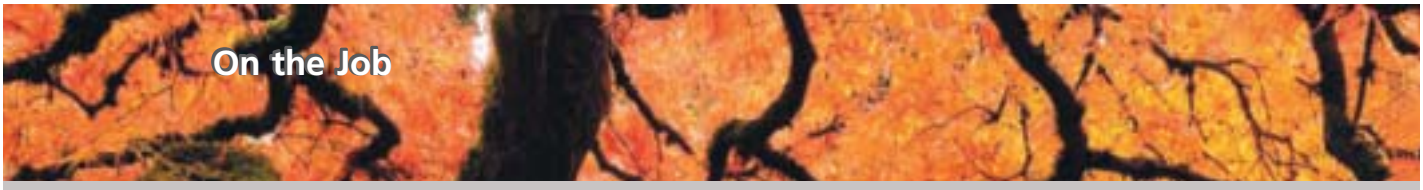
chapter 5

Topologies and Ethernet Standards

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

- Describe the basic and hybrid LAN topologies, and their uses, advantages, and disadvantages
- Describe the backbone structures that form the foundation for most networks
- Compare the different types of switching used in data transmission
- Explain how nodes on Ethernet networks share a communications channel
- Identify the characteristics of several Ethernet standards



On the Job

To a large extent, topologies and technologies have converged in today's networks, a fact that ultimately makes our IT design choices a little easier. However, it helps to know where we came from to better understand where we are going and why.

As the IT director for a community college, I was tasked with keeping about 1000 computers in four buildings up and running. Our network backbone was a distributed FDDI ring topology running over fiber-optic cable connecting all four buildings. Workstations and servers were connected via 10Base-T Ethernet hubs and switches over Cat 5 cable. One morning, we were alerted to the fact that users in Building 2 had lost connectivity to other buildings, and that no devices in Building 2 could be contacted from other buildings. A faulty FDDI concentrator was found to be the culprit.

At this point, I had a decision to make: Replace the faulty FDDI concentrator at the whopping cost of over $6000, or replace the distributed backbone FDDI ring topology with a collapsed backbone star topology using Ethernet switches for about $2000 and some design and cabling work. The former solution was easier to implement because it only required replacing one piece of equipment and no change to the design. However, a star topology with a collapsed backbone using Ethernet switches would bring our network into the twenty-first century. In addition, by updating the design, we were future-proofing our network rather than depending on more expensive 1990s technology. To me, it was a no-brainer. We spent a long Saturday afternoon, ultimately working into the wee hours of Sunday morning, reconfiguring the fiber-optic cables to work with our new collapsed backbone design. But, for the peace of mind, easier management, and better performance, it was well worth it.

Greg Tomsho
Former IT Director, Catawba Valley Community College

Just as an architect must decide where to place walls and doors, where to install electrical and plumbing systems, and how to manage traffic patterns through rooms to make a building more livable, a network architect must consider many factors, both seen and unseen, when designing a network. This chapter details some basic elements of network architecture: physical and logical topologies. These elements are crucial to understanding networking design, troubleshooting, and management, all of which are discussed later in this book.

In this chapter, you will also learn about the most commonly used network access method, Ethernet, including its many Physical layer standards. After you master the physical and logical fundamentals of network architecture, you will have all the tools necessary to design a network as elegant as the Taj Mahal.

Simple Physical Topologies

Net+ 3.5

Physical topology refers to the physical layout of the media, nodes, and devices on a network. It depicts a network in broad scope. It does not specify device types, connectivity methods, addressing schemes, or other specific details. Physical topologies are divided into three fundamental shapes: bus, ring, and star. These shapes can be mixed to create hybrid topologies.

Before you design a network, you need to understand physical topologies because they are integral to the type of network (for example, Ethernet), cabling infrastructure, and transmission media you use. You must also understand a network's physical topology to troubleshoot its problems or change its infrastructure. A thorough knowledge of physical topologies is necessary to obtain Network+ certification.

Physical topologies and logical topologies (discussed later) are two different networking concepts. You should be aware that when used alone, the word *topology* often refers to a network's *physical* topology.

