CHAPTER 3

NETWORK TOPOLOGIES AND TECHNOLOGIES

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

Describe the primary physical networking topologies in common use

Describe the primary logical networking topologies in common use

Describe major LAN networking technologies

Compare Wi-Fi standards

Not so long ago, there was a real choice to be made between available network topologies and technologies when designing and building a new internetwork. Thankfully, this area of networking has gotten simpler rather than more complex, mainly because the choices have narrowed, with inferior or costly solutions becoming obsolete.

This chapter discusses network topologies, which describe both the physical arrangement of cabling or pathways between network devices and the logical manner in which data is transferred from device to device. Next, you learn about network technologies or architectures that describe the methods computers use to transmit data to the networking medium in an orderly fashion. As you'll see, the topology and technology are often tightly coupled, as certain technologies can be used only with certain topologies. The choices have been limited because only a few combinations of technologies and topologies remain viable. As is often the case, however, it helps to know where networking started to get an idea of where it might be heading. So, even

though some information covered in this chapter is obsolete or nearly so, your understanding of these older technologies will help you better understand current and future technologies. Finally, you learn about 802.11 Wi-Fi standards and methods. Wi-Fi is developing as rapidly as wired Ethernet and is replacing wired LANs as the connection of choice in some environments.

Table 3-1 summarizes what you need for the hands-on projects in this chapter.

Table 3-1 Hands-on project requirements

Hands-on project	Requirements	Time required	Notes
Hands-On Project 3-1: Building a Physical Star Topology Network	Three lab computers, hub, three patch cables	20 minutes	
Hands-On Project 3-2: Determining and Changing Your Ethernet Standard	Two lab computers, switch, two patch cables	15 minutes	
Hands-On Project 3-3: Viewing an Ethernet Frame	Two lab computers, switch, two patch cables	20 minutes	

Physical Topologies

Certification

98-366 Understanding network infrastructures:

Understand wireless networking

Understand network topologies and access methods

The word "topology," for most people, describes the lay of the land. A topographic map, for example, shows the hills and valleys in a region, whereas a street map shows only the roads. A network topology describes how a network is physically laid out and how signals travel from one device to another. However, because the physical layout of devices and cables doesn't necessarily describe how signals travel from one device to another, network topologies are categorized as physical and logical.

The arrangement of cabling and how cables connect one device to another in a network are considered the network's **physical topology**, and the path data travels between computers on a network is considered the network's **logical topology**. You can look at the physical topology as a topographic map that shows just the lay of the land along with towns, with only simple lines showing which towns have pathways to one another. The logical topology can be seen as a street map that shows how people

actually have to travel from one place to another. As you'll see, a network can be wired with one physical topology but pass data from machine to machine by using a different logical topology.

All network designs are based on four basic physical topologies: bus, star, ring, and point-to-point. A bus consists of a series of computers connected along a single cable segment. Computers connected via a central device, such as a hub or switch, are arranged in a star topology. Devices connected to form a loop create a ring topology. Two devices connected directly to each other make a point-to-point topology. Keep in mind that these topologies describe the physical arrangement of cables. How the data travels along these cables might represent a different logical topology. The dominant logical topologies in LANs include switching, bus, and ring, all of which are usually implemented as a physical star (discussed later in "Logical Topologies").

Physical Bus Topology

The **physical bus topology**, shown in Figure 3-1, is by far the simplest topology, and at one time was the most common method for connecting computers. It's a continuous length of cable connecting one computer to another in daisy-chain fashion. One of this topology's strengths is that you can add a new computer to the network simply by stringing a new length of cable from the last computer in the bus to the new machine. However, this strength is countered by some weaknesses:

- There is a limit of 30 computers per cable segment.
- The maximum total length of cabling is 185 meters (607 feet).
- Both ends of the bus must be terminated.
- Any break in the bus brings down the entire network.
- Adding or removing a machine brings down the entire network temporarily.
- Technologies using this topology are limited to 10 Mbps half-duplex communication because they use coaxial cabling, as discussed in Chapter 4.

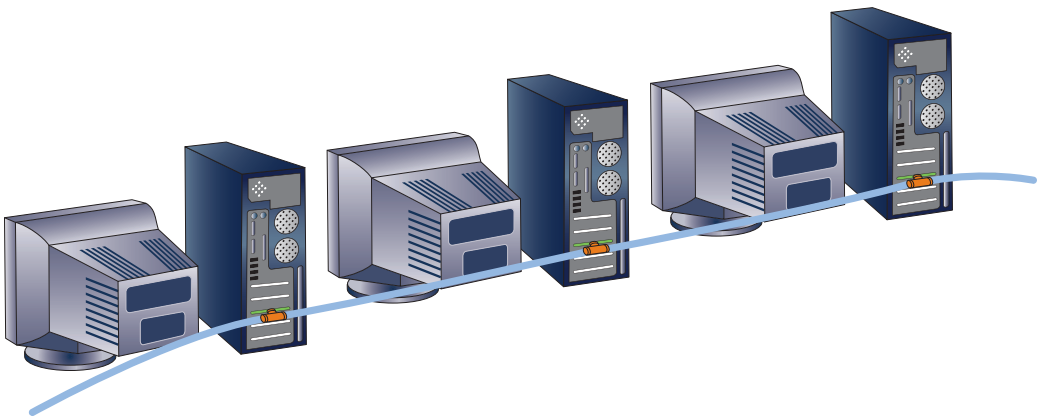

Figure 3-1 A physical bus topology network

Because of the preceding limitations, a physical bus topology is no longer a practical choice, and technology has moved past this obsolete method of connecting computers. However, the original Ethernet technology was based on this topology, and the basis of current LAN technology has its roots in the physical bus. So, your understanding of bus communication aids your general understanding of how computers communicate with one another across a network.

How Data Travels in a Physical Bus

Two properties inherent in a physical bus are signal propagation and signal bounce. In any network topology, computers communicate with one another by sending information across the media as a series of signals. When copper wire is the medium, as in a typical physical bus, these signals are sent as a series of electrical pulses that travel along the cable's length in all directions. The signals continue traveling along the cable and through any connecting devices until they weaken enough that they can't be detected or until they encounter a device that absorbs them. This traveling across the medium is called **signal propagation**. However, even if a signal encounters the end of a cable, it bounces back and travels in the other direction until it weakens or is otherwise impeded.

When a signal hits the end of a cable and bounces back up the cable's length, it interferes with signals following it, much like an echo. Imagine if you were trying to communicate in an empty room with hard walls that caused your voice to echo continuously. The echo from the first words out of your mouth would garble the sound of words that followed, and your message would be unintelligible. The term used when electricity bounces off the end of a cable and back in the other direction is called **signal bounce** (or "reflection"). To keep signal bounce from occurring, you do what you would to keep excessive echo from occurring; you install some type of material at both ends of the medium to absorb the signal. In a physical bus, you install a **terminator**, which is an electrical component called a "resistor" that absorbs the signal instead of allowing it to bounce back up the wire.

Physical Bus Limitations

Now that you know more about how a physical bus works, the previous list of weaknesses needs some additional explanation. The limitation of 30 stations per cable segment means only 30 computers can be daisy-chained together before the signal becomes too weak to be passed along to another computer. As an electrical signal encounters each connected workstation, some of its strength is absorbed by both the cabling and the connectors until the signal is finally too weak for a computer's NIC to interpret. For the same reason, the total length of cabling is limited to 185 meters (607 feet), whether there's one connected station or 30. The network can be extended in cable length and number of workstations by adding a repeater, which, as you know, regenerates the signal before sending it out.

At all times, both ends of the bus must be terminated. An unterminated bus results in signal bounce and data corruption. When a computer is added or removed from the

network, both ends are no longer terminated, resulting in an interruption to network communication.

For a small network of only a few computers, you might think a bus topology is fine, until you consider the last weakness: a maximum bandwidth of 10 Mbps half-duplex communication. A physical bus uses coaxial cable (a cabling type discussed in Chapter 4, similar to what's used in cable TV connections), which is limited to a top speed of 10 Mbps and communication in only half-duplex mode. Most networks now use twisted-pair cabling, which can operate at 1000 Mbps or faster and run in full-duplex mode, so communication between devices is much faster. For all these reasons, the physical bus topology has long since fallen out of favor and been replaced largely by the star topology, which is discussed next.

Physical Star Topology

The **physical star topology** uses a central device, such as a hub or switch, to interconnect computers in a LAN (see Figure 3-2). Each computer has a single length of cable going from its NIC to the central device.

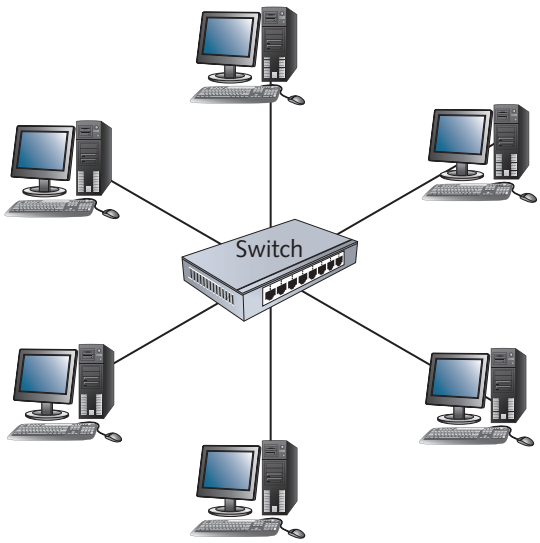

Figure 3-2 A physical star topology network

Some advantages of a physical star topology are the following:

- Much faster technologies are used than in a bus topology.
- Centralized monitoring and management of network traffic are possible.
- Network upgrades are easier.

A physical star is the topology of choice for these reasons and more. With a central device, communication options are available that simply aren't possible with a physical

bus. For example, the central device can be a 1000 Mbps switch, which increases a physical bus's top speed by 100 times and works in full-duplex mode, further increasing overall bandwidth.

As a budding network administrator, being able to monitor and manage your network with a central device is a big advantage over what was possible with a physical bus topology. Today's switches can include software that collects statistics about your network traffic patterns and even alerts you when excessive errors or unusually high traffic rates are occurring on your network. You don't get these features in a $19.99 switch, but enterprise-level devices can be equipped with several network management tools.

As long as your current cabling and installed NICs support it, your network can be upgraded quickly and easily from a ponderous 10 Mbps hub-based LAN to a blazing fast 1000 Mbps switched network simply by replacing the central device. In addition, if your NICs must also be upgraded, you can upgrade in steps because most devices support multiple speeds. So, if you want to upgrade from 100 Mbps to 1000 Mbps, you can replace the central device with a switch that supports both speeds, and then upgrade NICs as time and money allow. The switch transmits and receives on each port at the speed supported by the NIC connected to that port.

What happens if the number of workstations you need to connect exceeds the number of ports on the central device? In this case, you can connect switches together, as you learned in Chapter 2. When several switches must be connected, usually one device is used as the central connecting point, forming an extended star.

Extended Star

The **extended star topology**, shown in Figure 3-3, is the most widely used in networks containing more than just a few computers. As the name implies, this topology is a star of stars. A central device, usually a switch, sits in the middle. Instead of attached

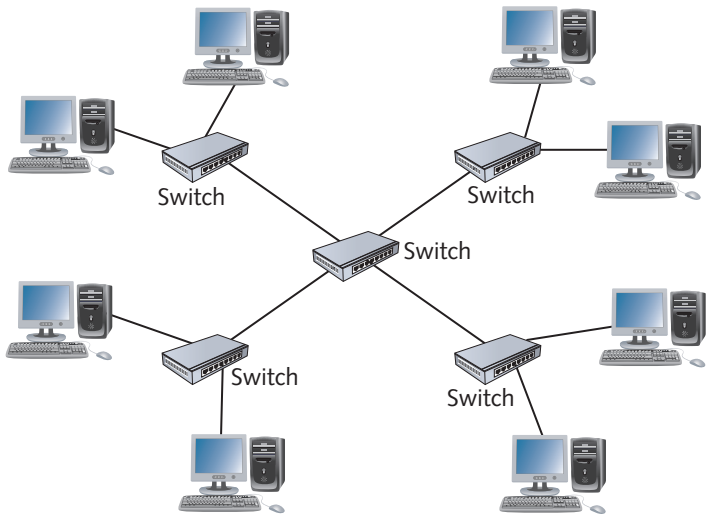

Figure 3-3 An extended star topology network

computers forming the star's arms, other switches are connected to the central switch's ports. Computers and peripherals are then attached to these switches, forming additional stars. The extended star is sometimes referred to as a "hierarchical star" because there are two or more layers of stars, all connecting back to the central star.

The extended star can be used to connect many computers, with the central device running at a very fast speed to shuttle data between the LAN's outer stars. This topology is most effective when the center of the star is running at a much faster speed than other devices; for example, the central device can run at 1000 Mbps while other devices run at 100 Mbps.

How Data Travels in a Physical Star

The details of how data travels from computer to computer in a physical star depend on the type of central device. Data transmission starts at a device at the end of one of the central device's arms. From there, it travels along the network medium's length until it arrives at the central device. As you know from learning how hubs and switches work, the transmission path differs, depending on the device. Other devices, such as multistation access units (MAUs) used in token ring networks, move data differently. The type of central device therefore determines the logical topology, as discussed later in "Logical Topologies."

Physical Star Disadvantages

With all the clear advantages of a physical star, you might wonder whether there are any disadvantages. None outweigh the advantages, but it's worth mentioning that the central device represents a single point of failure. In other words, if the switch fails or someone kicks the power cord out of the outlet, down goes the entire network. Thankfully, these devices tend to be reliable and are usually placed out of the way of everyday foot traffic. That being said, they do fail from time to time, and having a spare on hand is a good idea.

When a physical bus was still the norm and the physical star was just coming on the networking scene in the late 1980s, it was often argued that because each computer must be cabled directly to the central device, instead of a bus's daisy-chain arrangement, more cable was required to connect computers. This point is indeed true, and at the time, the amount of cabling needed was a factor in designing a network with a bus or star arrangement. By the time the star network's advantages were fully realized in the mid-1990s, however, the cabling cost difference had diminished substantially, and the advantages clearly outweighed the minor cost disadvantage.

Physical Ring Topology

A **physical ring topology** is like a bus, in that devices are daisy-chained one to another, but instead of terminating each end, the cabling is brought around from the last device back to the first device to form a ring. This topology had little to no following in LANs as a way to connect computers. It was used, however, to connect LANs to each other with a technology called Fiber Distributed Data Interface (FDDI).

FDDI was most often used as a reliable and fast **network backbone**, which is cabling used to communicate between LANs or between switches. In Figure 3-4, the devices used to connect buildings form a ring, but computers on each LAN are connected with a physical star topology.

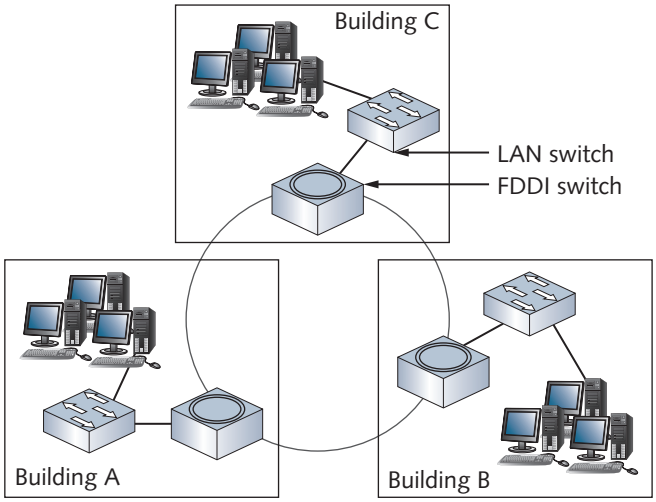

Figure 3-4 A physical ring topology is typically used to connect LANs

The physical ring also had reliability issues because data had to be forwarded from one station to the next. Unlike a bus, in which data travels in all directions and is terminated at both ends, a ring doesn't have any beginning or end. So, each station must reproduce data and pass it along to the next station until it reaches the destination or the originator of the data. In other words, data always travels in one direction. If any station in the ring fails, data can no longer be passed along, and the ring is broken.

Technologies such as FDDI overcome some problems with a physical ring network by creating a dual ring, in which data can travel in both directions so that a single device failure doesn't break the entire ring. However, this technology is costly, and physical rings have mostly been supplanted by extended star Ethernet installations.

Point-to-Point Topology

As its name implies, a **point-to-point topology** is a direct link between two devices. It's most often used in WANs, in which a device on a business's network has a dedicated link to a telecommunication provider, such as the local phone company. The connection then hooks into the phone company's network to provide Internet access or a WAN or MAN link to a branch office. The advantage of this topology is that data travels on a dedicated link, and its bandwidth isn't shared with other networks.

The disadvantage is that it tends to be quite expensive, particularly when used as a WAN link to a distant branch office.

Point-to-point topologies are also used with wireless networks in what is called a **wireless bridge**. This setup can be used to connect two buildings without using a wired network (see Figure 3-5) or to extend an existing wireless network.

