

Key Terms

access point (AP)
bandwidth sharing
broadcast domain
broadcast frame
clear to send (CTS)
dedicated bandwidth
default gateway
default route
full-duplex mode
half-duplex mode
hub
network bandwidth
network interface card (NIC)
promiscuous mode
repeater
request to send (RTS)
router
service set identifier (SSID)
switch
switching table
unicast frame
uplink port
uplinking

Review Questions

1. Which of the following is a limitation of early networks that used a daisy-chain method of connecting computers? (Choose two.)
   a. Total number of computers that could be connected
   b. The processing speed of the computers connected
   c. Cable length
   d. No Internet access
2. Which of the following is true of a repeater?
   a. Receives frames and forwards them
   b. Determines to which network to send a packet
   c. Receives bit signals and strengthens them
   d. Has a burned-in MAC address for each port
3. Which of the following is true of a hub? (Choose two.)
   a. Usually has just two ports
   b. Transmits regenerated signals to all connected ports
   c. Usually has four or more ports
   d. Works with MAC addresses
4. Which of the following is the unit of measurement by which a network device's bandwidth is usually specified?
   a. Bytes per second
   b. Bits per second
   c. Packets per second
   d. Bytes per minute
5. Which of the following is a step in the operation of a switch? (Choose two.)
   a. Reads source and destination IP addresses
   b. Reads source and destination MAC addresses
   c. Updates the switching table with destination IP address and port information
   d. Looks up the destination MAC address in its switching table
6. What unit of information do switches work with?
   a. Frames
   b. Bits
   c. Packets
   d. Bytes
7. Which of the following describes how devices connected to a switch use the bandwidth of the switch?
   a. Dedicated bandwidth
   b. Half-duplex bandwidth
   c. Half-scale bandwidth
   d. Shared bandwidth
8. Which element of incoming data does a switch use to create its switching table?
   a. Source IP address
   b. Destination logical address
   c. Destination physical address
   d. Source MAC address
9. What purpose does the timestamp serve in a switching table?
   a. Tells the switch when to forward a frame
   b. Tells the switch how long to wait for a response
   c. Tells the switch when to delete an entry
   d. Tells the switch how long it has been running

10. What feature of a switch allows devices to effectively communicate at 200 Mbps on a 100 Mbps switch?
    a. Uplink port
    b. Full-duplex mode
    c. Shared bandwidth
    d. Bit strengthening
    e. Frame doubling

11. To which device is a wireless access point most similar in how it operates?
    a. Hub
    b. Switch
    c. NIC
    d. Router

12. What's the purpose of an RTS signal in wireless networking?
    a. It allows the AP to request which device is the transmitting station.
    b. It allows the AP to tell all stations that it's ready to transmit data.
    c. It allows a client to notify the AP that it's ready to send data.
    d. It allows a client to request data from the AP.

13. Which of the following is a common operating speed of a wireless access point?
    a. 10 Kbps
    b. 110 Gbps
    c. 600 Kbps
    d. 54 Mbps

14. Which of the following is a task performed by a NIC and its driver? (Choose three.)
    a. Provides a connection to the network medium
    b. Converts bit signals into frames for transmission on the medium
    c. Receives packets from the network protocol and creates frames
    d. Adds a header before sending a frame to the network protocol
    e. Adds error-checking data to the frame

15. Which of the following best describes a MAC address?
    a. A 24-bit number expressed as 12 decimal digits
    b. Two 24-bit numbers, in which one is the OUI
    c. A 48-bit number composed of 12 octal digits
    d. A dotted decimal number burned into the NIC

16. Under which circumstances does a NIC allow inbound communications to pass through the interface? (Choose two.)
    a. The source MAC address is the broadcast address.
    b. The destination MAC address matches the built-in MAC address.
    c. The destination MAC address is all binary 1s.
    d. The NIC is operating in exclusive mode.

17. How does a protocol analyzer capture all frames?
    a. It configures the NIC to capture only unicast frames.
    b. It sets all incoming destination addresses to be broadcasts.
    c. It configures the NIC to operate in promiscuous mode.
    d. It sets the exclusive mode option on the NIC.
    e. It captures only multicast frames.

18. Where do you usually find a MAC address?
    a. In nonvolatile memory on the NIC
    b. In a switch's configuration file
    c. In the routing table
    d. In the header of a packet

19. Which of the following is the purpose of an SSID?
    a. Assigns an address to a wireless NIC
    b. Acts as a unique name for a local area connection
    c. Acts as a security key for securing a network
    d. Identifies a wireless network
20. Which of the following describe the function of routers? (Choose two.)
    a. Forward frames from one network to another.
    b. Connect LANs.
    c. Attach computers to the internetwork.
    d. Work with packets and IP addresses.
21. What information is found in a routing table?
    a. Computer names and IP addresses
    b. Network addresses and interfaces
    c. MAC addresses and ports
    d. IP addresses and MAC addresses
22. You currently have 15 switches with an average of 20 stations connected to each switch. The switches are connected to one another so that all 300 computers can communicate with one another in a single LAN. You have been detecting a high percentage of broadcast frames on this LAN. You think the number of broadcasts might be having an impact on network performance. What should you do?
    a. Connect the switches in groups of five and connect each group of switches to a central hub.
    b. Configure the switches to operate in half-duplex mode.
    c. Reorganize the network into smaller groups and connect each group to a router.
    d. Disable broadcast forwarding on the switches.
23. Which of the following is true about a router versus a switch?
    a. Routers connect LANs, switches connect computers.
    b. Routers work with physical (MAC) addresses, switches work with logical (IP) addresses.
    c. Routers work with frames, switches work with packets.
    d. Routers forward broadcast packets, switches do not.
24. If a router receives a packet with a destination network address unknown to the router, what does the router do?
    a. Sends the packet out all interfaces
    b. Discards the packet
    c. Adds the destination network to its routing table
    d. Queries the network for the destination network
25. Which of the following is true about a router? (Choose two.)
    a. Forwards broadcasts
    b. Uses default routes for unknown network addresses
    c. Forwards unicasts
    d. Is used primarily to connect workstations

Packet Tracer Labs

Packet Tracer Lab 2-1: Using Packet Tracer to See How a Hub Works

Time Required: 10 minutes

Objective: Use Packet Tracer to see how a hub works.