Bus

A **bus topology** consists of a single cable, called the **bus**, that connects all nodes on a network without intervening connectivity devices. A bus topology can support only one channel for communication; as a result, every node shares the bus's total capacity. Most bus networks—for example, Thinnet and Thicknet—use coaxial cable as their physical medium. Bus networks rely on a **passive topology**, which means each node passively listens for, then accepts, data directed to it. When one node wants to transmit data to another node, it broadcasts an alert to the entire network, informing all nodes that a transmission is being sent; the destination node then picks up the transmission. Nodes other than the sending and receiving nodes ignore the message.

For example, suppose that you want to send an instant message to your friend Diane, who works across the hall, asking whether she wants to have lunch with you. You click the Send button after typing your message, and the data stream that contains your message is sent to your NIC. Your NIC then sends a message across the shared wire that essentially says, "I have a message for Diane's computer." The message passes by every NIC between your computer and Diane's computer until Diane's computer recognizes that the message is meant for it and responds by accepting the data.

At the ends of each bus network are 50-ohm resistors known as terminators. **Terminators** stop signals after they have reached the end of the wire. Without these devices, signals on a bus network would travel endlessly between the two ends of the network—a phenomenon known as **signal bounce**—and new signals could not get through. To understand this concept, imagine that you and a partner, standing at opposite sides of a canyon, are yelling to each other. When you call out, your words echo; when your partner replies, his words also echo. Now imagine that the echoes never fade. After a short while, you could not continue conversing because all of the previously generated sound waves would still be bouncing around, creating too much noise for you to hear anything else. On a network, terminators prevent this problem by halting the transmission of old signals. A bus network must also be grounded at one end to help remove static electricity that could adversely affect the signal. Figure 5-1 depicts a terminated bus network.

Net+
3.5

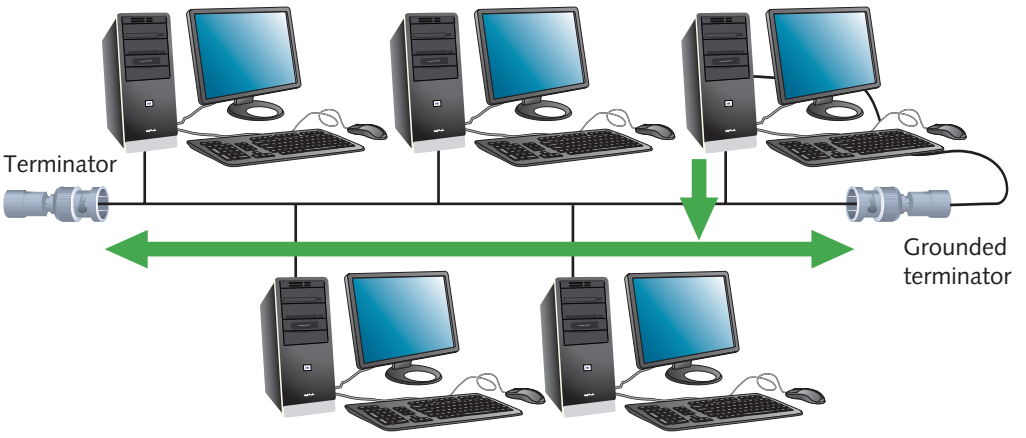


Figure 5-1 A terminated bus topology network

Although networks based on a bus topology are relatively inexpensive to set up, they do not scale well. As you add more nodes, the network's performance degrades. Because of the single-channel limitation, the more nodes on a bus network, the more slowly the network will transmit and deliver data. A bus topology is rarely practical for networks with more than a dozen workstations.

Bus networks are also difficult to troubleshoot because it is a challenge to identify fault locations. To understand why, think of the game called "telephone," in which one person whispers a phrase into the ear of the next person, who whispers the phrase into the ear of another person, and so on, until the final person in line repeats the phrase aloud. The vast majority of the time, the phrase recited by the last person bears little resemblance to the original phrase. When the game ends, it's hard to determine precisely where in the chain the individual errors cropped up. Similarly, errors may occur at any intermediate point on a bus network, but at the receiving end it's possible to tell only that an error occurred. Finding the source of the error can prove very difficult.

A final disadvantage to bus networks is that they are not very fault tolerant. **Fault tolerance** is the capability for a component or system to continue functioning despite damage or malfunction. On bus networks, any single break or a defect affects the entire network.