Figure 3-5 A point-to-point wireless topology

A rudimentary LAN can also be set up with a point-to-point topology by connecting a cable between the NICs on two computers. Of course, this method allows only two computers on the network, but it can be used effectively for transferring files from one computer to another in the absence of a switch.

As you can see, point-to-point topologies are used for specialized purposes. They aren't commonly used in LANs; they're used more often in WANs and large internetworks.

Point-to-Multipoint Topology

A **point-to-multipoint (PMP) topology** is an arrangement in which a central device communicates with two or more other devices, and all communication goes through the central device. It's often used in WANs where a main office has connections to several branch offices via a router. Instead of the router having a separate connection to each branch office, a single connection is made from the router to a switching device, which then directs traffic to the correct branch office. In drawings of PMP networks, the switching device is often shown as a cloud, as in Figure 3-6. A PMP topology is also used in wireless network arrangements consisting of a single base station that communicates with multiple subscriber stations. Each subscriber station can communicate with the others, but all communication goes through the base station.

Mesh Topology

A **mesh topology** connects each device to every other device in a network. You can look at a mesh topology as multiple point-to-point connections for the purposes of redundancy and fault tolerance. Figure 3-7 shows a full mesh topology between four locations, with the switch in each location providing connectivity to multiple computers. Each switch is connected to every other switch, which is called a "full mesh." If each switch were connected to only two other switches, it would be called

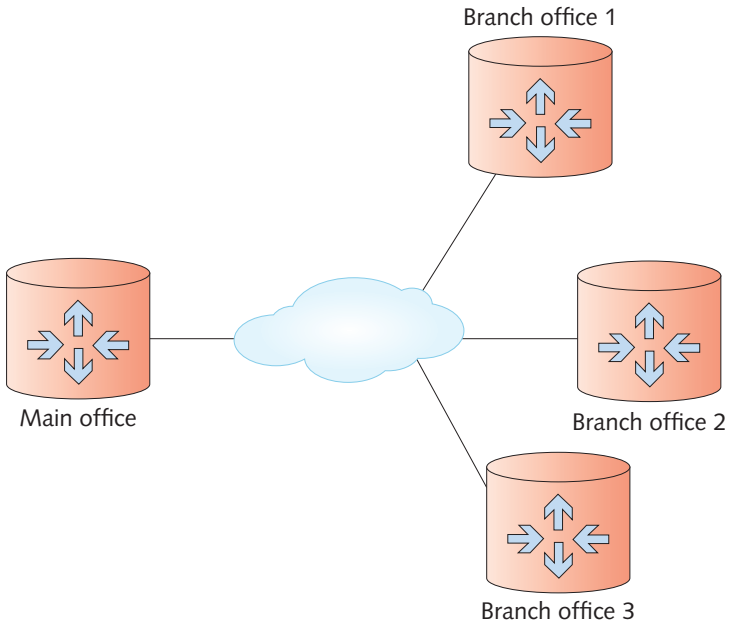

Figure 3-6 A point-to-multipoint topology

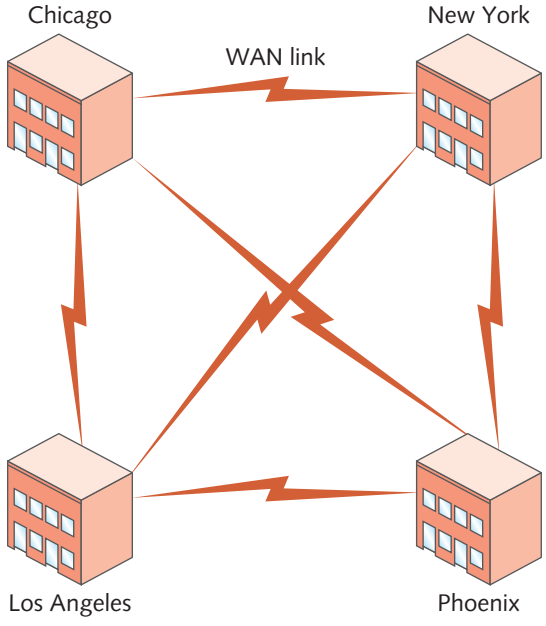

Figure 3-7 Switches in each building are connected in a full mesh topology

a "partial mesh." In either case, the purpose of creating a mesh topology is to ensure that if one or more connections fail, there's another path for reaching all devices on the network. For example, in the figure, two connections could fail, but all devices could still communicate with one another. This topology is used most commonly in large internetworks and WANs, where routers or switches in multiple buildings or towns are connected in a partial or full mesh. Parts of the Internet are also designed with a partial mesh topology, in which major ISPs are connected so that even if one ISP's network fails, data can bypass this part of the Internet to get to its destination.

Mesh topologies, although reliable, are also expensive because of the additional cabling and ports required. In most cases, the ports used to connect devices are the highest speed available, such as 1 Gbps or 10 Gbps, and they often use expensive fiber-optic cabling for connecting buildings.

Logical Topologies

Certification

98-366 Understanding network infrastructures:

Understand network topologies and access methods

As mentioned, a network's logical topology describes how data travels from computer to computer. In some cases, as with a physical bus and physical ring, the logical topology mimics the physical arrangement of cables. In other cases, as with a physical star, the electronics in the central device determine the logical topology. A network's logical topology reflects the underlying network technology (covered later in "Network Technologies") used to transfer frames from one device to another. Table 3-2 summarizes the main logical topologies, the technologies using them, and the physical topologies for implementing them.

Table 3-2 Logical topologies, associated network technologies, and physical topologies

Logical topology	Network technology	Physical topology	Description
Bus	Ethernet	Bus or star	A logical bus topology can be implemented as a physical bus (although this topology is now obsolete). When a logical bus is implemented as a physical star using wired Ethernet, the center of the star is an Ethernet hub. Whatever the physical topology is, data transmitted from a computer is received by all other computers.

(*continues*)

Table 3-2 Logical topologies, associated network technologies, and physical topologies (*continued*)

Logical topology	Network technology	Physical topology	Description
	Wireless LANs	Star	Wireless LANs use a physical star topology because they connect through a central access point. However, only one device can transmit at a time and all devices hear the transmission, so a wireless LAN can be considered a logical bus topology.
Ring	Token ring	Star	Token ring networks use a central device called a multistation access unit (MAU or MSAU). Its electronics form a logical ring, so data is passed from computer to computer in order, until it reaches the destination device.
	FDDI	Ring	FDDI devices are connected in a physical ring, and data passes from device to device until it reaches the destination.
Switched	Ethernet	Star	A switched logical topology using a physical star topology running Ethernet is by far the most common topology/technology combination now and likely will be well into the future. A switched topology creates dynamic connections or circuits between two devices whenever data is sent. This topology is sometimes considered a switched point-to-point topology because a circuit is established between two points as needed to transfer data (like turning on a switch), and then the circuit is broken when it's no longer needed (like turning off a switch).

You have seen what a logical bus looks like when implemented as a physical bus. All computers are daisy-chained to one another, and network signals travel along the cable's length in all directions, much like water flowing through interconnected pipes. When a logical bus is implemented as a physical star, the same process occurs, but the pathways are hidden inside the central hub. Figure 3-8 shows what a logical bus might look like when implemented with a hub.

Note

A logical bus is sometimes called a "shared media topology" because all stations must share the bandwidth the media provides.

A logical ring using a physical star implements the ring inside the central device's electronics, which is called an MAU in the token ring technology. Data is passed from one node or computer to another until it reaches the destination device

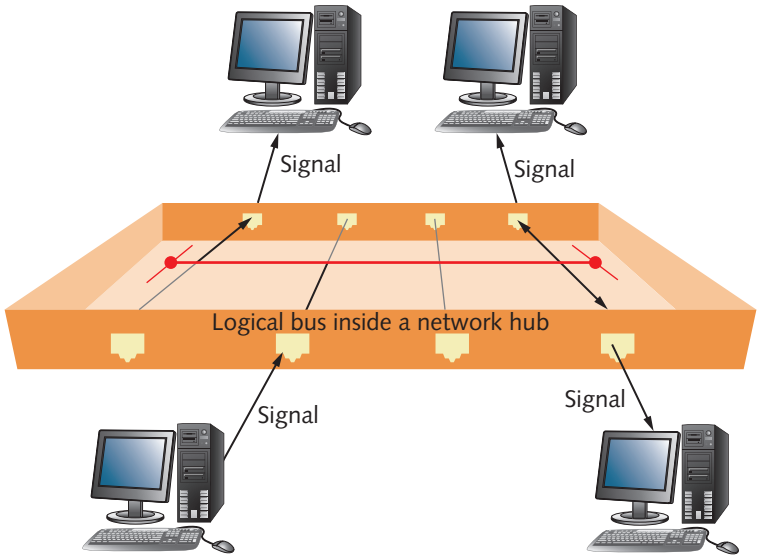

Figure 3-8 A logical bus implemented as a physical star

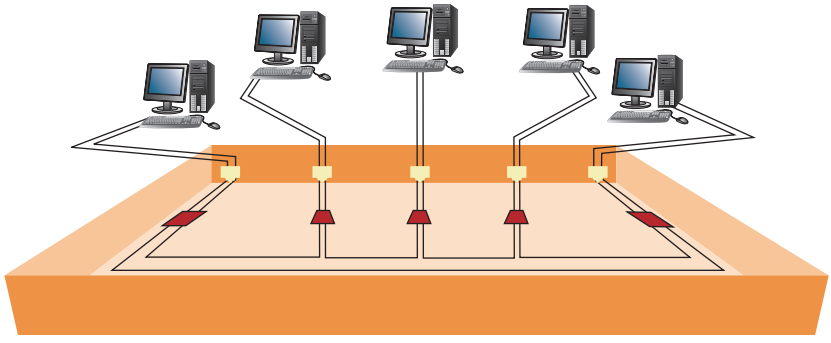

Figure 3-9 A logical ring implemented as a physical star

(see Figure 3-9). When a port has no device connected to it, it's simply bypassed, and data is sent out the next connected port.

A switched topology works something like what's shown in Figure 3-10. Although there's always an electrical connection between the computer and switch, when no data is being transferred, there's no logical connection or circuit between devices. However, when the switch receives a frame, a logical circuit is made between the source and destination devices until the frame is transferred.

To better understand how these logical topologies work, it helps to know the network technology that drives each topology (discussed later in "Network Technologies").

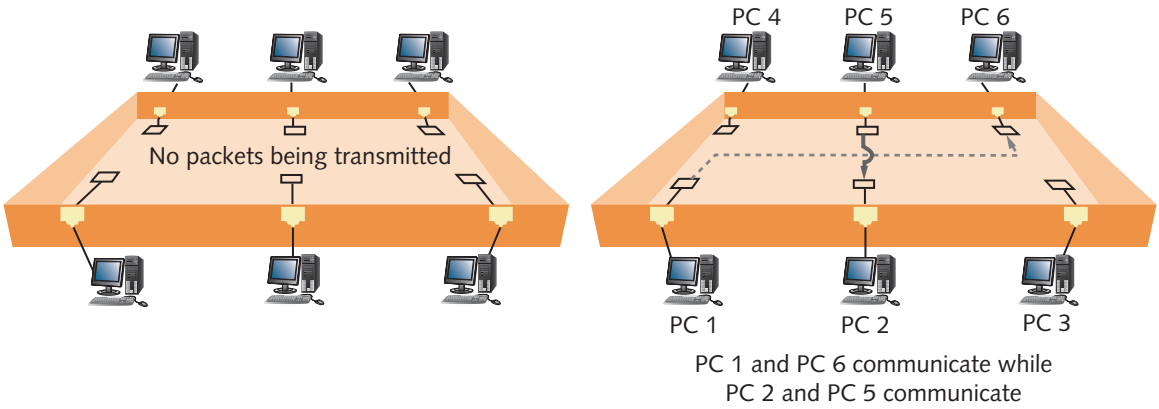

Figure 3-10 The logical functioning of a switch

Hands-On Project 3-1: Building a Physical Star Topology Network

Note

For a similar lab using Packet Tracer, see Packet Tracer Lab 3-1 at the end of the chapter.

Time Required: 20 minutes
Objective: Build a physical star topology network.
Required Tools and Equipment: Three lab computers named Computer1, Computer2, and Computer3; a hub; and three patch cables
Description: In this project, you build a small physical star topology. After each station is connected to the hub, you ping another station to verify connectivity. Next, you use Wireshark to capture ping packets so that you can determine the network's logical topology.

1. Power on the hub.
2. Connect each workstation to the hub with the supplied cables.
3. Inspect the hub and the workstation NIC to verify that you have a good connection with the hub. Write down how you determined whether the connection with the hub is good:
   _____
4. On each workstation, open a command prompt window, and then type **`ipconfig`** and press **Enter** to determine your IP address. Write down the IP address of each computer:
   - IP address of Computer1: _____
   - IP address of Computer2: _____
   - IP address of Computer3: _____

5. Ping each computer to verify that you can communicate with it. If the pings aren't successful, check that the IP addresses you wrote down are correct and the connection with the hub is good, and then try again.
6. Starting with this step, make sure you coordinate the rest of the project with students at the other computers. Start Wireshark, and start a capture session by clicking the interface name listed in the Interface List section.
7. At the command prompt, ping the next computer. For example, if you're at Computer1, ping Computer2; if you're at Computer2, ping Computer3; and if you're at Computer3, ping Computer1. Based on which packets Wireshark captured, what's your logical topology?

   _____

8. Exit Wireshark, close all open windows, and leave the computers running if you're continuing to the next project.

Network Technologies

Certification

98-366	Understanding network hardware:
	Understand media types
	Understanding network infrastructures:
	Understand wireless networking
	Understand network topologies and access methods

A network technology, as the phrase is used here, can best be described as the method a network interface uses to access the medium and send data frames, and the structure of these frames. Other terms include network interface layer technologies, network architectures, and Data Link layer technologies. Your network uses Ethernet, 802.11 wireless (Wi-Fi), or some combination of these and other technologies to move data from device to device in your network. Most LANs are now based on a combination of Ethernet and 802.11 wireless. WANs use technologies designed to carry data over longer distances, such as frame relay, SONET, and Asynchronous Transfer Mode (ATM).

The network technology sometimes, but not always, defines frame format and which media types can be used to transfer frames. For example, different Ethernet speeds specify a minimum grade of copper or fiber-optic cabling that must be used as well as the connectors attached to the ends of cables. FDDI requires fiber-optic cabling, but other technologies, such as frame relay, can run on a variety of media types.

This book focuses on LAN technologies, with particular emphasis on Ethernet and 802.11 wireless because they are the most commonly used. Some WAN technologies are described briefly in this chapter and in more detail in Chapter 12.

Network Technologies and Media

Because some of the network technologies discussed in this chapter specify the types of media they require to operate, the following sections summarize the most common media types. You can find more details on network media in Chapter 4.

Unshielded Twisted Pair

Unshielded twisted pair (UTP) is the most common media type in LANs. It consists of four pairs of copper wire, with each pair tightly twisted together and contained in a plastic sheath or jacket (see Figure 3-11).

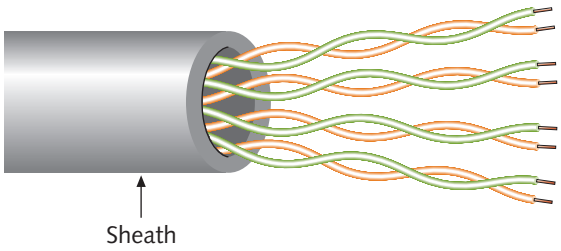

Figure 3-11 UTP cabling

UTP comes in numbered categories, and is up to Category 8 as of this writing. The higher the category number is, the higher the cable's bandwidth potential. Category 5 Enhanced (Cat 5E) and Category 6 (Cat 6) are the most common in wired LANs, allowing speeds up to 10 Gbps. UTP cabling is used in physical star networks; the maximum cable length from NIC to switch is 100 meters (328 feet) in LAN applications. UTP cabling is susceptible to electrical interference, which can cause data corruption, so it shouldn't be used in electrically noisy environments.

Fiber-optic Cabling

Fiber-optic cabling uses extremely thin strands of glass to carry pulses of light long distances and at high data rates. It's typically used in large internetworks to connect switches and routers and sometimes to connect high-speed servers to the network. Because of its capability to carry data over long distances (several hundred to several thousand meters), it's also used in WAN applications frequently. Fiber-optic cabling isn't susceptible to electrical interference, so, unlike UTP, it can be used in electrically noisy environments. In most cases, two strands of fiber are needed to make a network connection: one for transmitting and one for receiving.

Coaxial Cable

Best known for its use in cable TV, coaxial cable is obsolete as a LAN medium, but it is used as the network medium for Internet access via cable modem. Coaxial cable was the original medium used by Ethernet in physical bus topologies, but its limitation of 10 Mbps half-duplex communication made it obsolete for LAN applications after star topologies and 100 Mbps Ethernet became the dominant standard. Coaxial cable in LANs can be about 200 meters long.