Required Tools and Equipment: You'll need a computer with Packet Tracer installed per the instructions in Challenge Lab 1-1 from Chapter 1, and Packet Tracer file vlab2-1.pkt, which is available from the Cengage Web site. Please see the "Before You Begin" section of this book for instructions on accessing these files.

Description: In this project, you run Packet Tracer to see how a hub works. Figure 2-25 shows the topology for this lab.

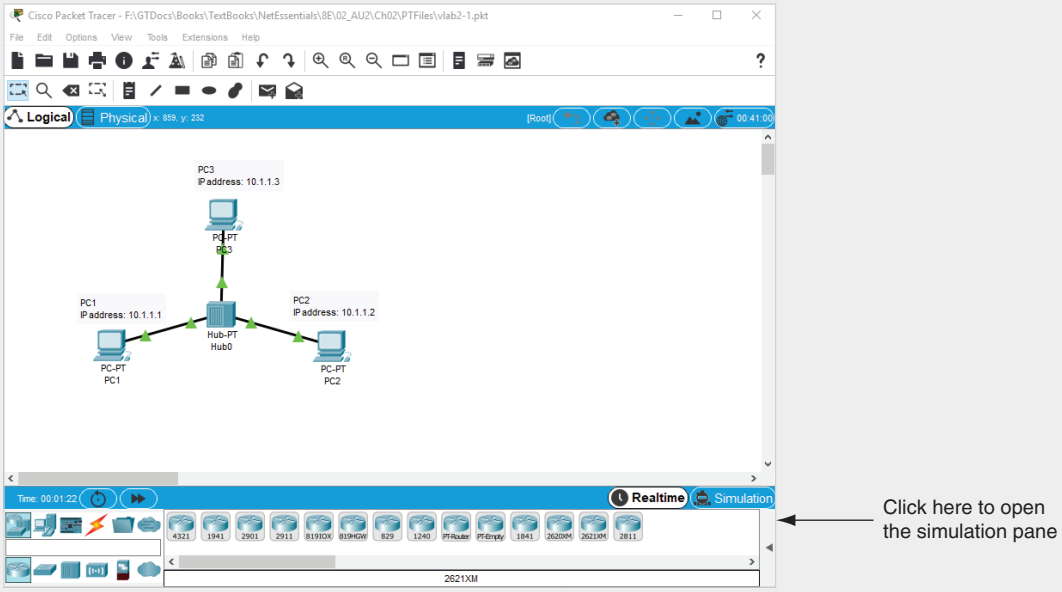

Figure 2-25 Packet Tracer Lab 2-1 topology

Source: Cisco Systems, Inc.

1. Open the vlab2-1.pkt file in Packet Tracer by double-clicking the file.
2. In the lower-right corner of the Packet Tracer window, click the left-pointing arrow to open the simulation pane (see Figure 2-25) so you can see the results of communication attempts between devices.
3. To send a packet from PC1 to PC2, click the **Add Simple PDU** icon (see Figure 2-26).

Note

A PDU is a protocol data unit, which in this case is just another way to say "packet." PDUs are explained in detail in Chapter 7.

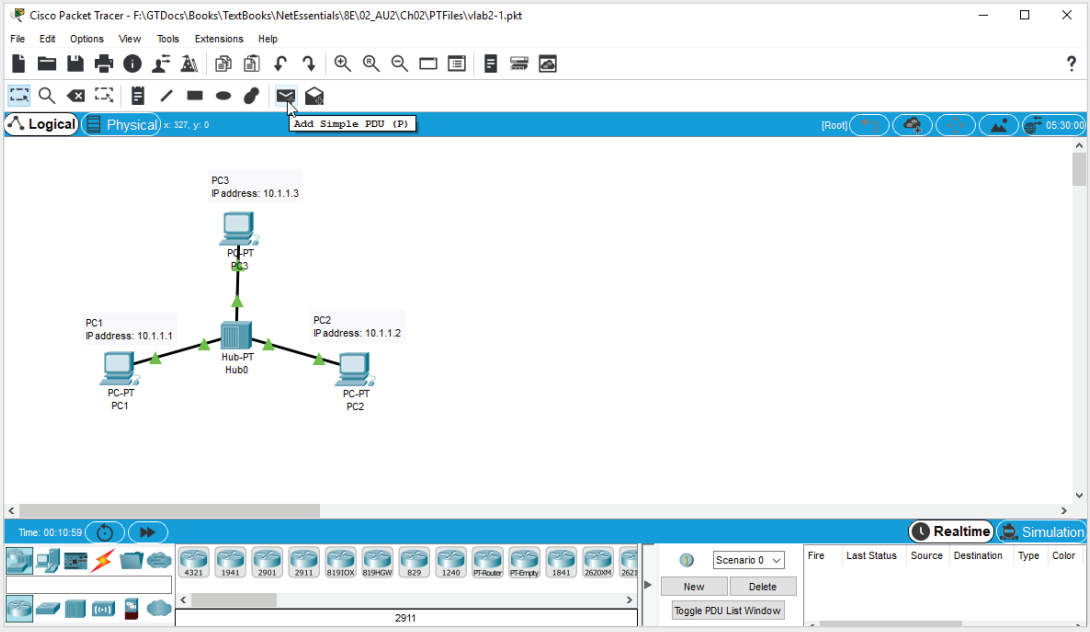

Figure 2-26 Add Simple PDU

Source: Cisco Systems, Inc.

4. Next, click **PC1** and then click **PC2**. The simulation pane in the lower-right corner of the Packet Tracer window reports Successful communication (see Figure 2-27).