Because they have poor fault tolerance, do not scale well, and are difficult to troubleshoot, pure bus topologies do not form the basis of modern networks. Understanding their faults, however, will help you recognize the advantages of the more popular topologies in use today.

Ring

In a **ring topology**, each node is connected to the two nearest nodes so that the entire network forms a circle, as shown in Figure 5-2. Data are transmitted clockwise in one direction around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring. Each workstation acts as a repeater for the transmission. The fact that all workstations participate in delivery makes the

Net+ 3.5

ring topology an **active topology**. This is one way a ring topology differs from a bus topology. A ring topology also differs in that it has no "ends" and data stop at their destination. In most ring networks, twisted pair or fiber-optic cabling is used as the physical medium.

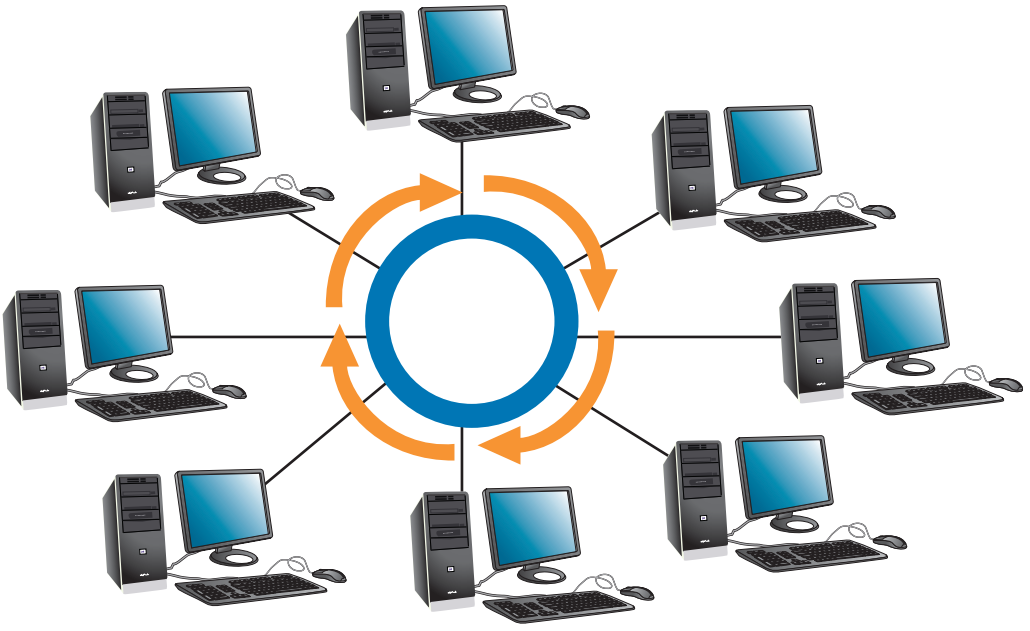


Figure 5-2 A ring topology network

One drawback of a simple ring topology is that a single malfunctioning workstation can disable the network. For example, suppose that you and five colleagues share a pure ring topology LAN in your small office. You decide to send an instant message to Cesar, who works three offices away, telling him you found his lost glasses. Between your office and Cesar's office are two other offices, and two other workstations on the ring. Your instant message must pass through the two intervening workstations' NICs before it reaches Cesar's computer. If one of these workstations has a malfunctioning NIC, your message will never reach Cesar.

In addition, just as in a bus topology, the more workstations that must participate in data transmission, the slower the response time. Consequently, pure ring topologies are not very flexible or scalable. Contemporary LANs rarely use pure ring topologies.

Star

In a **star topology**, every node on the network is connected through a central device. Years ago, the connecting device would have been a hub. On modern networks, the connecting device is a router or switch. Figure 5-3 depicts a typical star topology. Star topologies are usually built with twisted pair or fiber-optic cabling. Any single cable on a star network connects only two devices (for example, a workstation and a switch), so a cabling problem will affect

Net+ 3.5

two nodes at most. Devices such as workstations or printers transmit data to the connectivity device, which then retransmits the signal to the network segment containing the destination node.