Baseband and Broadband Signaling

Network technologies can use media to transmit signals in two main ways: baseband and broadband. The **baseband** transmission method sends digital signals in which each bit of data is represented by a pulse of electricity (on copper media) or light (on fiber-optic media). These signals are sent at a single fixed frequency, using the medium's entire bandwidth. In other words, when a frame is sent to the medium, it occupies the cable's entire bandwidth, and no other frames can be sent along with it—much like having cable TV that carries only a single channel. LAN technologies, such as Ethernet and token ring, use baseband transmission. If cable TV used baseband signaling, you would need one cable for each channel!

Thankfully, cable TV and cable modem Internet access use broadband transmission. Instead of digital pulses, **broadband** systems use analog techniques to encode binary 1s and 0s across a continuous range of values. Broadband signals move across the medium in the form of continuous electromagnetic or optical waves rather than discrete pulses. On broadband systems, signals flow at a particular frequency, and each frequency represents a channel of data. That's why broadband systems, such as cable TV and Internet, can carry dozens or hundreds of TV channels plus Internet access on a single cable wire: Each channel operates at a different frequency. In addition, incoming and outgoing Internet data use separate channels operating at different frequencies from TV channels.

Ethernet Networks

Ethernet, the most popular LAN technology, has many advantages, including ease of installation, scalability, media support, and low cost. It supports a broad range of transmission speeds, from 10 Mbps to 10 Gbps. As discussed, it can operate in a bus or star physical topology and a bus or switched logical topology. It has been in use since the mid-1970s but didn't mature as a technology until the early to mid-1980s. Ethernet being around for more than 40 years is a testament to the original designers, whose forethought enabled Ethernet to scale from a 3 Mbps technology in its early years to a 100 Gbps technology today.

Although there are many variations of Ethernet, all forms are similar in their basic operation and frame formatting. What differs in the variations are the cabling, speed of transmission, and method by which bits are encoded on the medium. Because the frame formatting is the same, however, Ethernet variations are compatible with one

another. That's why you often see NICs and Ethernet switches described as 10/100 or 10/100/1000 devices. These devices can support multiple Ethernet speeds because the underlying technology remains the same, regardless of speed.

Ethernet Addressing

Every Ethernet station must have a physical or MAC address. As you learned in Chapter 2, a MAC address is an integral part of network interface electronics and consists of 48 bits expressed as 12 hexadecimal digits. When a frame is sent to the network medium, it must contain both source and destination MAC addresses. When a network interface detects a frame on the media, the NIC reads the frame's destination address and compares it with the NIC's own MAC address. If they match or if the destination address is the broadcast MAC address (all binary 1s or FF:FF:FF:FF:FF:FF in hexadecimal), the NIC reads the frame and sends it to the network protocol for further processing.

Ethernet Frames

A frame is the unit of network information that NICs and switches work with. It's the NIC's responsibility to transmit and receive frames and a switch's responsibility to forward frames out the correct switch port to get the frame to its destination.

Ethernet networks can accommodate frames between 64 bytes and 1518 bytes. Shorter or longer frames are usually considered errors. Each frame is composed of the following (see Figure 3-12):

- A 14-byte frame header composed of these three fields:
  - A 6-byte Destination MAC Address field
  - A 6-byte Source MAC Address field
  - A 2-byte Type field
- A Data field from 46 to 1500 bytes
- A frame trailer (frame check sequence [FCS]) of 4 bytes

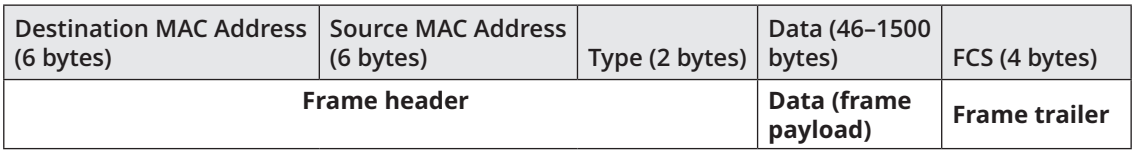

Figure 3-12 Ethernet frame format

You've already learned the purpose and format of destination and source MAC addresses. The Type field in the frame header indicates the network protocol in the data portion. For example, this field might indicate that the Data field contains an IP, IPv6, or ARP packet, to name just a few possibilities. The data portion, often referred to as the "frame payload," contains network protocol header information as well as the actual data an application is transferring. The FCS in the frame trailer is an error-checking code (discussed later in "Ethernet Error Handling").

Note

There are exceptions to the 1518-byte maximum frame size. For example, a function of some switches requires an additional 4-byte field in the Ethernet frame, bringing the maximum size to 1522 bytes. In addition, Jumbo frames of up to 9000 bytes are supported by some NICs and switches but aren't officially supported in the current Ethernet standards. To use Jumbo frames, the feature must be enabled on every device on the LAN and be implemented the same way by these devices. Some storage area network (SAN) devices also use Jumbo frames.

Ethernet Media Access

Before a NIC can transmit data to the network medium, it must adhere to some rules governing how and when the medium can be accessed for transmission. The rules ensure that data is transmitted and received in an orderly fashion and all stations have an opportunity to communicate. The set of rules for each networking technology is referred to as its **media access method** (or "media access control").

Note

The acronym for "media access control" is MAC, which is where the term "MAC address" comes from.

The media access method that Ethernet uses in half-duplex mode is **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**. To understand this method better, break the term down into parts. "Carrier sense" means to listen. The rules for half-duplex Ethernet state that a device can send or receive data but can't do both simultaneously. So, before a device can send, it must listen to determine whether the medium is already busy, much like a group of people having a conversation. Each person listens for a pause in the conversation before speaking up. "Multiple access" simply means that multiple computers can be listening and waiting to transmit at the same time, which brings you to "collision detection." A **collision** occurs if two or more devices on the same medium transmit simultaneously. For example, if two people are waiting to chime in on a group conversation, they both hear a lull in the conversation at the same time and might speak up simultaneously, causing a "collision" in the conversation. Ethernet's collision detection method is much like a person's; Ethernet detects, or "hears," the other station transmit, so it knows a collision has occurred. The NIC then waits for a random period before attempting to transmit again. Ethernet repeats the "listen before transmitting" process until it transmits the frame without a collision.

As you determined in Hands-On Project 2-3 when you attempted to create enough traffic to generate a collision, the CSMA/CD access method is efficient. It takes quite a bit of traffic to generate collisions, especially on a 100 Mbps or 1 Gbps network. However, the more devices a logical bus topology has and the more data they transmit, the greater the chance of a collision. So, although CSMA/CD works well, today's multimedia-heavy networks have outgrown it, and Ethernet has adapted to this development.

Note

CSMA/CD is considered a contention-based access method, which means computers are allowed to send whenever they have data ready to send. CSMA/CD modifies this rule somewhat by stipulating that the computer must listen first to ensure that no other station is in the process of transmitting.

Collisions and Collision Domains

Remember that collisions can occur only in an Ethernet shared-media environment, which means a logical bus topology is in use. In this environment, all devices interconnected by one or more hubs hear all signals generated by all other devices. The signals are propagated from hub to hub until there are no more devices or until a device is encountered that doesn't use a logical bus topology, such as a switch or a router. The extent to which signals in an Ethernet bus topology network are propagated is called a **collision domain**. Figure 3-13 shows a network diagram with two collision domains enclosed in circles. All devices in a collision domain are subject to the possibility that whenever a device sends a frame, a collision might occur with another device sending a frame at the same time. This fact has serious implications for the number of computers that can reasonably be installed in a single collision domain. The more computers there are, the more likely it is that collisions occur. The more collisions there are, the slower the network performance is.

Notice in this figure that all computers connected to Hubs 1 to 3 are in the same collision domain, and computers connected to Hubs 4 to 6 are in a different collision domain. This is because a switch port delimits the collision domain, which means collisions occurring in one collision domain don't propagate through the switch.

Although collisions in an Ethernet network are usually associated with hubs, technically it's possible for a collision to occur with a computer connected to a switch, but it can happen only if the NIC connected to the switch port is operating in half-duplex mode. In addition, the collision domain is limited to only the devices connected to a single switch port. The same is true of routers. However, given that an Ethernet frame of maximum size is transmitted on a 10 Mbps switch in just over a millisecond and on a 100 Mbps switch in just over a microsecond, the likelihood of a collision with a switch is low.

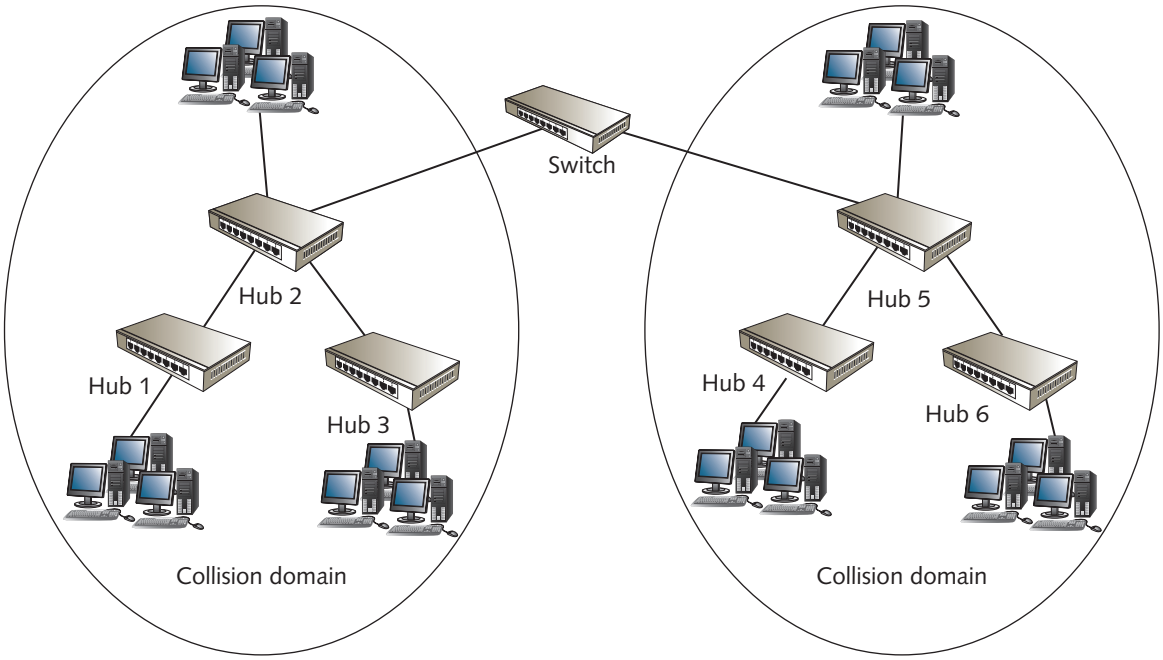

Figure 3-13 A network diagram showing two collision domains delimited by a switch

Ethernet Error Handling

One reason for Ethernet's low cost and scalability is its simplicity. It's considered a best-effort delivery system, meaning that when a frame is sent, there's no acknowledgment or verification that the frame arrived at its intended destination. Ethernet relies on network protocols, such as TCP/IP, to ensure reliable delivery of data. It's similar to the package delivery guy at a company. His job is to take what he's given to its intended destination; it's the package receiver's job to verify its contents and let the sender know it was received.

Ethernet can also detect whether a frame has been damaged in transit. The error-checking code in an Ethernet frame's trailer is called a **Cyclic Redundancy Check (CRC)**, and is the result of a mathematical algorithm computed on the frame data. The CRC is calculated and placed in the frame trailer before the frame is transmitted. When the frame is received, the calculation is repeated. If the results of this calculation don't match the CRC in the frame, it indicates that the data was altered in some way, possibly from electrical interference. If a frame is detected as damaged, Ethernet simply discards the frame but doesn't inform the sending station that an error occurred (because it's a best-effort delivery system). Again, it's the network protocol's job to ensure that all expected data was actually received. The network protocol or, in some cases, the application sending the data is responsible for resending damaged or missing data, not Ethernet.

Note

A collision is the exception to Ethernet's lack of action when an error occurs. When frames are involved in a collision, Ethernet resends them automatically because all stations detect that a collision has occurred.

Half-Duplex versus Full-Duplex Communication

As discussed in Chapter 2, half-duplex communication means a station can transmit and receive data but not at the same time, much like a two-way radio. When Ethernet is implemented as a logical bus topology (using hubs), NICs can operate only in half-duplex mode and must use the CSMA/CD access method. However, a network switch allows half-duplex or full-duplex communication. If a NIC is operating in half-duplex mode while connected to a switch, it must use CSMA/CD. Thus, the only time a collision can occur in this circumstance is if the switch happens to transmit a frame to the NIC at the same time the NIC is attempting to transmit.

Full-duplex mode, by definition, means a NIC can transmit and receive simultaneously. Therefore, when an Ethernet NIC is operating in full-duplex mode connected to a switch, CSMA/CD isn't used because a collision can't occur in full-duplex mode. Because full-duplex mode eliminates the delays caused by CSMA/CD and allows double the network bandwidth, Ethernet LANs operate in this mode using switches.

Ethernet Standards

Ethernet can operate at different speeds over different types of media, and each variation is associated with an IEEE standard. The following sections discuss many of these standards, some of which are obsolete or had limited use.

Standards Terminology

Ethernet standards are generally expressed in one of two ways. One way is using the IEEE document number defining the standard. For example, IEEE 802.3 is the parent document specification for 10 Mbps Ethernet using thick coaxial cable, which was ratified in 1983. All other variations and speeds of Ethernet are subdocuments of the original 802.3 specification.

The second way of expressing an Ethernet standard is to use the XBaseY terminology. Most IEEE 802.3 documents describe the transmission speed, type of transmission, and length or type of cabling and are designated with terms such as 100BaseT. In 100BaseT, for example, the "100" designates the speed of transmission (100 Mbps), the "Base" indicates a baseband signaling method, and the "T" specifies twisted-pair cabling. All the BaseT Ethernet standards use a physical star topology. The following sections discuss the major standards and their designations.

10BaseT Ethernet

10BaseT Ethernet, defined by IEEE 802.3i, has been the mainstay of Ethernet networks since the early 1990s. It runs over Category 3 or higher UTP cabling and uses two of the four wire pairs. Because of its slower transmission speed, 10BaseT networks using a logical bus topology (with hubs) are more susceptible to collisions than faster 100BaseT networks. In addition, the amount of data sent and received by a typical user makes 10BaseT seem slow in typical media-heavy environments compared with the more common 100BaseT and 1000BaseT standards.

If you work for an organization that's still using hubs, you need to know that there are limits to how many hubs you can string together to connect all computers. The rule for expanding a 10BaseT network with hubs is that no more than four hubs can be placed between two communicating workstations. This rule ensures that all stations on the network can detect a collision. Because of the limited time for signals to propagate through a network, if more than four hubs exist between end stations, a collision on one end of the network might not be detected by stations on the other side of the network in time for them to react properly. If switches rather than hubs are used, there's no such limitation because a collision on a switch can take place only between the switch and a single workstation.

A business network still using 10BaseT should upgrade to 100 or 1000BaseT to take full advantage of current technology. A home or small-office network used mainly for sharing Internet access and transferring documents can still use 10BaseT effectively if its Internet connection is considerably slower than 10 Mbps. However, 10BaseT is essentially an obsolete technology, and networks using it should upgrade as soon as circumstances permit.

100BaseTX Ethernet

100BaseTX (often called simply "100BaseT"), defined by IEEE 802.3u, is still the most common Ethernet variety. It runs over Category 5e or higher UTP cable and uses two of the four wire pairs: one to transmit data and the other to receive data. There are other varieties of 100BaseT Ethernet (discussed later in this section), but 100BaseTX is the standard that's usually in mind when discussing 100 Mbps Ethernet. It's also sometimes called "Fast Ethernet."

100BaseFX Ethernet

In environments that aren't conducive to using copper wiring to carry network data (such as electrically noisy settings) or where the cable run length exceeds the reach of twisted-pair wiring, the only real choice in a wired network is fiber optics. In these settings, **100BaseFX** (with the F indicating "fiber optic"), which uses two strands of fiber-optic cable, is often the best choice of network technology. Fiber-optic cable installation is still far more expensive than twisted-pair cable, but its advantages of being impervious to electrical noise and supporting longer cable segment lengths are worth the cost if the network requires these properties. 100BaseFX is rarely used as a complete replacement for 100BaseTX; instead, it's typically used as backbone cabling

between hubs or switches and to connect wiring closets between floors or buildings. It's also used to connect client or server computers to the network when immunity to noise and eavesdropping is required.

1000BaseT Ethernet

1000BaseT Ethernet, released as the IEEE 802.3ab standard, supports 1000 Mbps Ethernet (usually called "Gigabit Ethernet") over Category 5e or higher UTP cable. The 1 Gbps data rate results from sending and receiving data simultaneously (in full-duplex mode) at 250 Mbps in both directions over each of the four wire pairs in Category 5e cable. In other words, each wire pair can send and receive data at the same time at 250 Mbps, which results in a bandwidth of 1000 Mbps (or 1 Gbps) in each direction in full-duplex mode. To support full-duplex transmission over a single pair of wires, 1000BaseT uses hybrid and canceller technology, which combines multiple signals and cancels interference. So, if the link operates in half-duplex mode, the channel speed is 1000 Mbps (250 Mbps times four wire pairs). When operating in full-duplex mode, 1000BaseT actually delivers 2 Gbps total bandwidth. In most cases, it runs in full-duplex mode connected to switches.