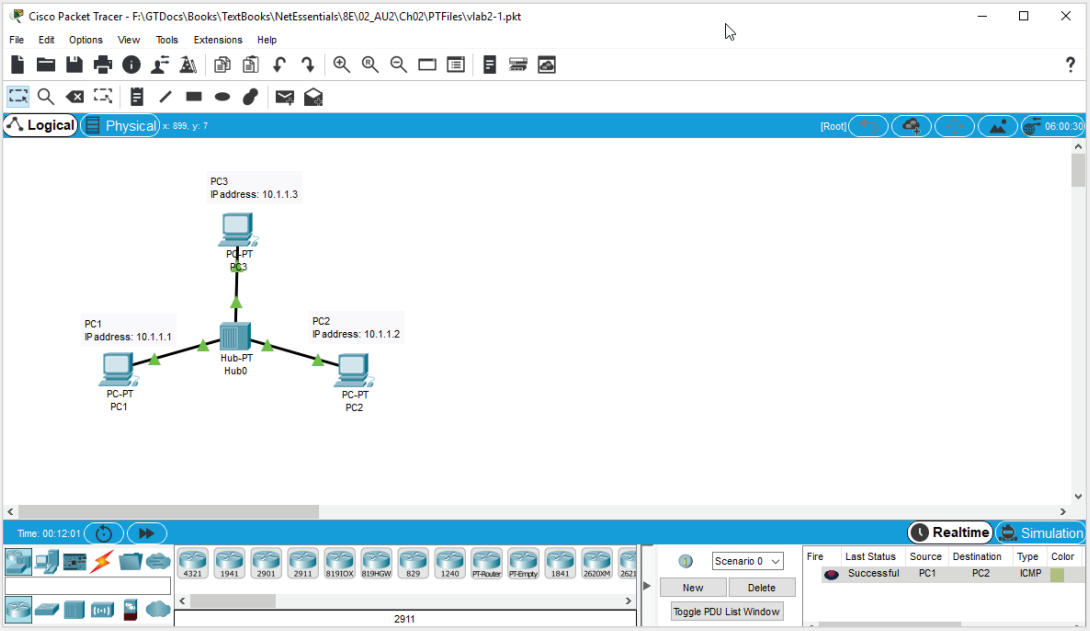

Figure 2-27 Successful communication from PC1 to PC2

Source: Cisco Systems, Inc.

5. Unfortunately, you didn't see anything happen because you're in Realtime mode; packets are sent so fast that you don't see much, except maybe the flicker of the link lights on the network connections. Click the **Simulation** button, which is above the simulation pane and next to the Realtime button, to enter Simulation mode.
6. The Simulation panel opens. For now, you don't need to see this panel, so close it. If you see any packets on the workspace, click the **Delete** button in the simulation pane.
7. To send the packet again in Simulation mode, click the **Add Simple PDU** icon, click **PC1**, and then click **PC2**.

8. You see the packet on PC1. Click the **Capture then Forward** button (see Figure 2-28) to move the packet to the next device. The packet is now at the hub. Click **Capture then Forward** again to move the packet to the next device. Notice that the hub sent two copies of the packet: one to PC2 and one to PC3. That's because the hub repeats all signals it sees to all connected ports. However, the packet at PC3 has a red X, indicating that PC3 discarded the packet because it wasn't meant for PC3.

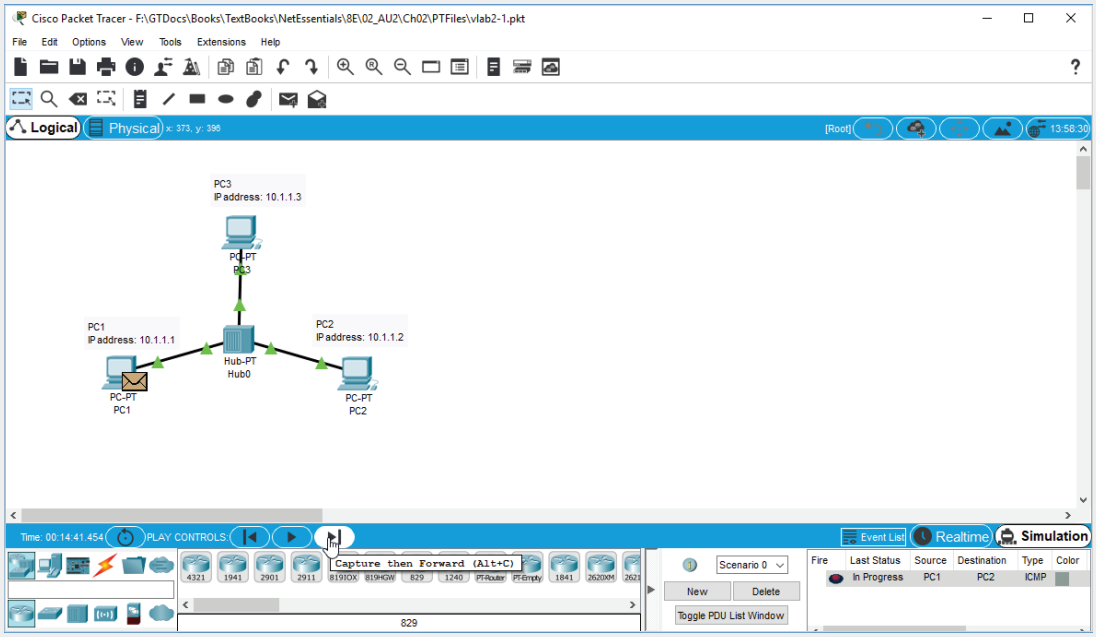

Figure 2-28 Capture and forward a packet

Source: Cisco Systems, Inc.

9. Click **Capture then Forward** again. You see the reply from PC2 go to the hub. Click **Capture then Forward** again to see that the hub repeated the packet to both PC3 and PC1. PC3 again discards the packet. The packet at PC1 has a green check mark, indicating a successful transmission (see Figure 2-29).
10. Close Packet Tracer. Click **No** when you are prompted to save your work.