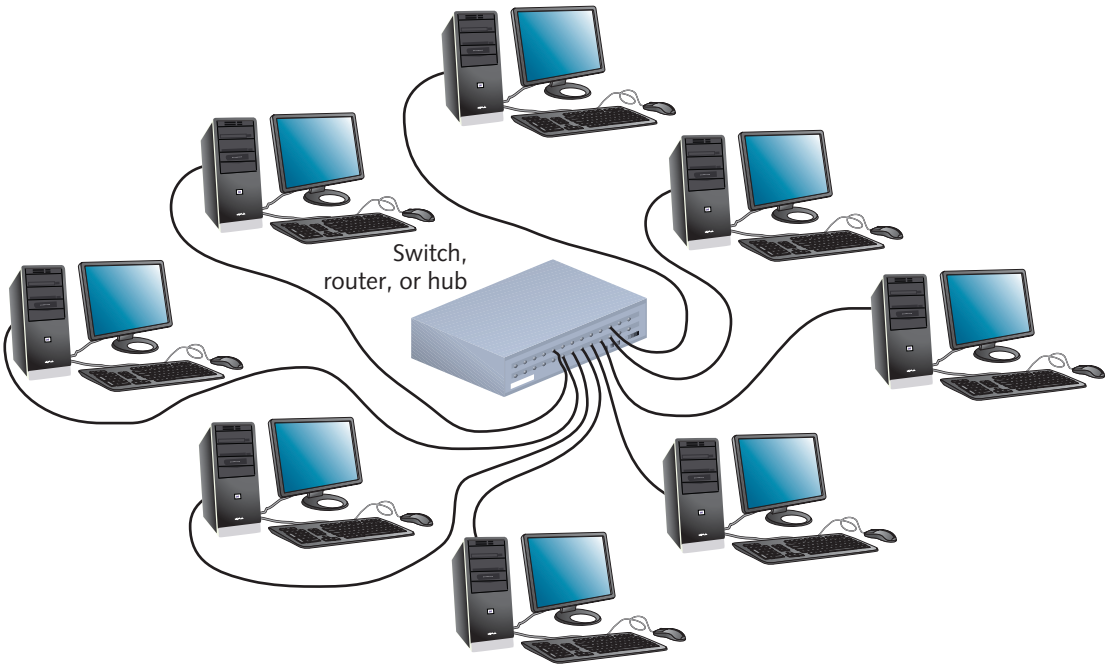


Figure 5-3 A star topology network

Star topologies require more cabling than ring or bus networks. However, because each node is separately connected to a central connectivity device, they are more fault tolerant. A single malfunctioning workstation cannot disable an entire star network. A failure in the central connectivity device can take down a LAN segment, though.

Because they include a centralized connection point, star topologies are also flexible. Nodes can easily be moved and segments can be isolated or interconnected with other networks. Star networks are, therefore, scalable. For this reason, and because of their fault tolerance, the star topology has become the most popular fundamental layout used in contemporary LANs. Single star networks are commonly interconnected with other networks through switches or routers to form more complex topologies. Modern Ethernet networks are based on the star topology.

Star networks can support a maximum of only 1024 addressable nodes on a logical network. For example, if you have a campus with 3000 users, hundreds of networked printers, and scores of other devices, you must strategically create smaller logical networks. Even if you had 1000 users and *could* put them on the same logical network, you wouldn't, because doing so would result in poor performance and difficult management. Instead, you would use routers or switches to separate segments. You'll learn more about such techniques later in this chapter and in Chapter 6.

Hybrid Topologies

Net+ 3.5

Except in very small networks, you will rarely encounter a network that follows a pure bus, ring, or star topology. Simple topologies are too restrictive, particularly if the LAN must accommodate a large number of devices. More likely, you will work with a complex combination of these topologies, known as a **hybrid topology**. Two kinds of hybrid topologies are explained in the following sections.

Star-Wired Ring

The **star-wired ring topology** uses the physical layout of a star in conjunction with the ring logical topology. In Figure 5-4, which depicts this architecture, the solid lines represent a physical connection and the dotted lines represent the flow of data. Data are sent around the star in a circular pattern. This hybrid topology benefits from the fault tolerance of the star topology, as data transmission does not depend on each workstation to act as a repeater. Token ring networks, as specified in IEEE 802.5, use this hybrid topology.