Unlike 10BaseT and 100BaseT Ethernet, 1000BaseT Ethernet doesn't dedicate a wire pair to transmitting or receiving. Each wire pair is capable of transmitting and receiving data simultaneously, thereby making the 1000 Mbps data rate possible in both half-duplex and full-duplex modes.

2.5GBaseT and 5GBaseT

In September 2016, the IEEE ratified the 802.3bz specification that defines 2.5 and 5 Gigabit Ethernet running over Cat 5e/6 cabling. This specification was largely in response to increasing Wi-Fi speeds, with 802.11ac Wave 2 access points coming to market that support speeds beyond 1 Gbps. Faster wired Ethernet speeds are needed as uplink ports from these new 802.11ac access points to prevent the wired connection from being the bottleneck on wireless LANs. Because the new **2.5/5 GBaseT** Ethernet standard works over Cat5e and Cat6 cabling, there is no need for a change in the wiring infrastructure, as most cabling plants use Cat5e or Cat6. Also, as noted below, the next iteration of Ethernet (10GBaseT) requires Cat 6A cabling, which is only installed in a small percentage of organizations.

10GBaseT Ethernet

The 2006 IEEE 802.3an standard defines 10 Gigabit Ethernet as running over four pairs of Category 6A or Category 7 UTP cabling. Unlike the other BaseT Ethernet standards, **10GBaseT** operates only in full-duplex mode, so there is no such thing as a 10 Gbps hub—only switches. 10GBaseT NICs are expensive compared with NICs supporting 1 Gbps and less, but prices continue to drop. As of this writing, you can purchase a 10GBaseT NIC for under $100; several years ago, the price was more than $1000. Although this cost might still be a lot for a desktop computer, you might need to equip network servers with 10 Gigabit Ethernet NICs so that they can keep up with desktop systems that commonly operate at 1 Gbps.

Additional Ethernet Standards

Although the standards discussed previously constitute the majority of Ethernet LANs, quite a few other standards exist; some are common, and others are uncommon or obsolete. The following sections briefly describe these other standards and their use in current networks.

100BaseT4

As the name implies, 100BaseT4 Ethernet uses all four pairs of wires bundled in a UTP cable. The one advantage that 100BaseT4 has over 100BaseTX is the capability to run over Category 3 cable. When 100 Mbps speeds became available, many companies wanted to take advantage of the higher bandwidth. However, if the cable plant consisted of only Category 3 cable, there were just two choices: Replace the cabling with higher-grade Category 5 cabling so that 100BaseTX could be used, or use 100BaseT4 Ethernet. One of the biggest expenses of building a network is cable installation, so many organizations chose to get higher speeds with the existing cable plant by using 100BaseT4. Although these differences from 100BaseTX might seem like good ideas, 100BaseT4 never caught on and is essentially obsolete.

1000BaseLX

1000BaseLX uses fiber-optic media; the "L" stands for "long wavelength," the kind of laser used to send signals across the medium. These lasers operate at wavelengths between 1270 and 1355 nanometers and work with single-mode fiber (SMF) and multimode fiber (MMF). Long-wavelength lasers cost more than short-wavelength lasers but can transmit their signals over longer lengths of cable.

Although the 1000BaseLX standard specifies a maximum cable segment length of 5000 meters, some manufacturers have extended it by using specialized and proprietary optical transceivers. Cisco Systems, for example, offers 1000BaseLH ("LH" stands for "long haul"), which provides a maximum cable segment length of 10,000 meters over SMF cable. For extremely long-distance Gigabit Ethernet communication, 1000BaseZX, another Cisco product, is capable of distances up to 100,000 meters over SMF cable.

1000BaseSX

1000BaseSX uses fiber-optic media; the "S" stands for "short wavelength." These lasers operate at wavelengths between 770 and 860 nanometers and work only with MMF cable. Short-wavelength lasers can't cover as much distance as long-wavelength lasers, but they are less expensive (and use cheaper MMF cable).

1000BaseCX

1000BaseCX uses specially shielded, balanced, copper jumper cables; the "C" stands for "copper," the kind of electrical signaling used. Jumper cables are normally used for interconnections between devices or to link virtual LANs (VLANs) on a switch; these jumper cables might also be called "twinax" (short for "twin-axial") or "short-haul" copper cables. Segment lengths for 1000BaseCX cables top out at 25 meters, which means they're used mostly in wiring closets or equipment racks.

10 Gigabit Ethernet IEEE 802.3ae Standards

The 802.3ae standard, which governs several varieties of 10 Gigabit Ethernet before 10GBaseT, was adopted in June 2002. This Ethernet version is much like the others in frame formats and media access method. However, it does have some important technical differences. It is defined to run only on fiber-optic cabling, but the 10 Gigabit Ethernet standard specifies a maximum distance of 40 km, compared with just 5 km for 1000BaseLX Gigabit Ethernet. This distance has important implications for WANs and MANs because, although most WAN and MAN technologies can be measured in megabits, 10 Gigabit Ethernet provides bandwidth that can transform how WAN speeds are considered. Like 10GBaseT Ethernet, 802.3ae 10 Gigabit Ethernet technologies run in full-duplex mode only, so the CSMA/CD access method isn't necessary.

The primary use of 10 Gigabit Ethernet technologies is as the network backbone, interconnecting servers and network segments running 100 Mbps and 1000 Mbps Ethernet technologies. However, they also have their place in storage area networks (SANs) and, along with 10GBaseT, can be used as the interface for enterprise-level servers.

As this technology matured, a number of implementations were developed that are divided into two basic groups: 10GBaseR for LAN applications and 10GBaseW for WAN applications. The W group of standards uses SONET framing over OC-192 links. (SONET and OC standards are explained in Chapter 12.) Both groups have (S)hort range, (L)ong range, and (E)xtended range versions. The short-range versions use MMF fiber-optic cabling, and the long-range and extended-range versions run over SMF fiber-optic cabling. (These fiber-optic types are discussed in Chapter 4.) The following list summarizes the 802.3ae technologies:

- *10GBaseSR*—Runs over short lengths (between 26 and 82 meters) on MMF cabling. Applications are likely to include connections to high-speed servers, interconnecting switches, and SANs.
- *10GBaseLR*—Runs up to 10 km on SMF cabling and is used for campus backbones and MANs.
- *10GBaseER*—Runs up to 40 km on SMF cabling; used primarily for MANs.
- *10GBaseSW*—Uses MMF cabling for distances up to 300 meters; used for SONET campus network applications.
- *10GBaseLW*—Uses SMF cabling for distances up to 10 km; used for SONET WAN applications.
- *10GBaseEW*—Uses SMF cabling for distances up to 40 km; used for SONET WAN applications.

40 Gigabit and 100 Gigabit Ethernet

IEEE 802.3ba was ratified in 2010, and it paves the way for extremely fast communication channels. Pricing on 40 Gbps and 100 Gbps products is still prohibitive, and adoption of these standards has been slow. Fiber-optic cabling is the primary medium for supporting these speeds, although there are provisions to use special copper assemblies over short distances. Related standards that support 100 Gbps include 802.3bj and 802.3bm.

Tip

Although the 802.3ba task force has completed its work, you can read about how this standard came to be at *www.ieee802.org/3/ba/index.html*.

As you can see, Ethernet has come a long way since Xerox transmitted at 3 Mbps over coaxial cable, and the journey from 3 Mbps to 100 Gbps isn't over yet. Table 3-3 summarizes many features and properties of the Ethernet standards discussed in this section.

Table 3-3 Ethernet standards and properties

Ethernet standard	IEEE document #	Transmission speed	Cable type	Minimum cable grade	Maximum distance	Design notes
10BaseT	802.3i	10 Mbps	UTP	Cat 3	100 meters	Maximum four hubs between stations
100BaseT/TX	802.3u	100 Mbps	UTP	Cat 5	100 meters	Maximum two hubs between stations
100BaseFX	802.3u	100 Mbps	MMF or SMF	N/A	2 km over MMF, 10 km over SMF	
1000BaseT	802.3ab	1000 Mbps	UTP	Cat 5 (Cat 5e or 6 preferred)	100 meters	Maximum one hub between stations
2.5/5GBaseT	802.3bz	2.5 and 5 Gbps	UTP	Cat 5e/6	100 meters	Compatible with most existing cable plants
10GBaseT	802.3an	10 Gbps	UTP	Cat 6A	100 meters	Full-duplex only; no hubs
100BaseT4	802.3u	100 Mbps	UTP	Cat 3	100 meters	Obsolete; saw little use
1000BaseLX	802.3z	1000 Mbps	MMF or SMF	N/A	550 meters over MMF, 5 km over SMF	

(*continues*)

Table 3-3 Ethernet standards and properties (*continued*)

Ethernet standard	IEEE document #	Transmission speed	Cable type	Minimum cable grade	Maximum distance	Design notes
1000BaseSX	802.3z	1000 Mbps	MMF	N/A	550 meters	
1000BaseCX	802.3z	1000 Mbps	Twinax	N/A	25 meters	Succeeded by 1000BaseT
10GBaseSR 10GBaseLR 10GBaseER 10GBaseSW 10GBaseLW 10GBaseEW	802.3ae	10 Gbps	MMF or SMF	N/A	Varies from 82 meters up to 40 km	Choice of technology depends on application
40 Gigabit Ethernet and 100 Gigabit Ethernet	802.3ba	40 and 100 Gbps	MMF, SMF, and copper assembly	N/A	40 km over SMF, 7 meters over copper	Standard ratified June 2010

What's Next for Ethernet?

Estimations are that Ethernet speeds will continue to increase, with Terabit Ethernet (1000 Gbps) as part of the discussion. In March 2013, a study group began work on a 200 and 400 Gbps standard (802.3bs); the work was completed in 2017, although devices are not yet readily available that operate at these speeds. This kind of mind-boggling speed will allow networks to transfer data across a city faster than some CPUs can transfer data to memory. When Internet providers begin using this level of bandwidth to connect to the Internet backbone, and when homes and businesses can tap into it as well, extraordinary amounts of information will be at your fingertips. This speed has major implications for the entertainment industry and many other fields.

Hands-On Project 3-2: Determining and Changing Your Ethernet Standard

Time Required: 15 minutes

Objective: Determine your Ethernet standard and change your connection speed to use a different standard.

Required Tools and Equipment: You need two lab computers, a switch, and two patch cables. The switch and NICs must be capable of connecting at multiple speeds. For example, if you're using a 10/100 Mbps switch and your NICs are capable of 10/100 Mbps, change the connection speed to the slower rate. Work in pairs.

Description: In this project, you view your network connection properties to see at what speed your NIC is operating. Then you send a large ping message to a partner and note how long the reply takes. Next, you change the speed if your NIC driver allows it, and perform the same ping to see whether you can detect a time difference.

Note

This project works better with physical computers rather than virtual machines. Even if you change the connection speed on the virtual machine, it transmits bits at the host computer's connection speed.

1. Log on to your computer as **NetAdmin**.
2. Open a command prompt window, and then type `ipconfig` and press **Enter**. Exchange your IP address with your partner and write down your partner's IP address on the following line. Leave the command prompt window open for later.

   _____

3. Right-click **Start** and click **Network Connections**. Right-click **Ethernet0** and click **Status** (see Figure 3-14).

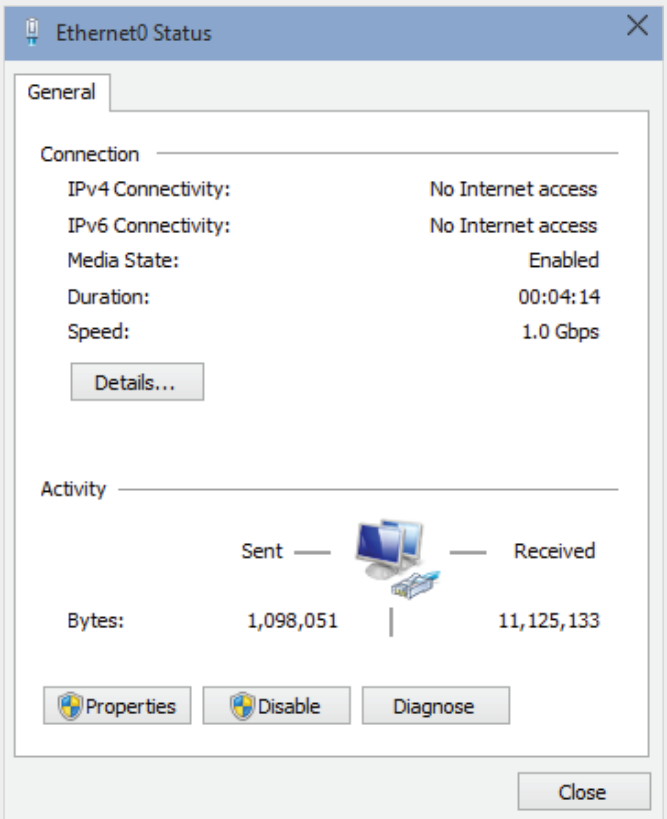

Figure 3-14 The Ethernet0 Status dialog box

4. In the Connection section, find the line labeled "Speed." Write down this information and, based on the speed listed, the Ethernet variety your computer is running:
   - Connection speed: _____
   - Ethernet variety (10BaseT, 100BaseT, etc.): _____
5. At the command prompt, ping your partner by typing **`ping -l 60000 IPaddress`** and pressing **Enter** (replacing *`IPaddress`* with the IP address of your partner's computer). The `-l 60000` option in the command specifies that the ping message should be 60000 bytes instead of the typical length of 32 bytes. Note the time values in the ping replies and write them down. For example, one of yours might be "time<1ms," meaning the reply took less than 1 millisecond. The times might not all be the same. Sometimes the first time is slower than the rest. Try pinging a few times to get an idea of the average time. Write the ping reply times on the following line:

   _____
6. Click the **Properties** button in the Ethernet0 Status dialog box. In the Ethernet0 Properties dialog box, click the **Configure** button under the Connect using text box.
7. Click the **Advanced** tab. In the Property list box, click **Speed & Duplex** (or a similar name). Figure 3-15 shows the connection options. Not all NICs have the same options, so you might see different options.
8. The default setting is usually Auto Negotiation. Click **10 Mbps Half Duplex** if this option is available, and then click **OK**. If you were able to set this option, what speed and variety of Ethernet is your computer running now?
   - Connection speed: _____
   - Ethernet variety: _____
9. After you and your partner have changed the connection speed to a lower value, repeat the `ping` command you used in Step 5. Write down the reply times on the following lines, and state whether they were different:

   _____

   _____
10. Figure 3-16 shows two sets of ping results. The first result was from two computers connected at 1 Gbps (1000 Mbps) in full-duplex mode. The average reply took 5 ms. The second result was with the same computers connected at 10 Mbps half-duplex, and the average reply took 103 ms. Change your connection speed and duplex mode back to Auto Negotiation, and then close all open windows. Leave your computer running for the next project.