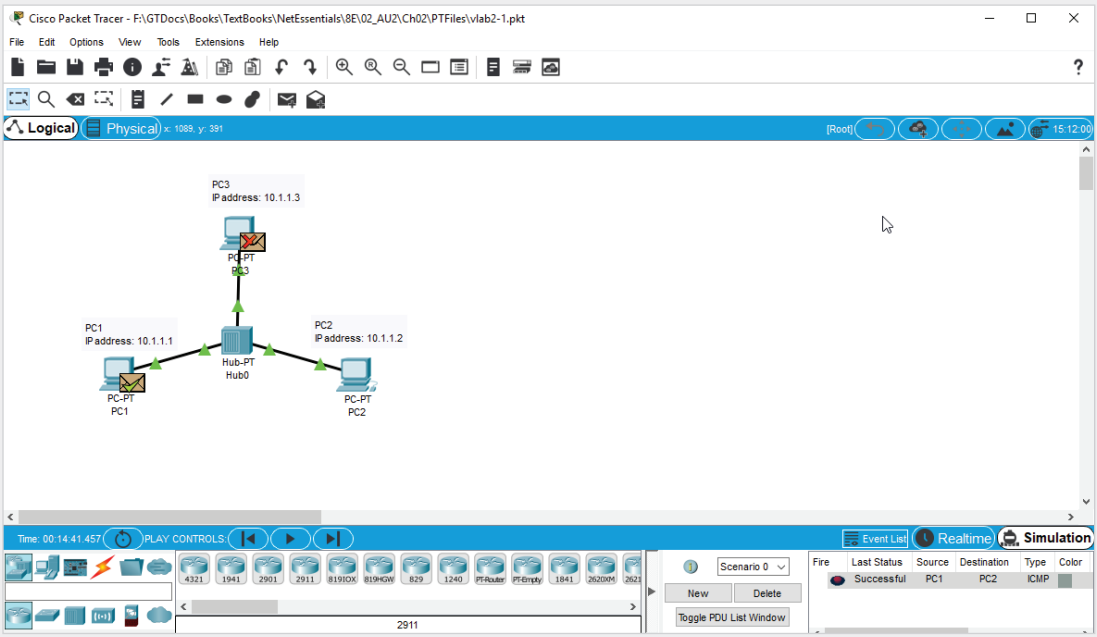

Figure 2-29 A successful transmission from PC1 to PC2 and back again

Source: Cisco Systems, Inc.

Packet Tracer Lab 2-2: Using Packet Tracer to See How a Switch Works

Time Required: 10 minutes

Objective: Use Packet Tracer to see how a switch works.

Required Tools and Equipment: A computer with Packet Tracer installed per the instructions in Challenge Lab 1-1, and Packet Tracer file vlab2-2.pkt, available from the Cengage Web site

Description: In this project, you run Packet Tracer to see how a switch works. Figure 2-30 shows the topology for this lab.

1. Open vlab2-2.pkt in Packet Tracer by double-clicking the file.
2. In the lower-right corner of the Packet Tracer window, click the left-pointing arrow to open the simulation pane so you can see the results of communication attempts between devices.
3. A switch takes a little time before it makes the connection to the network device. Wait until you see two green "lights" on each connection between the switch and the PCs. To send a packet from PC1 to PC2, click the **Add Simple PDU** icon.

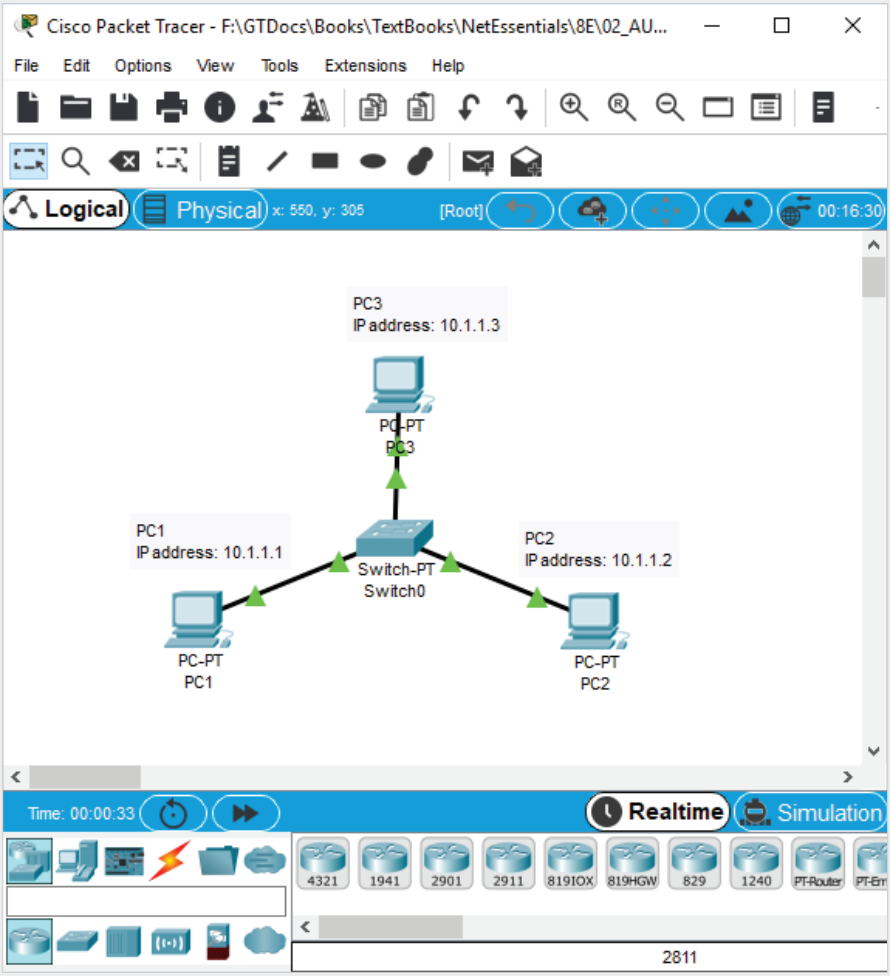

Figure 2-30 Packet Tracer Lab 2-2 topology

Source: Cisco Systems, Inc.

4. Next, click **PC1** and then click **PC2**. The simulation pane in the lower-right corner of the Packet Tracer window reports Successful communication.
5. Click the **Simulation** button to enter Simulation mode.
6. Close the Simulation panel. If you see any packets on the workspace, click the **Delete** button in the simulation pane.
7. Send the packet again in Simulation mode: Click the **Add Simple PDU** icon, click **PC1**, and then click **PC2**.
8. You see the packet on PC1. Click **Capture then Forward** to move the packet to the next device. The packet is now at the switch. Click **Capture then Forward** again to

move the packet to the next device. Notice that the switch only forwards the packet to PC2, in contrast with the hub in the previous lab that forwarded the packet to PC3 as well.