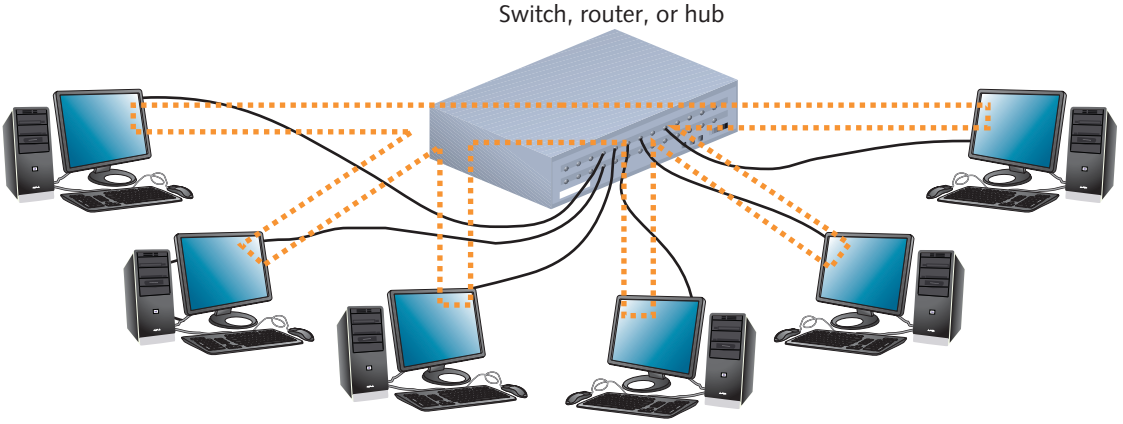


Figure 5-4 A star-wired ring topology network

Star-Wired Bus

Another popular hybrid topology combines the star and bus formations. In a **star-wired bus topology**, groups of workstations are star-connected to connectivity devices and then networked via a single bus, as shown in Figure 5-5. With this design, you can cover longer distances and easily interconnect or isolate different network segments. One drawback is that this option is more expensive than using the star topology alone because it requires more cabling and potentially more connectivity devices. However, compared with the benefits, these drawbacks are negligible. The star-wired bus topology forms the basis for modern Ethernet networks, which commonly use switches or routers as the connectivity devices.

Net+ 3.5

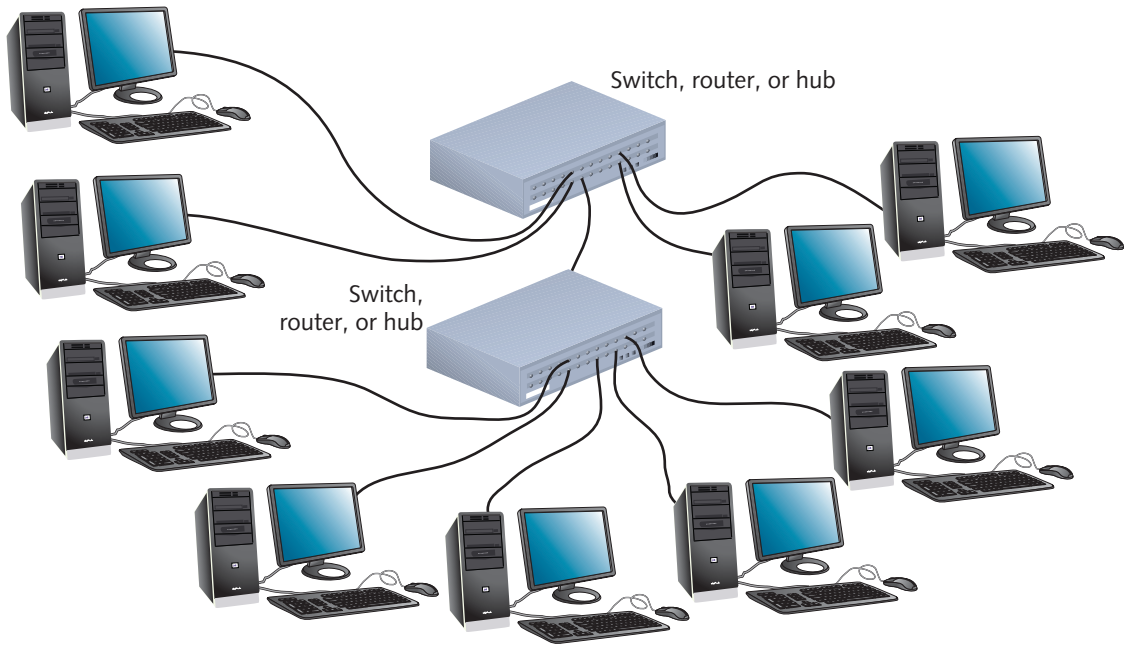


Figure 5-5 A star-wired bus topology network

Logical Topologies

Net+ 3.5

The term **logical topology** refers to the way in which data are transmitted between nodes, rather than the physical layout of the paths that data take. A network's logical topology will not necessarily match its physical topology.