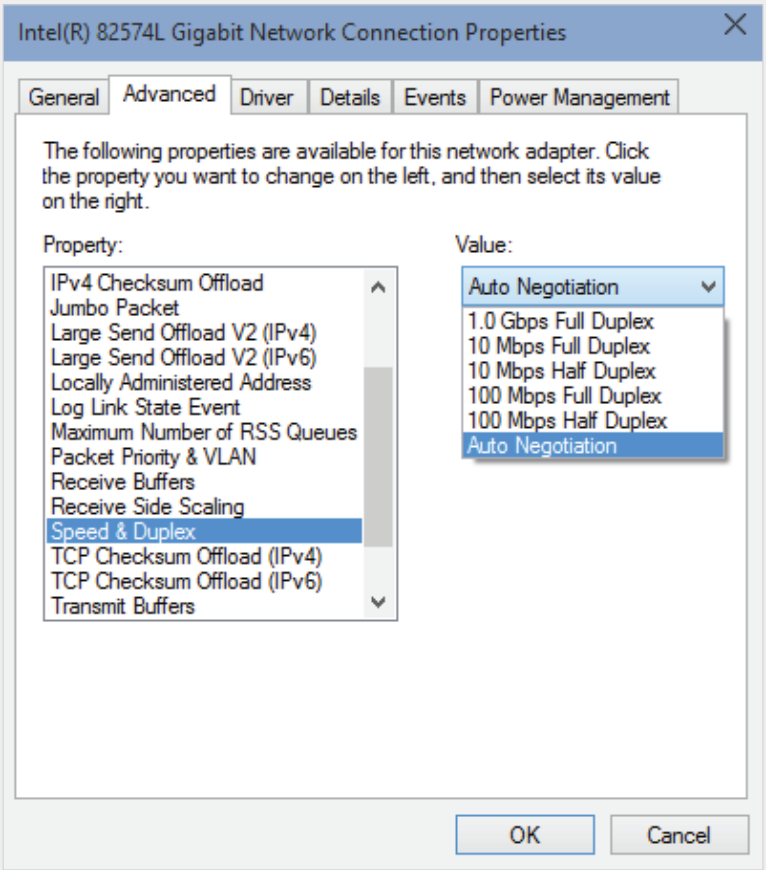

Figure 3-15 Settings for the Speed & Duplex property

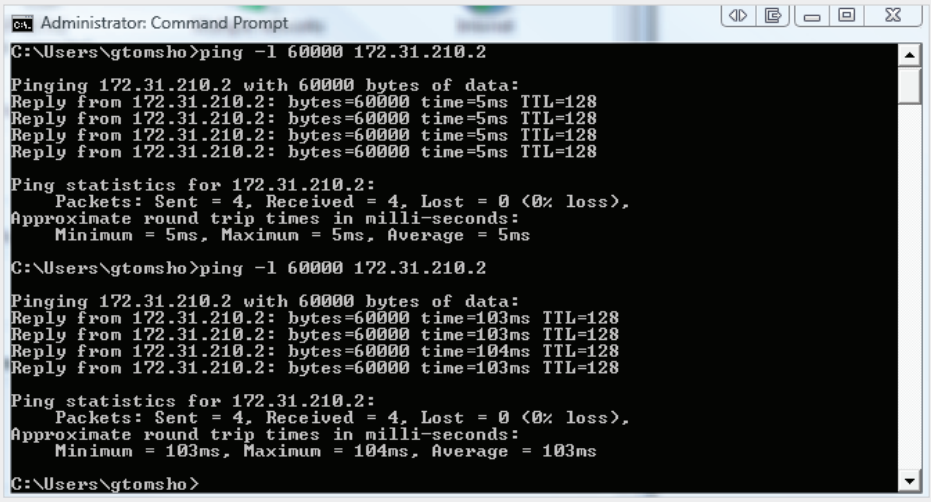

Figure 3-16 Ping results at different connection speeds

Hands-On Project 3-3: Viewing an Ethernet Frame

Time Required: 20 minutes
Objective: Capture packets and examine details of an Ethernet frame.
Required Tools and Equipment: Two lab computers, a switch, and two patch cables
Description: In this project, you capture some packets and then examine the frame and protocol headers.

1. If necessary, log on to your computer as **NetAdmin**.
2. Start Wireshark and click **Capture Options**. In the Capture Filter text box, type **icmp**, and then click **Start**.
3. Open a command prompt window, and then type **`ping IPaddress`** and press **Enter** (replacing *`IPaddress`* with the IP address of your partner's computer from Hands-On Project 3-2).
4. In Wireshark, click the **Stop the running live capture** toolbar icon to stop the capture.
5. Click a packet summary in the top pane with ICMP listed in the Protocol field. In the middle pane, click to expand the **Ethernet II** row (see Figure 3-17).

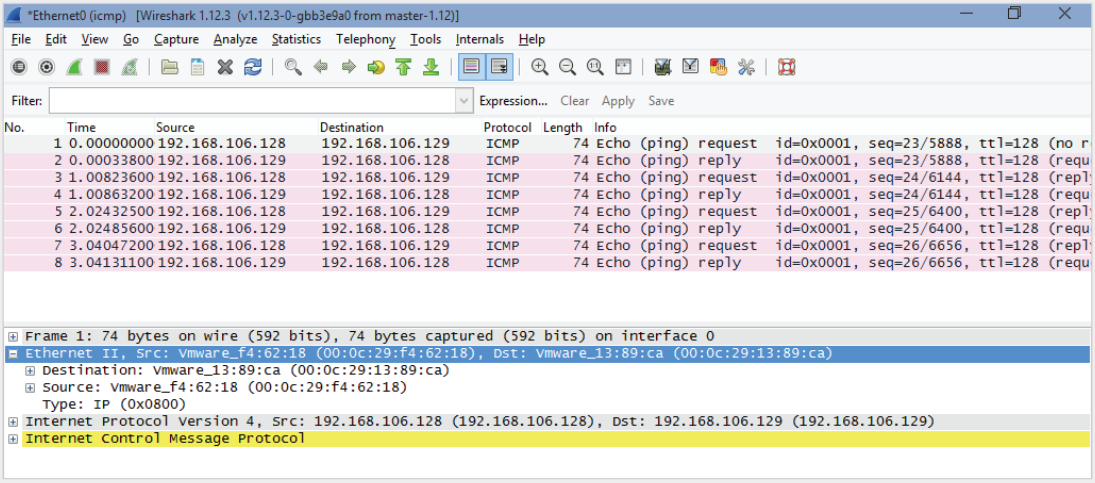

Figure 3-17 An Ethernet II frame in Wireshark
Source: Wireshark

6. Notice the three fields in the Ethernet II frame: Destination, Source, and Type. The Destination and Source fields are the destination and source MAC addresses in the frame. In Figure 3-17, you see "Vmware" before the source and destination addresses because Wireshark attempts to resolve the NIC manufacturer coded in the MAC address's first six digits. The full MAC address (without manufacturer name) is shown in parentheses. The Type field has the value 0x800, which indicates that the protocol in the frame is IP. Click to expand the **Internet Protocol Version 4** row.

7. Under Internet Protocol Version 4, you see details of the IP header, including the destination and source IP addresses. Click to expand the **Internet Control Message Protocol** row to view details of the ICMP protocol header. (You learn more about IP-related protocols in Chapter 5.)
8. Click to expand the **Data** portion of the frame, and then click the **Data** field to see the ICMP message data in hexadecimal in the bottom pane (see Figure 3-18). The right side of this pane shows the translation from hexadecimal to ASCII (human-readable characters); as you can see, it's just portions of the alphabet repeated. Some `ping` programs include more clever data, such as "Hello, are you there?" The actual data in a ping message doesn't matter; what matters is that the reply contains the same data as the ping request.

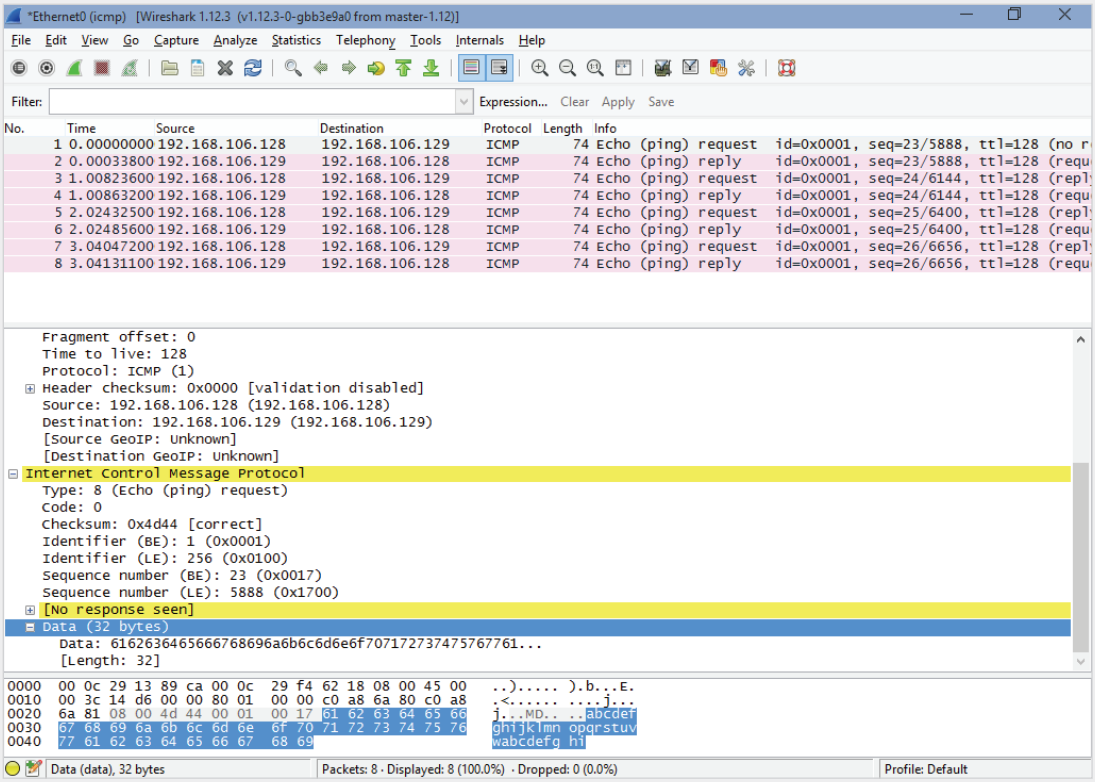

Figure 3-18 The data portion of an ICMP message

Source: Wireshark

9. Exit Wireshark and click **Quit without Saving** when prompted. Close the command prompt window. Stay logged on if you're going on to the next project; otherwise, shut down your computer.

802.11 Wi-Fi

Certification

98-366 Understanding network infrastructures:

Understand wireless networking

Understand network topologies and access methods

The 1997 802.11 wireless networking standard, also referred to as **Wireless Fidelity (Wi-Fi)**, has continued to undergo development. With it, manufacturers of wireless networking devices have brought inexpensive, reliable wireless LANs (WLANs) to homes and businesses. In fact, Wi-Fi has become so affordable that some businesses give it away free. In most towns, you can usually find a public Wi-Fi network, called a **hotspot**, at a local library or McDonald's, where you can connect with your tablet or smartphone.

Note

Wi-Fi networks are also known as "wireless LANs (WLANs)," and the terms can be used interchangeably.

Essentially, 802.11 wireless is an extension to Ethernet, using airwaves instead of cabling as the medium, although most 802.11 networks incorporate some wired Ethernet segments. The 802.11 networks can extend from several feet to several thousand feet, depending on equipment (such as antennas) and environmental factors, such as obstructions and radio frequency interference. The following sections discuss these aspects of 802.11 Wi-Fi:

- Modes of operation
- Channels and frequencies
- Antennas
- Access methods and operation
- Signal characteristics
- Standards

Wi-Fi Modes of Operation

Wi-Fi networks can operate in one of two modes: infrastructure and ad hoc. Most Wi-Fi networks operate in **infrastructure mode**, meaning wireless stations connect through a wireless AP before they can begin communicating with other devices. Infrastructure mode uses a logical bus topology because all nodes hear all

communications (in most cases). The physical topology is more difficult to describe because there are no physical wires; however, with a central device that all nodes communicate with, it most resembles a star topology. **Ad hoc mode**, sometimes called "peer-to-peer mode," is a wireless mode of operation typically used only in small or temporary installations. There's no central device, and data travels from one device to another in a line (more or less). If you want to describe ad hoc mode in terms of a physical and logical topology, it most resembles a physical and logical bus. Most of this chapter's discussion of Wi-Fi focuses on infrastructure mode.

Note

Ad hoc mode shouldn't be used in public environments because it's less secure than infrastructure mode. Microsoft removed the capability to create an ad hoc wireless network in the Network and Sharing Center starting with Windows 8; however, you can still create one in Windows 8 and later by using the `netsh wlan hostednetwork` command at a command prompt.

Wi-Fi Channels and Frequencies

Wi-Fi networks operate at one of two radio frequencies: 2.4 GHz and 5.0 GHz. However, this frequency is not fixed. The 2.4 GHz Wi-Fi variety operates from 2.412 GHz through 2.484 GHz, divided into 14 channels spaced 5 MHz apart, with each channel being 22 MHz wide. Because of radio frequency use restrictions, only the first 11 channels are used in North America. Other regions have channel use restrictions, too, but Japan allows using all 14 channels. The 5.0 GHz Wi-Fi variety divides frequencies between 4.915 GHz and 5.825 GHz into 42 channels of 10, 20, 40, 80, or 160 MHz each, depending on the Wi-Fi standard in use. The remainder of the discussion on Wi-Fi channels pertains to 2.4 GHz Wi-Fi because it's the most popular, but most points also apply to the 5.0 GHz varieties.

A wireless channel works somewhat like a TV channel, in which each channel works at a different frequency and can therefore carry different streams of data. When you configure a wireless AP, you can choose the channel in which it operates (see Figure 3-19). By choosing a channel that's not in heavy use, you can improve reception and throughput rate. However, 2.4 GHz channels are spaced 5 MHz apart, but each channel is actually 22 MHz wide, resulting in channel overlap. So, if you're configuring several Wi-Fi networks, you should choose channels that are five apart; for example, if you configure three Wi-Fi networks in close proximity, choose channels 1, 6, and 11 because those channels don't overlap one another.

Wi-Fi networks using the 5.0 GHz frequency have up to 24 nonoverlapping channels because they are spaced 20 MHz apart, and each channel has the option to use 20 MHz of bandwidth. Access points operating in this frequency can be configured

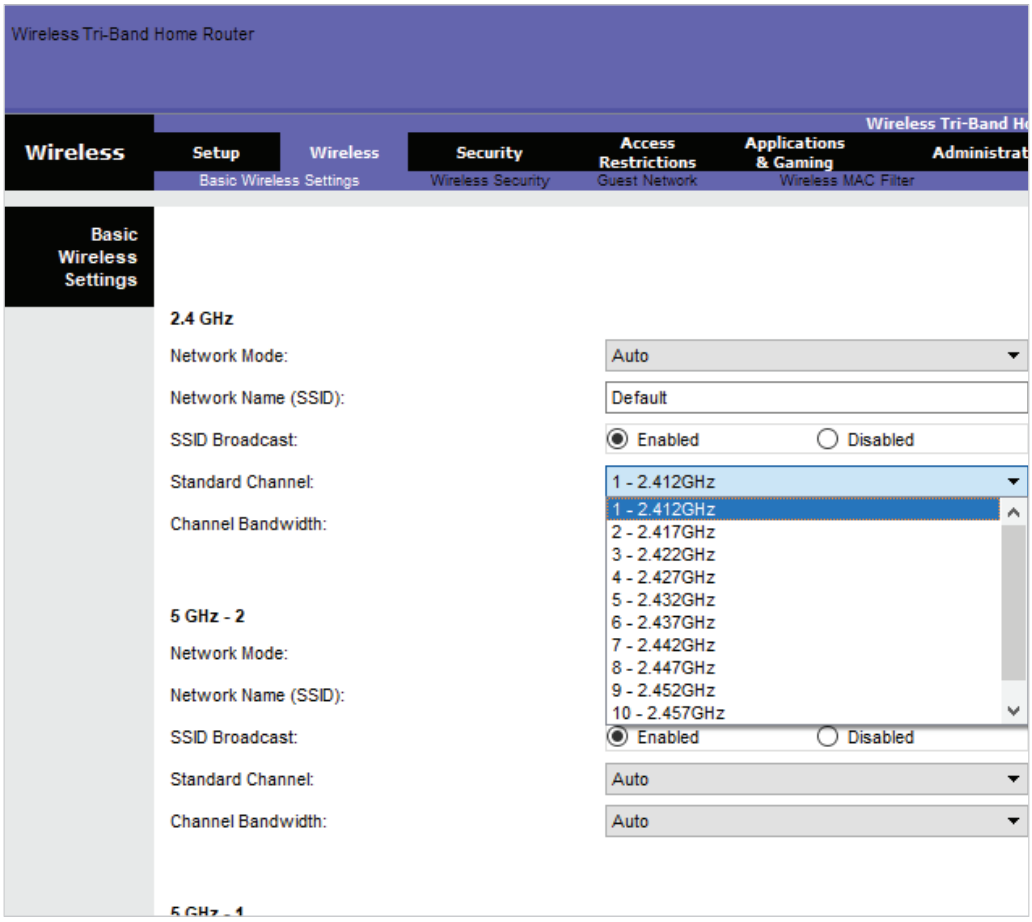

Figure 3-19 Selecting a Wi-Fi channel on an access point

Source: Linksys

to use channels wider than 20 MHz, however, which then causes adjacent channels to overlap, a fact you should be aware of when configuring 5.0 GHz Wi-Fi networks. The newer Wi-Fi standards, such as 802.11ac, configure the channel and channel bandwidth automatically, so in most cases, configuring a channel manually isn't necessary.

Several tools are available that scan channels to see how much activity is on each channel. You can then configure the AP to operate on a less frequently used channel. Figure 3-20 is an example of the output of the inSSIDer program; it shows that several Wi-Fi networks were detected. Each is labeled with its SSID and channel setting.