9. Click **Capture then Forward** again. You see the reply from PC2 go to the switch. Click **Capture then Forward** again to see that the switch forwards the packet only to PC1. The packet at PC1 has a green check mark, indicating a successful transmission.
10. To see how the switch knew which port to use to forward the packet to reach PC2, click the **Inspect** icon (which looks like a magnifying glass) in the right pane. Click the switch and click **MAC Table** to view the MAC address table the switch uses to keep track of which devices are connected to its ports (see Figure 2-31). You see that there are two entries, each with a MAC address and a port number.

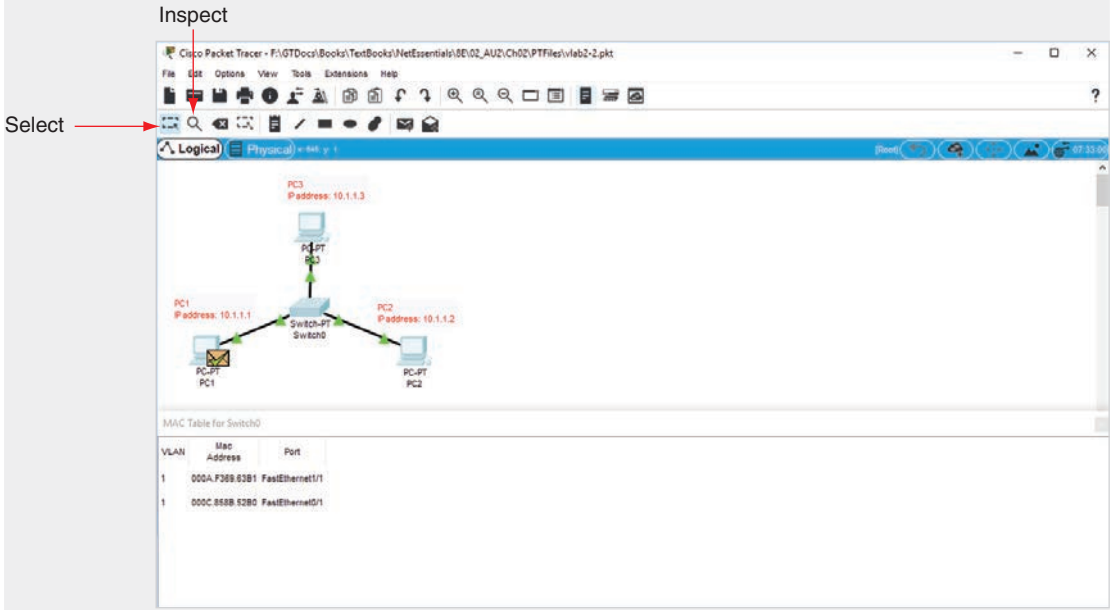

Figure 2-31 A switch's MAC address table

Source: Cisco Systems, Inc.

11. Click the **Select** icon (see Figure 2-31) and hover the mouse over **PC1** to see details about its network configuration (see Figure 2-32). Notice that the MAC address of the Ethernet connection on PC1 matches the MAC address of one of the entries in the MAC table. Hover your mouse over **PC2** and you'll see that PC2's MAC address matches the other entry. There is no entry for PC3 because it has not sent any packets for the switch to learn its MAC address.
12. Close Packet Tracer. Click **No** when you are prompted to save your work.

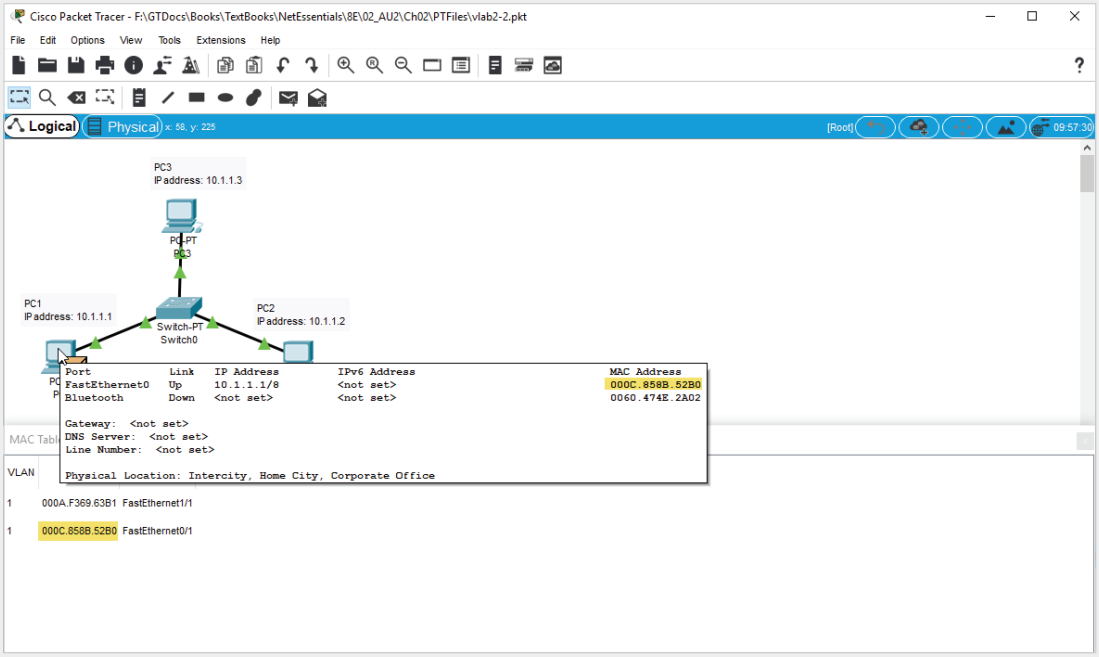

Figure 2-32 Looking at the MAC address of a PC in Packet Tracer

Source: Cisco Systems, Inc.

Packet Tracer Lab 2-3: Using Packet Tracer to Connect to a Wireless Access Point

Time Required: 10 minutes

Objective: Use Packet Tracer to connect to a wireless access point.