Wi-Fi runs in the vast range of frequencies encompassed by microwave radio. For this reason, a microwave oven can cause interference in a Wi-Fi network. The result of this interference can vary from a slight loss in signal strength to disconnection from the network while the oven is running. A change in Wi-Fi channels can sometimes lessen

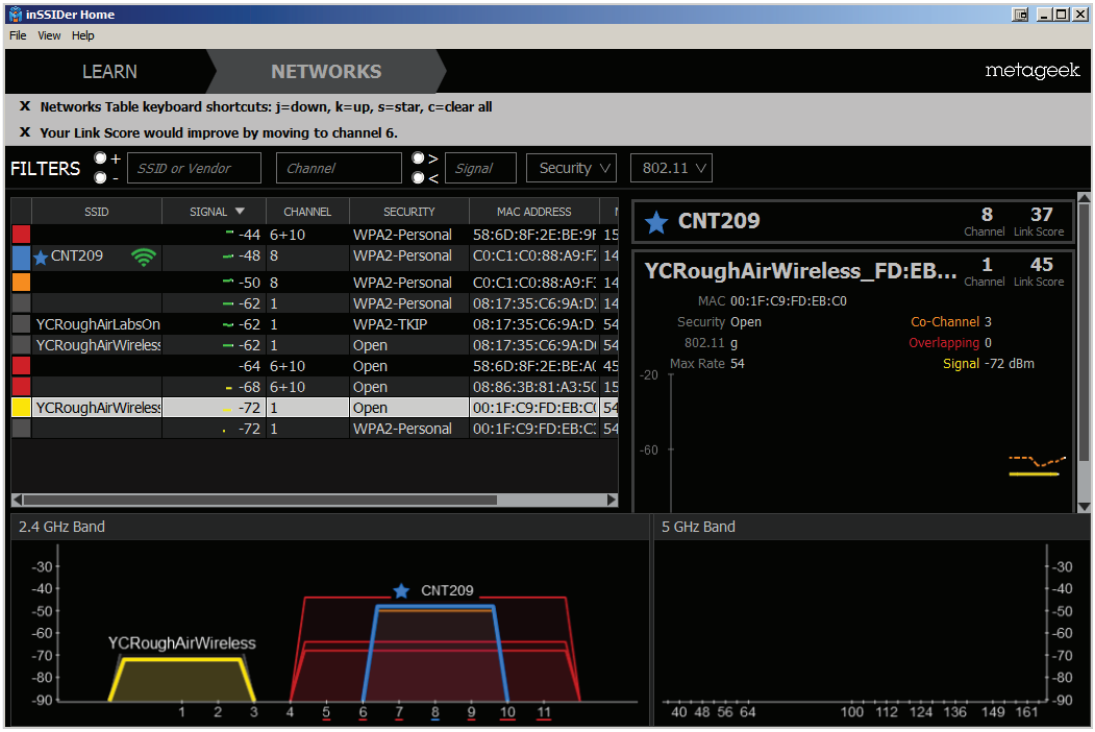

Figure 3-20 Wi-Fi network activity

Source: MetaGeek, LLC

the effects of microwave oven interference. In addition, some cordless phones use the same frequencies as Wi-Fi networks. If a cordless phone is causing interference, try changing the channel of the AP, the cordless phone (if possible), or both.

Wi-Fi Antennas

The antenna on a Wi-Fi device is both the transmitter and receiver. Its characteristics and placement determine how well a device transmits or receives Wi-Fi signals in an environment. Antennas are usually categorized by their radiation pattern, which describes how signals radiate out from the antenna:

- *Omnidirectional antenna*—In an **omnidirectional antenna**, the signals radiate out from the antenna with equal strength in all directions. If you had a perfect antenna, the radiation pattern would look like a sphere with the antenna in the center of the sphere. However, in the real world, the pattern looks more like a doughnut with the antenna situated in the center of the doughnut hole. This means signal strength is higher in spaces horizontal to the antenna's axis (see Figure 3-21) and weaker in spaces above and below the antenna. Omnidirectional antennas are used most often in WLANs because they cover a broad area. They

should be placed in a central location where mobile devices are evenly situated in all directions horizontally around the antenna, such as on a single floor of a building. Omnidirectional antennas usually look like a pole and can often be articulated up or down to change the coverage area.

Figure 3-21 The radiation pattern of an omnidirectional antenna

- *Unidirectional antenna*—With a **unidirectional antenna**, signals are focused in a single direction, which makes them ideal for placement at one end of long, narrow spaces or to cover distances between buildings. Common unidirectional antennas include the Yagi, which looks like a cylinder and produces an egg-shaped radiation pattern extending in the direction the antenna is pointed. Another common example is a dish antenna, much like those used in satellite TV installations. With this type, the dish's parabolic shape focuses received signals toward the antenna, which sticks out from the center of the dish. Transmitted signals radiate out from the dish in a column focused in the direction the antenna is pointed.

Wi-Fi Access Methods and Operation

You have learned about CSMA/CD as the access method in wired forms of Ethernet, but wireless networks have a special problem with this access method. CSMA/CD requires that all stations be able to hear each other so that each station knows when another station is sending data. This requirement is reasonable, but if two stations try to send at the same time, a collision can occur. Fortunately, in a wired network, sending stations hear the collision and attempt to resend the data. If you've ever used a push-to-talk handheld radio, you know that when you're talking, you can't hear anybody else talking, and vice versa. 802.11 networks work the same way. If a station transmits data, it can't hear whether any other station is transmitting, so if a collision does occur, the sending station doesn't detect it. For this reason, 802.11 specifies the **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** access method, in which an acknowledgment is required for every packet sent, as explained in Chapter 2. With this requirement, if a collision occurs, the sending station knows the packet didn't arrive safely because there's no acknowledgment.

Another problem exists in wireless networks that doesn't happen in wired networks. It's quite possible that in a three-station wireless network, all workstations can communicate with the AP but cannot hear each other: For example, workstation A can hear workstation B and workstation B can hear workstation C, but workstation A can't hear workstation C, perhaps because the two are out of range. This situation is called the "hidden node problem." CSMA/CA doesn't work because workstation A never knows whether workstation C is sending, and vice versa. To counteract this problem, the 802.11 standards specify another feature that uses handshaking before transmission. If this feature is enabled, a station must send the AP a request-to-send (RTS) packet requesting transmission. If it's okay to transmit, the AP sends a clear-to-send (CTS) message, and the workstation starts its communication. All other devices communicating with the AP hear the exchange of RTS and CTS messages, informing them that another device has control of the medium.

The 802.11b standard specifies a transmission rate of 11 Mbps, but this value isn't absolute. Environmental conditions can prevent transmission at this speed. Therefore, transmission speeds might be dropped incrementally from 11 Mbps to 5.5 Mbps to 2 Mbps, and finally to 1 Mbps to make a reliable connection. In addition, there's no fixed segment length for wireless networks because reliable communication relies heavily on the environment—for example, the number of walls between stations and the AP. The other 802.11 standards behave similarly.

In general, an 802.11 network operating at 2.4 GHz has a maximum distance of 300 feet at full speed with no obstructions. However, this distance can be longer with 802.11n and large, high-quality antennas. Keep in mind that the data rate might suffer as the distance and number of obstructions increase.

Tip

For an excellent tutorial on wireless networking, visit *https://computer.howstuffworks.com/wireless-network3.htm*.

Wi-Fi Signal Characteristics

In a perfect world, Wi-Fi signals would be transmitted from a device and received directly by the destination device. However, in the real world, radio signals meet with all types of obstructions, from water droplets in the air to solid walls, that affect signal quality and can severely affect a WLAN's performance and reliability. The following list explains some common types of signal interference caused by physical objects lying in the path between the transmitter and receiver:

- *Absorption*—Wi-Fi signals can pass through solid objects, such as walls and trees, but they don't get through unscathed. Solid objects absorb radio signals, causing them to **attenuate** (weaken). The denser and thicker the material, the

more signals attenuate, so a thick cinderblock wall, for example, absorbs more of the signal than a thin plywood wall. Other materials that cause absorption include water, so Wi-Fi installations outside can be affected by rain or even high humidity. The Wi-Fi signal's frequency also plays a part; the higher 5.0 GHz frequency is affected by solid objects more adversely than the 2.4 GHz frequency.

- *Refraction*—Refraction is the bending of a radio signal as it passes from a medium of one density through a medium of a different density, altering the angle of the signal's trajectory. It's similar to how light waves bend when they hit water, causing an underwater object to look like it's in a slightly different location than it actually is when viewed from outside the water. Refraction is most likely to have adverse effects with unidirectional antennas because the signals might not end up where you think they should, depending on where the antenna is pointed.
- *Diffraction*—Look at a Wi-Fi radio signal as a wave. When the wave runs into an object, it tries to bend around the object and come together on the other side. However, the wave is slightly altered, or distorted, on the far side of the object. Think of a wave of water in the ocean as it hits a small boat. The boat doesn't cause the part of the wave that hits it to disappear, but the wave is not quite the same as it continues past the boat. This is diffraction. If the object is very large so that the signal can't travel around it on all sides, part of the signal is absorbed; what's not absorbed might change direction, resulting in signal loss. This type of diffraction is a problem, especially with unidirectional signals because the change in direction could cause the signal to miss the targeted receiver.
- *Reflection*—Reflection occurs when a signal hits a dense, reflective material, such as a mirror or sheet of metal. Many metal objects, such as steel doors and furniture, can cause signal reflection, as can water or reflective glass. Reflection creates a copy of the original signal, like an echo. You don't notice an echo if the original sound and the copy arrive at your ear at the same time, but if they arrive at different times, the sound can be distorted. Signals arriving at different times (referred to as "out of phase") are called **multipath**. Multipath signals can cause distortion and errors in transmission that require the sender to retransmit.
- *Scattering*—Scattering is caused by small, irregular objects, such as leaves, chain-link fences, dust, water droplets, and so forth. The signal changes direction in unpredictable ways, causing a loss in signal strength.

Besides interference from physical obstacles, Wi-Fi signals can be degraded by other radio waves, also known as "noise." Wi-Fi signals are most susceptible to other signals in the same frequency range. Noise can come from equipment (such as microwave ovens), other wireless devices (such as cordless phones), and other wireless networks, of course. Electrical equipment can also produce electromagnetic waves that interfere with a Wi-Fi signal. So, although there's no escaping noise on a Wi-Fi network, what's important is the amount of noise compared with the signal strength, which is called the **signal-to-noise ratio**. Imagine you're having a conversation with

someone in a small, quiet room. You can both use normal speaking voices, but as more people enter the room and begin having conversations, you need to speak louder and louder so that you can be heard. In other words, you need to increase your signal (volume) to be heard over the noise of other conversations—increase your signal-to-noise ratio. If you don't, your conversation can no longer continue. Many wireless devices can increase the transmitter's power level (volume) to overcome noise and other types of interference.

All the preceding types of interference can cause signal degradation and errors that reduce the overall speed of data transfers over a wireless network. The actual amount of data transferred, not counting errors and acknowledgments, is called **throughput**. So, even though a Wi-Fi standard has a bandwidth rating of 54 Mbps, for example, the actual amount of data sent and received over the network is considerably less—usually about half the rated speed.

The actual application-to-application data transfer speed is the **goodput**, which is essentially the throughput minus the protocol headers that don't contain application data. For example, if a file containing 5 MB of data is transferred across the network in 5 seconds, the goodput is calculated at 1 MB per second, even though 10 or more MB of information might have had to be transferred in that same 5 seconds. The extra 5 MB comes in the form of packet and frame headers, acknowledgments, and retransmissions, collectively known as **overhead**. The following example uses values for maximum data transfer speed, throughput, and goodput, with megabits used instead of megabytes for easier computation:

File to be transferred: 45 megabits
Amount of nonfile data in packet and frame headers: 9 megabits
Total amount of data to be transferred: 54 megabits
Maximum data transfer speed: 54 Mbps
Amount lost to errors and acknowledgments: 27 Mbps
Throughput: 54 Mbps - 27 Mbps = 27 Mbps
Time it takes to transfer the entire file: 54 megabits/27 Mbps = 2 seconds
Goodput (size of the original file/time): 45 megabits/2 seconds = 22.5 Mbps

Wi-Fi Standards

Current Wi-Fi standards include 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac, with speeds starting at 11 Mbps for 802.11b and up to more than 5 Gbps for some versions of 802.11ac. Besides the operating speeds, the properties that distinguish these standards include the frequency at which they operate, the channel bandwidth, and support for multiple transmissions and receptions to occur simultaneously (data streams). Standards that use the same frequency are generally backward-compatible with older and slower standards. For example, an 802.11b device can still be used in an 802.11n network because both standards can operate at 2.4 GHz. Table 3-4 summarizes Wi-Fi standards and their properties.

Table 3-4 802.11 Wi-Fi standards

Wi-Fi standard	Operating frequency	Maximum data transfer speed	Indoor range[1]	Backward-compatibility	Channels, nonoverlapping	Data streams
802.11a	5.0 GHz	54 Mbps	75 ft	N/A	24 (8), 24[2]	N/A
802.11b	2.4 GHz	11 Mbps	150 ft	N/A	14 (11), 3[3]	N/A
802.11g	2.4 GHz	54 Mbps	150 ft	802.11b	14 (11), 3[3]	N/A
802.11n	5.0 and 2.4 GHz	600 Mbps	200 ft	802.11a, 802.11b, 802.11g	3 (2.4 GHz), 12 (5.0 GHz)	4
802.11ac	5.0 GHz	6 Gbps+	200 ft	802.11a, 802.11n	2, 2	Up to 8

[1]Range is difficult to measure because it can be affected by obstacles and interference sources. This table represents only approximate average values. Also, keep in mind that transfer speed decreases as the distance between devices increases.

[2]802.11a offers up to 24 channels, but only 8 are typically used in North America.

[3]802.11b and 802.11g offer 14 channels, but only 11 can be used in North America.

Take a look at the advantages and disadvantages of each standard:

- *802.11a*—This 5.0 GHz standard came out in 1999; although it was released about the same time as 802.11b, it didn't see as much commercial success. The higher frequency requires more power and has a shorter indoor range because the signals are more easily absorbed by obstructions. This standard transfers data at 54 Mbps, and because it operates at 5.0 GHz, there aren't as many sources of interference as with 2.4 GHz networks.
- *802.11b*—Operating at 2.4 GHz, 802.11b was perhaps the most widely accepted Wi-Fi standard because of its low cost and comparatively good indoor range. However, because it operates at only 11 Mbps, the newer 802.11g and 802.11n standards running at much faster speeds have rapidly replaced it. The 2.4 GHz frequency range is crowded, with cordless phones, Bluetooth devices, and microwave ovens posing interference problems for these networks.
- *802.11g*—This 2.4 GHz standard is backward-compatible with 802.11b, so people looking to upgrade to 54 Mbps can do so easily without having to replace all their devices at the same time. However, 802.11g suffers from the same interference problems as 802.11b networks. Nonetheless, both standards fueled the Wi-Fi revolution, and until recently they were the most common devices used in Wi-Fi networks.
- *802.11n*—The 802.11n standard takes much of what works in the earlier standards and improves on it by adding **multiple-input/multiple-output (MIMO)** antennas. MIMO takes advantage of multipath signals by using a separate antenna to process signals as they arrive slightly out of phase. Each separately processed signal is called a "data stream." 802.11n can use up to four antennas and achieve data rates up to 600 Mbps. It can work in the 2.4 GHz or 5.0 GHz frequency range, but the 2.4 GHz range is used more often. In an 802.11n network, you might see a Wi-Fi client connect to an AP, indicating a connection

type of 802.11a-ht or 802.11g-ht. The "ht" stands for high throughput; some manufacturers use this term to indicate that the client is connected to the AP in 802.11n mode, using 5.0 GHz (802.11a-ht) or 2.4 GHz (802.11g-ht).

- *802.11ac*—The 802.11ac standard was ratified at the end of 2013, although products based on the standard were available a few years earlier. It operates in the 5.0 GHz range only and continues to undergo development. Current implementations have data transfer speeds of about 1 Gbps, but future implementations will have speeds up to 6.93 Gbps. 802.11ac hardware will be developed in "waves," with each wave having additional data streams and faster speeds. 802.11ac improves on the MIMO technology in 802.11n by providing up to eight data streams and introducing **multiuser MIMO (MU-MIMO)**, which allows 802.11ac APs to send data to multiple client stations simultaneously. MU-MIMO works by using a process called "beamforming," in which the AP sends the signal in the direction of the receiving device instead of uniformly in all directions. Beamforming allows the AP to send data to multiple devices simultaneously if they aren't too close together. 802.11ac devices are still expensive compared with 802.11n devices and probably will be for several years, but with much faster speeds and multiuser support, 802.11ac is the standard for the future.

  Currently, Wave 2 access points are available that support data rates from over 2 Gbps to about 3.5 Gbps. Wave 1 access points typically had a maximum speed of 1.3 Gbps. Wave 3 is the full implementation of 802.11ac, with speeds up to 6.9 Gbps. Wave 3 is not the official name for the future standard of 802.11ac, but it is the most common name used.
- *802.11ax*—This is the next iteration of the 802.11 standard, and it is a work in progress. It promises speeds up to 10 Gbps and will possibly operate in the 1 GHz and 7 GHz frequency bands as well as the 2.4 GHz and 5 GHz bands of existing standards. While the top speed of this standard is expected to be just a modest improvement over the top 802.11ac speeds, efficiency improvements should allow for considerably faster throughput, resulting in much faster data transfer speeds from the user perspective.