Required Tools and Equipment: A computer with Packet Tracer installed and Packet Tracer file vlab2-3.pkt

Description: In this project, you run Packet Tracer to connect to a wireless access point.

1. Open vlab2-3.pkt in Packet Tracer by double-clicking the file. Figure 2-33 shows the topology for this lab.

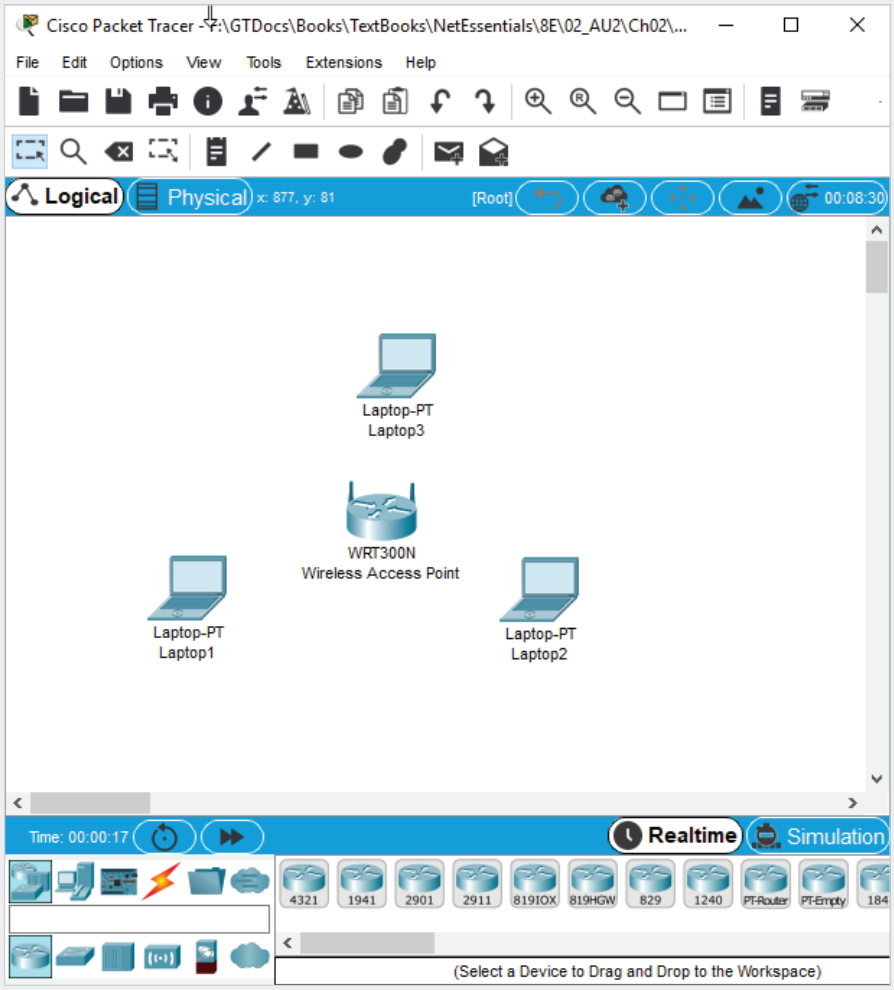

Figure 2-33 Packet Tracer Lab 2-3 topology

Source: Cisco Systems, Inc.

2. Open the simulation pane so you can see the results of communication attempts between devices.
3. The wireless access point (AP) is already configured. You will configure the laptops to connect to the access point. Click **Laptop1** to open its configuration settings.
4. Click the **Config** tab. Then click **Wireless0** in the left pane.
5. In the SSID text box, type **NetEss**, which is the SSID the AP is using. In the Authentication section, click **WPA2-PSK** and type **Networking** in the PSK Pass Phrase text box (see Figure 2-34) to set the authentication and encryption protocol used to communicate with the AP. Close the Laptop1 settings window. You see that Laptop1 has connected to the AP.

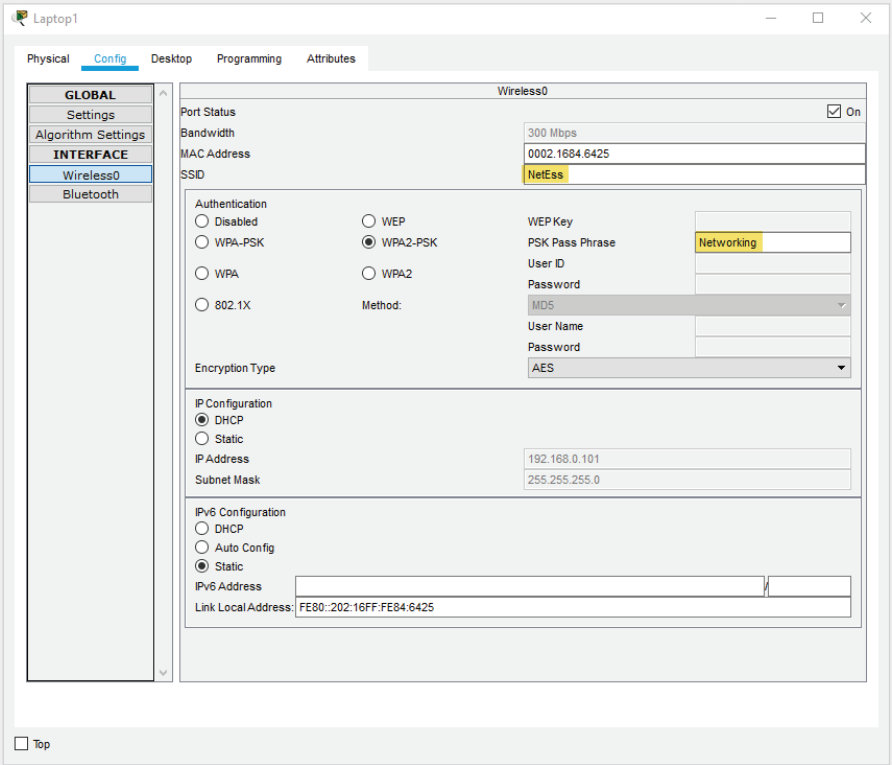

Figure 2-34 Wireless settings for Laptop1

Source: Cisco Systems, Inc.

6. Hover your mouse over **Laptop1**. You should see that it received an IP address from the AP of 192.168.0.101. Repeat steps 3 through 5 for Laptop2 and Laptop3. When you are done, the network should look like Figure 2-35. If any of the laptops don't show the connection graphic to the AP, check and correct the wireless settings on the laptop.
7. Send a simple PDU from any laptop to any other laptop. The results should be successful.
8. Change Packet Tracer to Simulation mode and send the packet again, being sure to click **Capture then Forward** until the results are successful. Notice that an AP acts somewhat like a hub in that all laptops receive the packet; however, with a wireless network, even the sending device receives a copy of its own packet and discards it.
9. Close Packet Tracer. Click **No** when you are prompted to save your work.

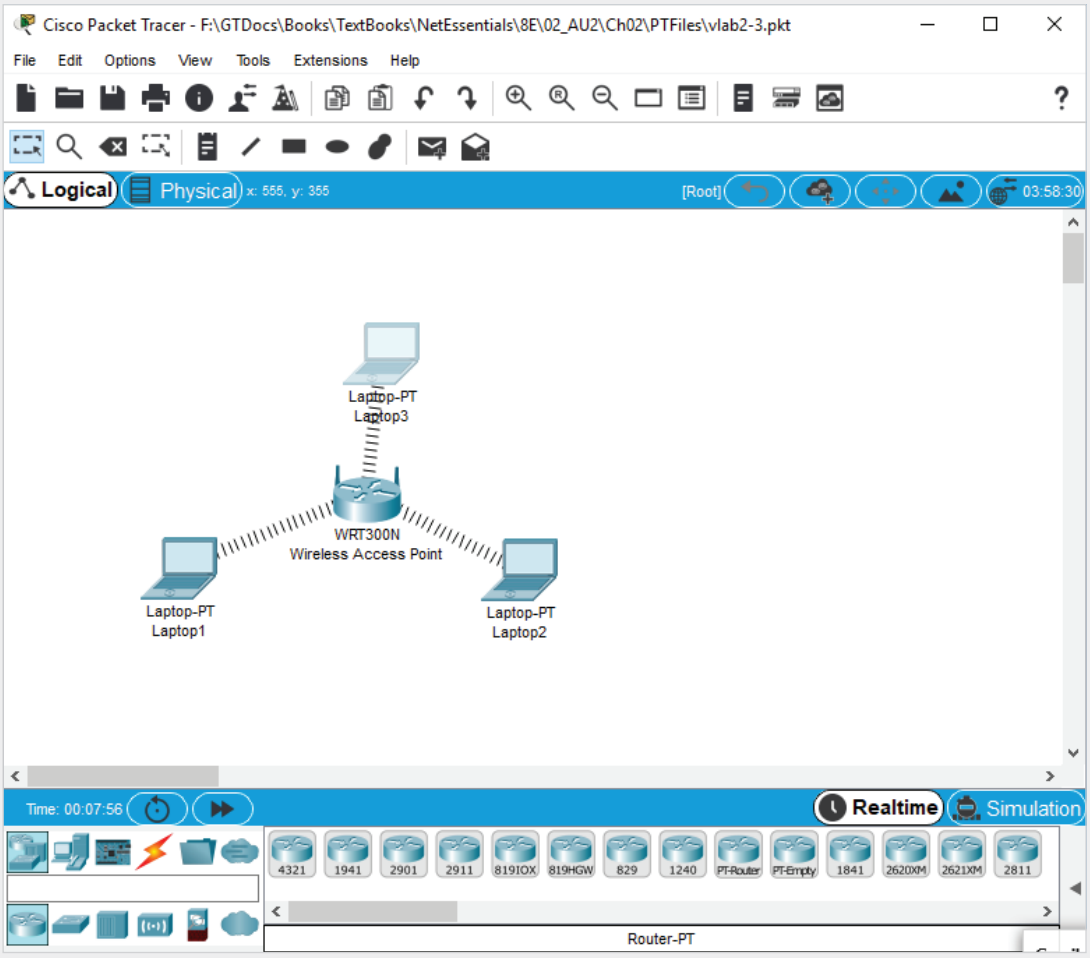

Figure 2-35 A working wireless network in Packet Tracer

Source: Cisco Systems, Inc.

Packet Tracer Lab 2-4: Using Packet Tracer to See How a Router Works

Time Required: 10 minutes

Objective: Use Packet Tracer to see how a router works.

Required Tools and Equipment: A computer with Packet Tracer installed and Packet Tracer file vlab2-4.pkt

Description: In this project, you run Packet Tracer to see how a router forwards packets in an internetwork.

1. Open vlab2-4.pkt in Packet Tracer by double-clicking the file. Figure 2-36 shows the topology for this lab.
2. Open the simulation pane so you can see the results of communication attempts between devices.