  With this new standard, the Wi-Fi Alliance has also introduced a new, simpler naming scheme for the various Wi-Fi standards. 802.11ax has been dubbed Wi-Fi 6, 802.11ac will now be referred to as Wi-Fi 5, and 802.11n is now called Wi-Fi 4. In addition to the new naming scheme, people will be able to tell which standard they are using. The familiar Wi-Fi signal indicator on phones and computers will be accompanied by a number—as of now, 4, 5, or 6. Standards below 802.11n will not have a numeric indicator.

Wi-Fi Security

Because the network signals and therefore the network data of a Wi-Fi network aren't constrained by physical media, access to a Wi-Fi network *must* be secure. The signals from a Wi-Fi network can travel several hundred feet, which means Wi-Fi devices

outside your home or business can detect them. A person with a Wi-Fi-enabled device sitting outside your home or business can connect to an unsecured network and use your Internet access to capture packets with a program such as Wireshark—or worse, access files on your computers.

At the least, a Wi-Fi network should be protected by an encryption protocol that makes data captured by unauthorized users extremely difficult to interpret. Wi-Fi devices typically support one of the following encryption protocols, listed in order of effectiveness: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2). Not all devices support all three protocols; in particular, older devices might support only WEP and/or WPA. Wi-Fi encryption is configured on the AP, so to connect to the network, Wi-Fi devices connecting to the AP must be configured for the specific encryption protocol. Wi-Fi security is discussed in more depth in Chapters 8 and 11.

Note

WEP should be used only when it's the sole option available because its encryption protocols can be broken easily.

Token Ring Networks

Developed by IBM in the mid-1980s, the **token ring** network technology provides reliable transport of data, although it's slow by current standards. Based on the IEEE 802.5 standard, token ring networks are cabled in a physical star topology but function as a logical ring, as shown earlier in Figure 3-9. Token ring originally operated at 4 Mbps, but this speed increased to 16 Mbps and later to 100 Mbps. A 1000 Mbps standard was approved in 2001, but by that time, the token ring technology had clearly lost out to 100 Mbps Ethernet, and no 1000 Mbps products were ever manufactured in quantity. Most token ring networks used Category 4 or higher UTP.

Token Ring Media Access

Token ring uses the token-passing media access method, which is where the technology gets its name. Using this method, a special frame called the "token" passes from one computer to the next. Only the computer holding the token can send data, and a computer can keep the token for only a specific amount of time. If the computer with the token has no data to send, it passes the token to the next computer.

Because only the computer with the token can transmit data, the method prevents collisions. Computers no longer spend time waiting for collisions to be resolved, as they do in a CSMA/CD network. All computers have equal access to the medium, which makes token-passing networks best suited for time-sensitive environments, such as banking transactions and databases requiring precise timestamps. Also, because traffic moves in a specific "direction" around a ring topology, faster access methods (such as 100 Mbps token ring) can circulate two tokens at the same time without fear of collision. (By keeping the two sets of messages from overlapping, both tokens can circulate in order.)

However, token passing has two disadvantages. First, even if only one computer on the network has data to send, it must wait to receive the token. If its data is large enough to warrant two or more "turns" at the token, the computer must wait until the token makes a complete circuit before starting its second transmission. Second, the complicated process of creating and passing tokens requires more expensive equipment than what's used on CSMA/CD networks. This additional expense and complication is in part what led to token ring quickly becoming second best in LAN technologies, compared with 100 Mbps and switched Ethernet. Because token ring is no longer a widely used LAN technology, additional operating details are no longer covered.

Fiber Distributed Data Interface Technology

Fiber Distributed Data Interface (FDDI) uses the token-passing media access method and dual rings for redundancy. The rings in an FDDI network are usually a physical ring of fiber-optic cable. FDDI transmits at 100 Mbps and can include up to 500 nodes over a distance of 100 km (60 miles). FDDI full-duplex technology, an extension to standard FDDI, can support up to 200 Mbps. Like token ring, FDDI uses token passing; however, FDDI's token-passing scheme is based on IEEE 802.4 rather than IEEE 802.5. An FDDI network has no hubs; devices generally connect directly to each other. However, devices called "concentrators" can serve as a central connection point for buildings or sites in a campus setting.

Much like token ring, FDDI technology lost out to faster versions of Ethernet and is now obsolete for new network designs. It had its heyday in the early to mid-1990s when Ethernet was operating at only 10 Mbps and switched Ethernet was just being developed.

Chapter Summary

- Networks can be described by a physical and logical topology. The physical topology describes the arrangement of cabling that connects one device to another. The logical topology describes the path data travels between devices. The logical and physical topology can be different, and often are.
- The main physical topologies are the bus, star, ring, and point-to-point. A physical bus topology is simple but is no longer in common use because of a number of weaknesses. A star topology, along with the extended star, is the most common for implementing LANs. A physical ring topology isn't in widespread use now, but was used mainly in network backbones. Point-to-point topologies are used primarily in WANs and with wireless bridges. Several point-to-point connections can create a mesh topology for the purpose of redundancy.
- The main logical topologies are bus, ring, and switched. A logical bus can be implemented as a physical star or a physical bus and is used with hub-based Ethernet and Wi-Fi networks. A logical ring can be implemented as a physical ring or a physical star and is most commonly seen in

token ring and FDDI networks. The switched topology uses a physical star and is used with Ethernet networks and a switch in the center of a star physical topology.

- A network technology defines the structure of frames and how a network interface accesses a medium to send frames. It often defines the media types that must be used to operate correctly.
- The most common network technology for LANs is Ethernet. It's described in IEEE 802.3 and has many subcategories, including 10BaseT, 100BaseT, and 1000BaseT, that use twisted-pair copper cabling. Ethernet uses the CSMA/CD access method, which is turned off when a full-duplex connection is established. Other Ethernet standards include fiber-optic implementations, such as 100BaseFX and 1000BaseLX, among others. Faster standards such as 2.5GBaseT and 5GBaseT are compatible with existing Cat 5e and Cat 6 cable plants, whereas 10GBaseT requires Category 6a cabling.
- Wi-Fi is a wireless technology based on Ethernet, but it uses the CSMA/CA media access method. The most common Wi-Fi standards are 802.11b, 802.11g, 802.11a, 802.11n, and 802.11ac, with speeds from 11 Mbps up to several Gbps. 802.11ax will be the next 802.11 standard; it is still in development.
- The antenna on a Wi-Fi device is both the transmitter and receiver. Its characteristics and placement determine how well a device transmits or receives Wi-Fi signals in an environment. Antennas are usually categorized by their radiation pattern: omnidirectional or unidirectional.
- Wi-Fi signal interference can severely affect a WLAN's performance and reliability. Common types of interference include absorption, refraction, diffraction, reflection, and scattering. Noise from equipment and other wireless devices and networks can also interfere with a Wi-Fi signal. This interference can cause signal degradation and errors that reduce the overall speed of data transfers over a wireless network.
- Token ring and FDDI are obsolete technologies that used a token-passing access method. Token ring operated at speeds of 4 Mbps and 16 Mbps and ran over twisted-pair cabling, whereas FDDI ran over fiber-optic cabling at 100 Mbps.

Key Terms

1000BaseT Ethernet
100BaseFX
100BaseTX
10BaseT
10GBaseT
2.5/5 GBaseT
ad hoc mode
attenuation
baseband
broadband
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
collision
collision domain
Cyclic Redundancy Check (CRC)
extended star topology
Fiber Distributed Data Interface (FDDI)
goodput
hotspot
infrastructure mode
logical topology
media access method
mesh topology
multipath

multiple-input/multiple-output (MIMO)
multiuser MIMO (MU-MIMO)
network backbone
omnidirectional antenna
overhead
physical bus topology
physical ring topology
physical star topology
physical topology
point-to-multipoint (PMP) topology
point-to-point topology
signal bounce
signal propagation
signal-to-noise ratio
terminator
throughput
token ring
unidirectional antenna
wireless bridge
Wireless Fidelity (Wi-Fi)

Review Questions

1. Which of the following describes the arrangement of network cabling between devices?
   a. Logical topology
   b. Networking technology
   c. Physical topology
   d. Media access method
2. Which of the following is an advantage of a star topology? (Choose all that apply.)
   a. Allows faster technologies than a bus does
   b. Requires less cabling than a bus
   c. Centralized monitoring of network traffic
   d. No single point of failure
3. Which topology is likely to be deployed in a WAN where there's a central office and three branch offices, and you want all traffic from the branch offices to go through the central office network?
   a. Ring
   b. PMP
   c. Mesh
   d. Point-to-point
4. Which technology is likely to be implemented as a point-to-point physical topology?
   a. Wi-Fi infrastructure mode
   b. FDDI
   c. Ethernet
   d. Wireless bridge
5. Which of the following describes a hub-based Ethernet network?
   a. Physical bus
   b. Logical bus
   c. Physical switching
   d. Logical star
6. You're configuring a WLAN in a long, narrow ballroom. The only place you can put the AP is at the far end of the room. Which type of antenna should you use?
   a. Unidirectional
   b. Bidirectional
   c. Omnidirectional
   d. Semidirectional
7. Which of the following best describes a typical wireless LAN?
   a. Logical ring topology
   b. Logical switching topology
   c. Logical bus topology
   d. Logical star topology
8. Which of the following is a characteristic of a switched logical topology? (Choose all that apply.)
   a. Uses a physical bus topology
   b. Creates dynamic connections
   c. Sometimes called a shared-media topology
   d. Uses a physical star topology

9. Which of the following is a characteristic of unshielded twisted-pair cabling? (Choose all that apply.)
   a. Consists of four wires
   b. Commonly used in physical bus topologies
   c. Has a distance limitation of 100 meters
   d. Susceptible to electrical interference
10. Which of the following is a characteristic of fiber-optic cabling? (Choose all that apply.)
   a. Can be used in electrically noisy environments
   b. Requires only a single strand of fiber for network connections
   c. Carries data over longer distances than UTP does
   d. Lower bandwidth capability
11. Which topology most likely uses coaxial cabling?
   a. Physical star
   b. Logical ring
   c. Physical bus
   d. Logical switching
12. Which of the following is true of a MAC address?
   a. All binary 1s in the source address indicate a broadcast frame.
   b. It's sometimes called a logical address.
   c. A destination address of 12 hexadecimal Fs is a broadcast.
   d. It's composed of 12 bits.
13. Which type of Wi-Fi signal interference is most likely to be caused by leaves on trees?
   a. Diffraction
   b. Reflection
   c. Refraction
   d. Scattering
14. Which of the following is a field of the most common Ethernet frame type? (Choose all that apply.)
   a. ARP trailer
   b. FCS
   c. Destination MAC Address
   d. Data
   e. MAC type
15. Which access method uses a "listen before sending" strategy?
   a. Token passing
   b. CSMA/CD
   c. Token bus
   d. Polling
16. Which of the following is true about full-duplex Ethernet? (Choose all that apply.)
   a. Stations can transmit and receive, but not at the same time.
   b. Collision detection is turned off.
   c. It's possible only with switches.
   d. It allows a physical bus to operate much faster.
17. Which of the following is defined by the extent to which signals in an Ethernet bus topology network are propagated?
   a. Physical domain
   b. Collision domain
   c. Broadcast domain
   d. Logical domain
18. Which of the following is considered a property of Ethernet? (Choose all that apply.)
   a. Scalable
   b. Best-effort delivery system
   c. Guaranteed delivery system
   d. Obsolete technology
19. Which of the following is true of IEEE 802.3an?
   a. Requires two pairs of wires
   b. Uses Category 5 or higher cabling
   c. Currently best for desktop computers
   d. Operates only in full-duplex mode

20. Which Ethernet standard can deliver up to 5 Gbps of bandwidth over Cat 5e and Cat 6 cabling?
    a. IEEE 802.3an
    b. 802.3ab
    c. 802.3bz
    d. 802.3u
21. Which Wi-Fi standard can provide the highest bandwidth?
    a. 802.11ac
    b. 802.11b
    c. 802.11n
    d. 802.11g
22. Which of the following is true about infrastructure mode in wireless networks? (Choose all that apply.)
    a. Best used for temporary networks
    b. Uses a central device
    c. Resembles a physical bus and logical ring
    d. Most like a logical bus and physical star
23. How many channels can be used on an 802.11b network in North America?
    a. 7
    b. 9
    c. 11
    d. 13
24. Which media access method does Wi-Fi use?
    a. CSMA/CD
    b. Token bus
    c. Demand priority
    d. CSMA/CA
25. Which Wi-Fi standard uses beamforming to allow an AP to send data to multiple devices simultaneously?
    a. 802.11ac
    b. 802.11n
    c. 802.11a
    d. 802.11g

Packet Tracer Labs

Packet Tracer Lab 3-1: Building a Physical Star Topology Network

Time Required: 10 minutes

Objective: Build a physical star topology network.

Required Tools and Equipment: A computer with Packet Tracer installed

Description: In this Packet Tracer lab, you build a small physical star topology network. After each station is connected to the hub, you ping another station to verify connectivity. You view the travel of packets in Simulation mode so you can determine the logical topology.

1. Open Packet Tracer.
2. Click **Network Devices** on the top row of the device selection palette, if necessary. Click and drag a hub (the third icon from the left) into the main window.
3. Click **End Devices** on the top row of the device selection palette and click and drag a PC into the main window. Drag two more PCs into the main window so there are three PCs.
4. Click **Connections** and then click the **Copper Straight-Through** connection. Click **PC0** and then click **FastEthernet0** to connect one end of the cable to PC0. Then click the hub and click **FastEthernet0** to connect the other end of the cable. Repeat the process with

the other two PCs, being sure to choose a different Ethernet port on the hub each time. Once complete, the network should look like Figure 3-22. You have built a physical star topology network. Now, we will see the logical topology.

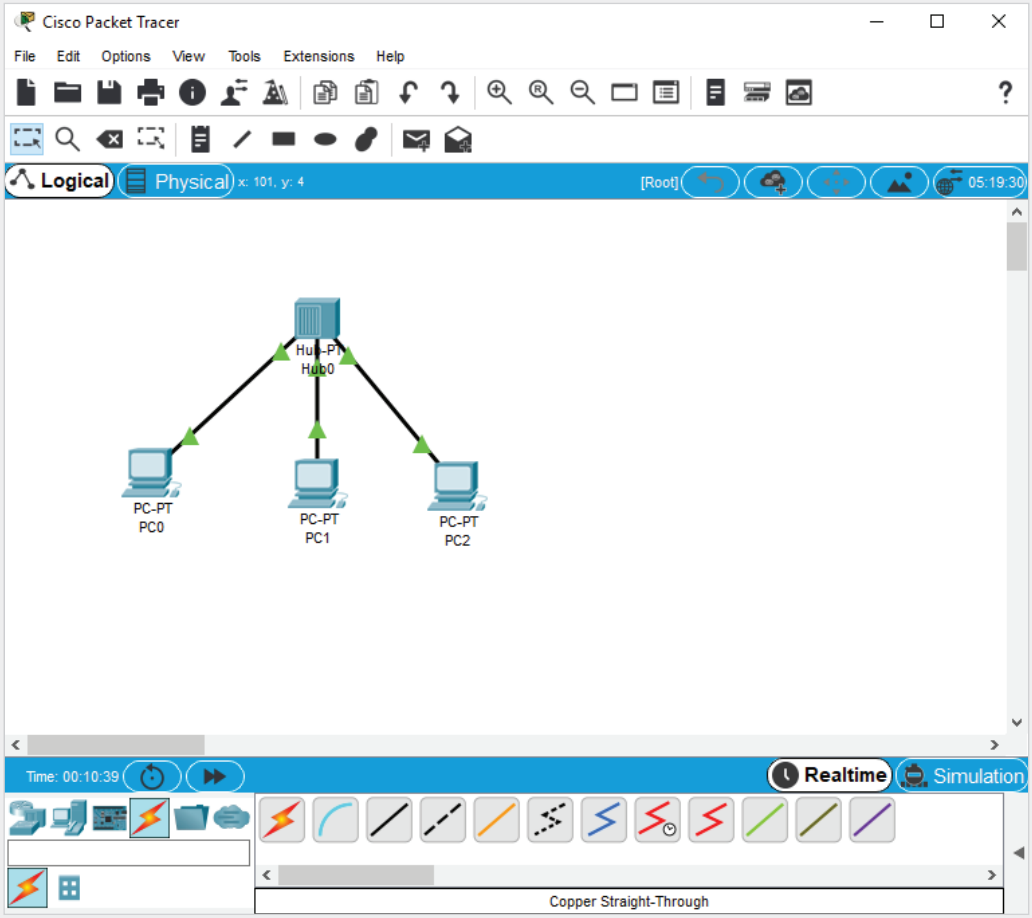

Figure 3-22 A star topology in Packet Tracer

Source: Cisco Systems, Inc.