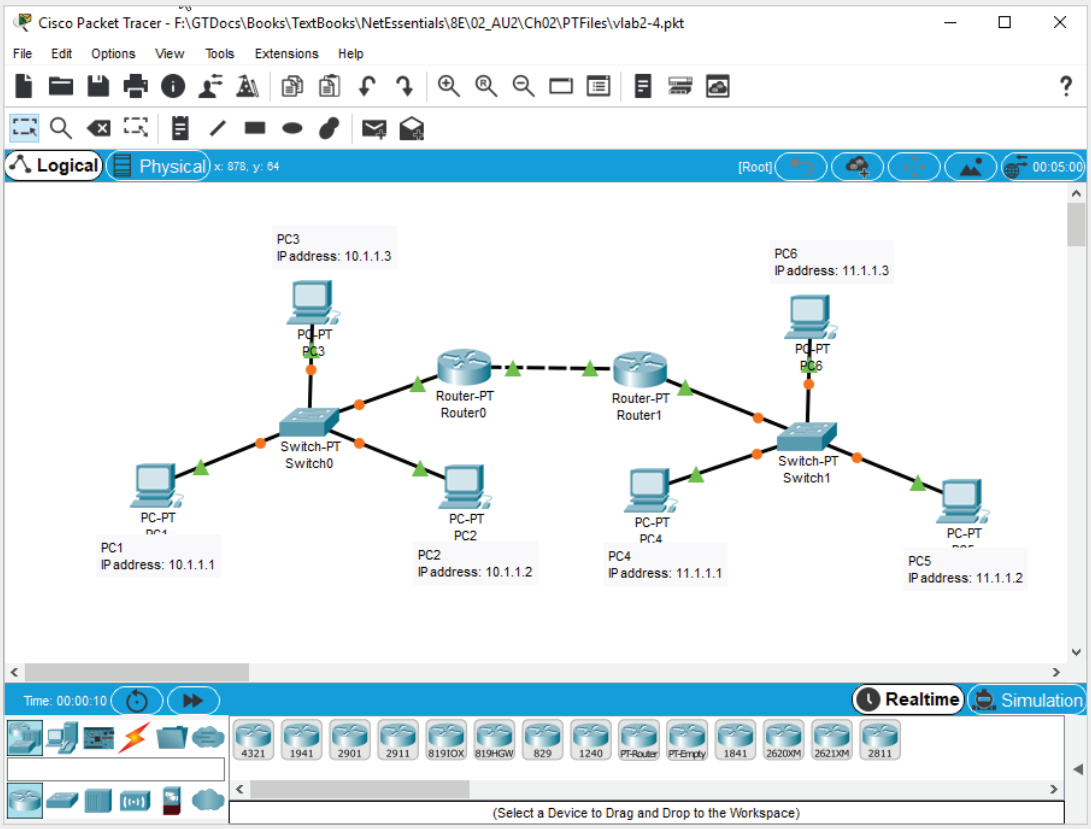

Figure 2-36 Packet Tracer Lab 2-4 topology

Source: Cisco Systems, Inc.

3. Send a simple PDU from PC1 to PC5. The results should be successful. If the communication fails, double-click the button under the Fire column in the simulation pane, where you see the results of the communication to send the packet again.
4. Change Packet Tracer to Simulation mode. Send a simple PDU again from PC1 to PC5. The packet is sent from PC1 to Switch0 to Router0, then from Router0 to Router1 to Switch1 to PC5, and then back again. How did Router0 and Router1 know where to send the packet? Click the **Inspect** icon, click **Router0**, and click **Routing Table** to see the routing table.
5. In Router0's routing table, you see three entries, one for each network Router0 knows about. PC5 is on network 11.0.0.0, and the entry in the routing table tells Router0 that it can get to that network by sending packets to address 12.1.1.101, which is the address of Router1. You'll learn much more about routing and routing tables in Chapter 8 and more about network and IP addresses in Chapter 6.
6. Close the routing table for Router0 and inspect Router1's routing table to see that it has an entry for the 10.0.0.0 network, which is where PC1 is located.
7. Close Packet Tracer and click **No** when you are prompted to save your work.

Challenge Packet Tracer Lab 2-5: Communicating across Routers

Note

Challenge Packet Tracer Labs pose a problem and the reader must implement a solution without step-by-step instructions.

Time Required: 15 minutes
Objective: Perform the necessary configuration steps to allow PC1 to communicate with PC2 across the router.
Required Tools and Equipment: A computer with Packet Tracer installed and Packet Tracer file vlab2-5.pkt
Description: In this project, you make the necessary configuration changes so that PC1 and PC2 can communicate across the router. (Hint: A change is required on both PC1 and PC2.)

Critical Thinking

The following activities give you critical thinking challenges. Challenge labs give you an opportunity to use the skills you have learned to perform a task without step-by-step instructions. Case projects offer a practical networking problem for which you supply a written solution.

Challenge Lab 2-1: Determining Whether Your Computer Is Connected to a Hub or Switch

Time Required: 15 minutes
Objective: Use packet information captured with Wireshark to determine whether your computer is attached to the rest of the classroom with a hub or switch.
Required Tools and Equipment: Net-*XX*
Description: You saw the difference between hubs and switches in earlier projects. Specifically, you saw which packets Wireshark captured when your computer was connected to a hub versus a switch. In this challenge lab, work with your classmates to set up a test that determines whether classroom computers are connected to a hub or switch. Write a short memo to your instructor to address the following questions:

- What filter options (if any) did you configure in Wireshark?
- What commands did you use to generate packets on the network?
- What IP addresses did you attempt to communicate with?
- What was your result? Is your computer attached to a hub or switch? Why did you come to this conclusion?

Challenge Lab 2-2: Capturing Traceroute Packets

Time Required: 15 minutes

Objective: Use Wireshark to capture traceroute packets.

Required Tools and Equipment: Net-*XX*

Description: In this challenge lab, you capture packets generated by the traceroute program. You need to determine what types of packets are generated so that you know which types of packets to capture and inspect. Run traceroute (using any Web site you like as the destination) and capture the packets your computer generates and the router responses. Remember, on a PC the traceroute program is run using tracert.exe from the command line. After you have finished this lab, write a short memo that addresses the following questions:

- What type of packets does traceroute use?
- What's the response each router sends back to your computer?
- How does your computer get a response from each router between your computer and the destination?

Tip

You can learn more about how traceroute works by checking out the YouTube video at *https://www.youtube.com/watch?v=G05y9UKT69s* or by doing a Google search for it.

Case Project 2-1

You have been hired by a manufacturing company that has had its network in place for many years. They currently have 50 computers connected to 10 Mbps hubs. You've been asked to upgrade the network. This long-overdue upgrade is necessary because of poor network response time caused by a lot of collisions occurring during long file transfers between clients and servers. How do you recommend upgrading this network? What interconnecting devices will you use, and what benefit will you get from using these devices? Write a short memo describing the upgrade and, if possible, include a drawing of the new network.

Case Project 2-2

Two hundred workstations and four servers on a single LAN are connected by a number of switches. You're seeing an excessive number of broadcast packets throughout the LAN and want to decrease the effect this broadcast traffic has on your network. What steps must you take to achieve this goal?

Case Project 2-3

In Chapter 3, you learn about network topologies and technologies. As preparation, do Internet research on the following topics:

- Physical versus logical topology
- Bus topology
- Star topology
- Ring topology
- Ethernet and CSMA/CD

Write a short explanation (two to three sentences) of each concept and be prepared to discuss it with the class.