5. Before you can send packets, recall that you need to assign an IP address to each PC. Click **PC0** and click the **Desktop** tab. Click **IP Configuration** and enter or check the following values:
   - IP Address: **192.168.1.1**
   - Subnet Mask: **255.255.255.0** (this value will automatically be filled in for you)
6. Close PC0's configuration window and repeat the process for PC1 and PC2, assigning **192.168.1.2** and **192.168.1.3**, respectively, with **255.255.255.0** as the subnet mask.
7. Open the results panel on the lower-left side of the screen by clicking the left-pointing arrow. Click **Add Simple PDU**, click **PC0**, and then click **PC1**. You should see a status

of Successful in the results panel in the lower-right corner. Unfortunately, you didn't see how the packets traveled, so the logical topology couldn't be determined. To enter Simulation mode, click the **Simulation** button above the results panel.

8. 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.
9. To send the packet again in Simulation mode, click **Add Simple PDU**, click **PC0**, and then click **PC1**.
10. You see the packet on PC1. Click the **Play** button, which is the right-pointing triangle next to the PLAY CONTROLS label. The packet moves from PC0 to the hub, and then you see that the hub forwards the packet to both PC1 and PC2. Recall that a hub repeats all signals it sees to all connected ports. When the packet arrives at PC2, you see a red X, indicating the packet was discarded. PC1 sends a reply and the hub again forwards the reply to all connected ports. Again, PC2 discards it and PC0 successfully receives the reply (see Figure 3-23).

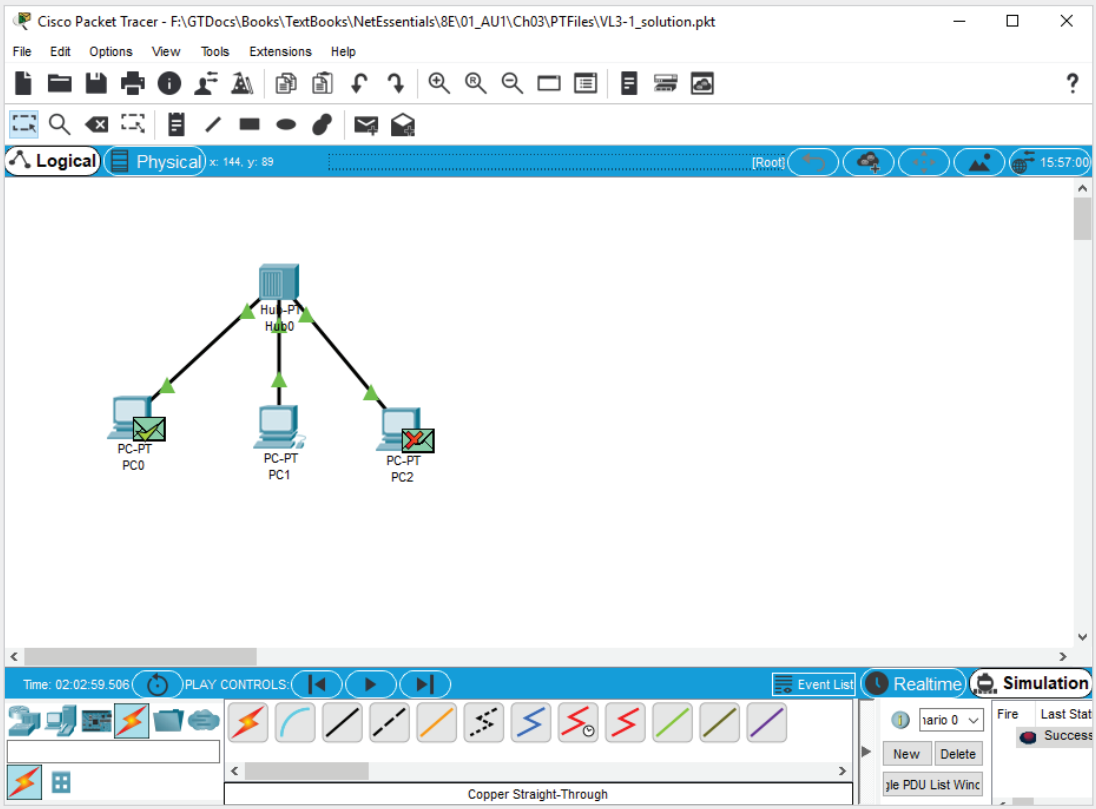

Figure 3-23 The results of a bus logical topology

Source: Cisco Systems, Inc.

11. You witnessed the behavior of a bus logical topology because all stations received the transmitted packets. Click the **Delete** button to clear the packets.
12. Keep Packet Tracer open for the next Packet Tracer lab or save the file and name it VL3-1.pkt.

Packet Tracer Lab 3-2: Viewing an Ethernet Frame in Packet Tracer

Time Required: 10 minutes

Objective: View the details of a packet sent from one computer to another.

Required Tools and Equipment: A computer with Packet Tracer installed and the completion of Packet Tracer Lab 3-1

Description: In this project, you send a packet from one computer to another and view the contents of the packet.

1. If necessary, open Packet Tracer and the file you saved in the previous Packet Tracer Labs. Make sure you are in Simulation mode.
2. Click **Add Simple PDU**, click **PC0**, and then click **PC1**.
3. Click the packet on PC0 to see details about the packet (see Figure 3-24). Read the description of what is occurring on the OSI Model tab. This may not make complete sense to you yet, but it will as you learn more about TCP/IP and packet movement through a network.

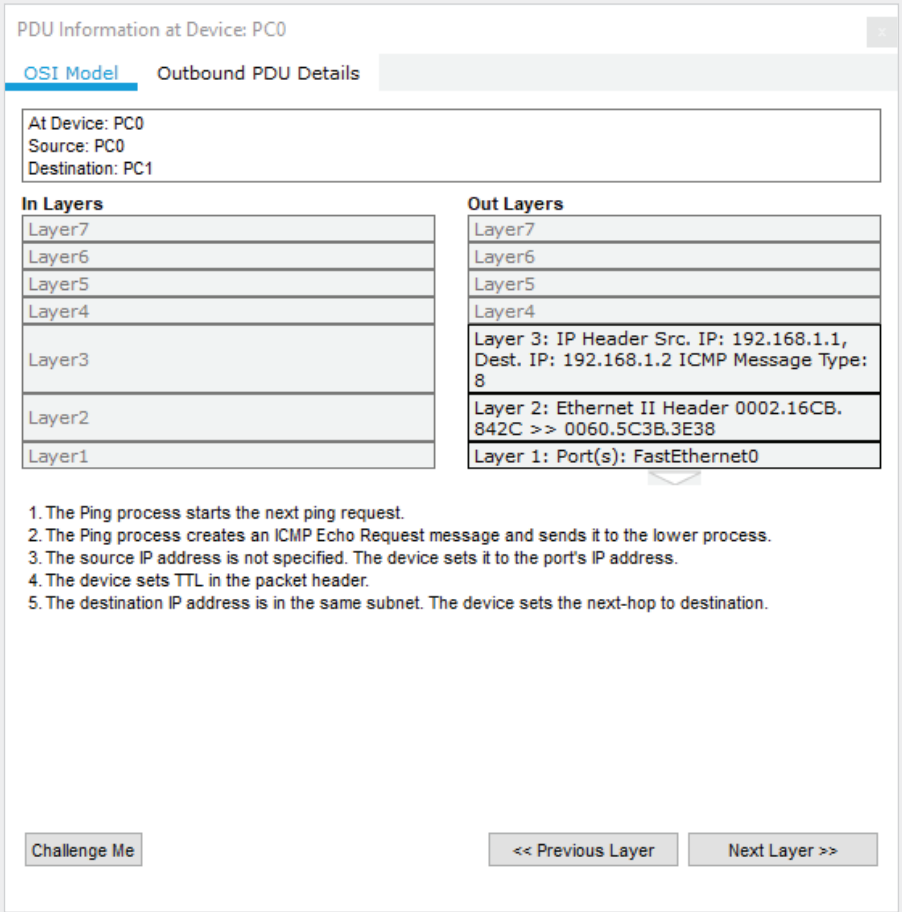

Figure 3-24 Viewing the details of an Ethernet frame in Packet Tracer

Source: Cisco Systems, Inc.

4. Click the **Outbound PDU Details** tab (see Figure 3-25). Under the Ethernet II section, ignore the PREAMBLE field for now, but notice the DEST ADDR and SRC ADDR fields. These fields contain the MAC addresses of the destination (receiving) computer and source (sending) computer, respectively. You also see a Type field with a value of 800, indicating that the frame contains an IP packet. Next, you see the DATA field and finally the FCS field, which is the error-checking field.

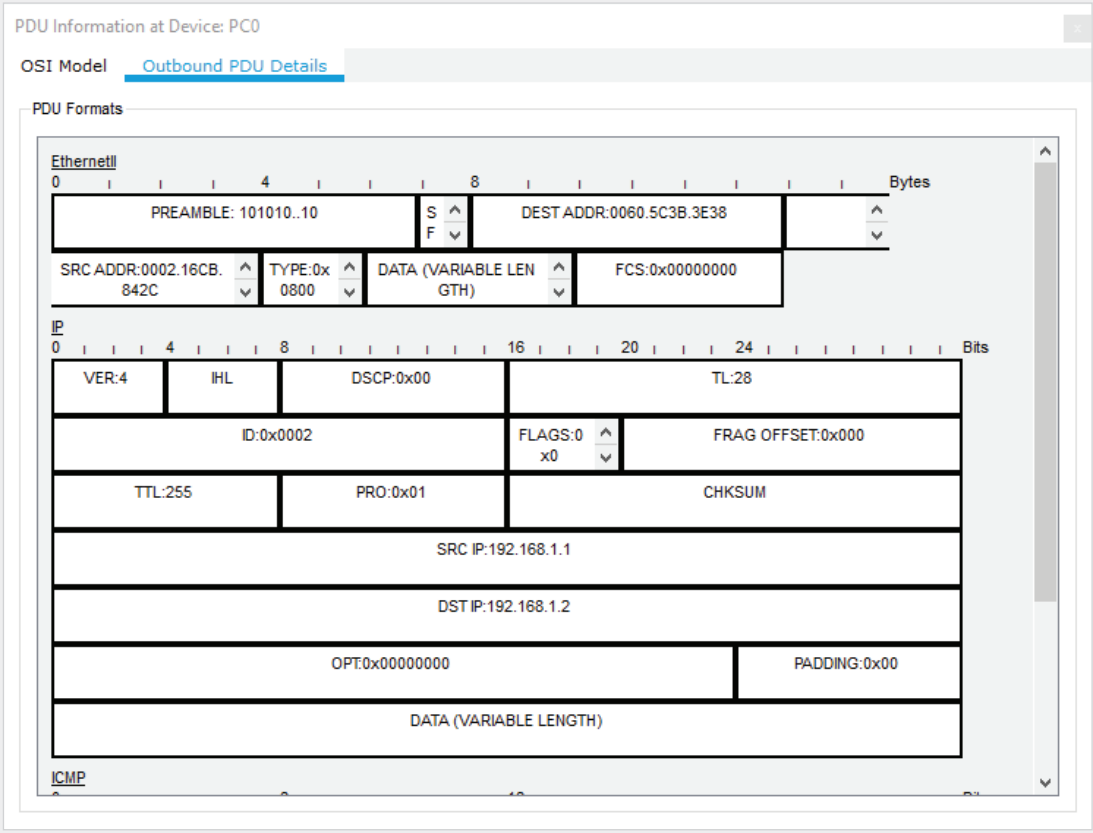

Figure 3-25 Outbound PDU details

Source: Cisco Systems, Inc.

5. Under the IP section, you see details about the IP protocol, including the source and destination IP address. Further down, under ICMP, you see information about the ping packet. Most of what you see will begin to make more sense as you continue studying network protocols, in particular TCP/IP.
6. Close the PDU Information at Device: PC0 window.
7. Close Packet Tracer. If desired, you can save the file and explore it later in more detail; otherwise, click **No** when prompted to save your work.

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 setup for which you supply a written solution.

Challenge Lab 3-1: Building an Extended Star Topology Network

Time Required: 30 minutes
Objective: Use hubs and switches to build an extended star topology network.
Required Tools and Equipment: Determine which type of devices and how many you need to build the network.
Description: In this lab, you build an extended star network in which the computers are connected in a physical star and a logical bus topology; the computers form the outer arms of the extended star. The center of the extended star should be a device that creates one collision domain per port. Build the network with as much equipment as you have available, distributing computers evenly around the outer edges of the extended star. Draw the final topology and label the devices. If you lack equipment, you can simply draw the topology without building the physical network. Then answer the following questions:

- To what type of device are the computers attached?

  _____

- What type of device is at the center of the extended star?

  _____

- How many collision domains are in this network?

  _____

Challenge Lab 3-2: Adding Wireless Access to the Extended Star Network

Time Required: 30 minutes
Objective: Add wireless networking to the extended star network you built in Challenge Lab 3-1.
Required Tools and Equipment: An access point or wireless router and some wireless NICs
Description: Add wireless networking to the extended star network you built in Challenge Lab 3-1. If you don't have the necessary equipment, just expand the drawing to include the AP or wireless router. Answer the following questions:

- To which device in your extended star did you connect the AP and why?

  _____

- Which wireless mode are you using: ad hoc or infrastructure?

  _____

- What logical and physical topology does adding wireless bring to this network?

  _____

Challenge Lab 3-3: Downloading and Installing inSSIDer

Time Required: 20 minutes

Objective: Install a wireless scanning tool and scan your network.

Required Tools and Equipment: A computer with a wireless NIC and access to the Internet or an already downloaded copy of inSSIDer

Description: In this lab, you download inSSIDer from *http://metageek.net* and install it on a computer with a wireless NIC. Your instructor might need to install it for you if you don't have the necessary permissions. After it's installed, start a scan of your network to look for access points. Answer the following questions:

- Approximately how many wireless networks did inSSIDer find?

  _____

- Which wireless channels are the most heavily used?

  _____

- If you were to set up a new wireless LAN based on what inSSIDer found, what channel would you use for the network?

  _____

Case Project 3-1

Old-Tech Corporation has 10 computers in its main office area, which is networked in a star topology using 10 Mbps Ethernet hubs, and it wants to add five computers in the manufacturing area. One problem with the existing network is data throughput. Large files are transferred across the network regularly, and the transfers take quite a while. In addition, when two or more computers are transferring large files, the network becomes unbearably slow for users. Adding the manufacturing computers will only make this problem worse and result in another problem. Because the ceiling in the manufacturing area is more than 30 feet high, there's no easy way to run cables to computers, and providing a secure pathway for cables is next to impossible. Devise a solution to this company's networking problems. As part of your solution, answer the following questions:

- What changes in equipment are required to bring this company's network up to date to solve the shared-bandwidth problem?

  _____

  _____

- What topology and which type of device can be used in the manufacturing area to solve the cabling difficulties?

  _____

  _____

Case Project 3-2

EBiz.com has 250 networked computers and five servers and uses a star topology wired network to reach employees' offices, with a bus interconnecting three floors in its office building. Because of a staggering influx of Internet business, the network administrator's task is to boost network performance and availability as much as possible. The company also

wants a network design that's easy to reconfigure and change because workgroups form and disband frequently, and their membership changes regularly. All computers must share sensitive data and control access to customer files and databases. Aside from the customer information and billing databases, which run on all servers, employees' desktop computers must run standard word-processing and spreadsheet programs.

Fill in the following lines to evaluate the requirements for this network. After you finish, determine the best network topology or topology combination for the company. On a blank piece of paper, sketch the network design you think best suits the needs of EBiz.com. Remember: High performance and easy reconfiguration are your primary design goals!

- What type of topology should be used in this network?

  _____

  _____

- Will the network be peer-to-peer or server based?

  _____

  _____

- How many computers will be attached to the network?

  _____

  _____

- What kind of networking device is easiest to reconfigure? What kind offers the best access to the network medium's bandwidth between pairs of devices?

  _____

  _____

Case Project 3-3

ENorm, Inc. has two sites in Pittsburgh that are 4 miles apart. Each site consists of a large factory with office space for 25 users at the front of the factory and up to 20 workstations in two work cells on each factory floor. All office users need access to an inventory database that runs on a server at the Allegheny Street location; they also need access to a billing application with data residing on a server at the Monongahela site. All factory floor users also need access to the inventory database at the Allegheny Street location.

Office space is permanently configured, but the manufacturing space must be reconfigured before each new manufacturing run begins. Wiring closets are available in the office space. Nothing but a concrete floor and overhead girders stay the same in the work cell areas. The computers must share sensitive data and control access to files. Aside from the two databases, which run on the two servers, office computers must run standard word-processing and spreadsheet programs. Work cell machines are used strictly for updating inventory and quality control information for the Allegheny Street inventory database. Workstations in the manufacturing cells are switched on only when they're in use, which might occur during different phases of a manufacturing run. Seldom is a machine in use constantly on the factory floor.

Fill in the following lines to evaluate the requirements for this network. After you finish, determine the best network topology or topology combination for the company. On a blank piece of paper, sketch the network design you think best suits the needs of ENorm, Inc.

- Will the network be peer-to-peer or server based?

  _____

  _____

- How many computers will be attached to the network?

  _____

  _____

- What topology works best for the offices, given the availability of wiring closets? What topology works best for the factory floor, given its need for constant reconfiguration?

  _____

  _____