The most common logical topologies are bus and ring. In a bus logical topology, signals travel from one network device to all other devices on the network or network segment. They may or may not travel through an intervening connectivity device (as in a star topology network). A network that uses a bus physical topology also uses a bus logical topology. In addition, networks that use either the star or star-wired bus physical topologies also result in a bus logical topology. Ethernet networks use the bus logical topology.

The fact that all nodes connected to a bus network can communicate directly via broadcast transmissions makes them part of a single **broadcast domain**. Similarly, all nodes connected to a single repeating device or switch belong to a broadcast domain—that is, unless the switch is specially configured to separate broadcast domains. Routers and other devices that operate at Layer 3 separate broadcast domains.

For designing and troubleshooting Ethernet networks, it is necessary to understand that all of a segment's broadcast traffic is transmitted to all of the segment's nodes. As an example, suppose you connect your laptop to your company's Ethernet network. In an attempt to contact a DHCP server and obtain an IP address, your laptop issues a DHCP discover packet in broadcast fashion. Therefore, the packet is sent to every workstation connected to the same Ethernet segment as your laptop, even though the request wasn't meant for them.

Net+ 3.5

In addition, if one device has a malfunctioning NIC that is issuing bad or excessive packets, those packets will be detected by the NICs of all devices on the same segment. The result is a waste of available bandwidth and potential transmission errors. As you will learn, however, modern Ethernet networks can overcome such drawbacks through speed and design techniques.

In contrast to a bus logical topology, in a ring logical topology, signals follow a circular path between sender and receiver. Networks that use a pure ring topology, such as the now-obsolete token ring networks, use a ring logical topology. As shown by the dashed lines in Figure 5-4, the ring logical topology is also used by the star-wired ring hybrid physical topology because signals follow a circular path, even as they travel through a connectivity device.

Backbone Networks

As you learned in Chapter 1, a network backbone is the part of a network to which segments and significant shared devices connect. Backbones usually are capable of more throughput than the media connecting nodes with connectivity devices. This added capacity is necessary because backbones carry more traffic. For example, LANs in large organizations commonly rely on a fiber-optic backbone but continue to use Cat 5 or better UTP to connect nodes with switches or routers.

Although even the smallest LAN technically has a backbone, on an enterprise-wide network, backbones are more complex and more difficult to plan. In networking, the term **enterprise** refers to an entire organization, including its local and remote offices, a mixture of computer systems, and a number of departments. Enterprise-wide computing must, therefore, take into account the breadth and diversity of a large organization's computer needs. The backbone is the most significant building block of enterprise-wide networks. It may take one of several different shapes, as described in the following sections.

Serial Backbone

A **serial backbone** is the simplest kind of backbone. It consists of two or more devices connected to each other by a single medium in a daisy-chain fashion. In networking, a **daisy chain** is simply a linked series of devices. Switches can be connected in a daisy chain to extend a network. For example, suppose you manage a small star-wired bus topology network in which a single switch serves a workgroup of eight users. When new employees are added to that department and you need more network connections, you could connect a second switch to the first switch in a daisy-chain fashion. The new switch would offer open ports for new users. Because the star-wired hybrids provide for modular additions, daisy-chaining is a logical solution for growth. Also, because switches can easily be connected through cables attached to their ports, a LAN's infrastructure can be expanded with little additional cost.

Switches are not the only devices that can be connected in a serial backbone. In fact, gateways and routers also commonly form part of the backbone. Figure 5-6 illustrates a serial backbone network, in which the backbone is indicated by a dashed line.

When designing and troubleshooting serial backbone networks, it's important to remember that only so many repeating devices can be connected in a serial fashion. Therefore, the distance you can span between connected repeating devices is limited. Later in this chapter, you will learn

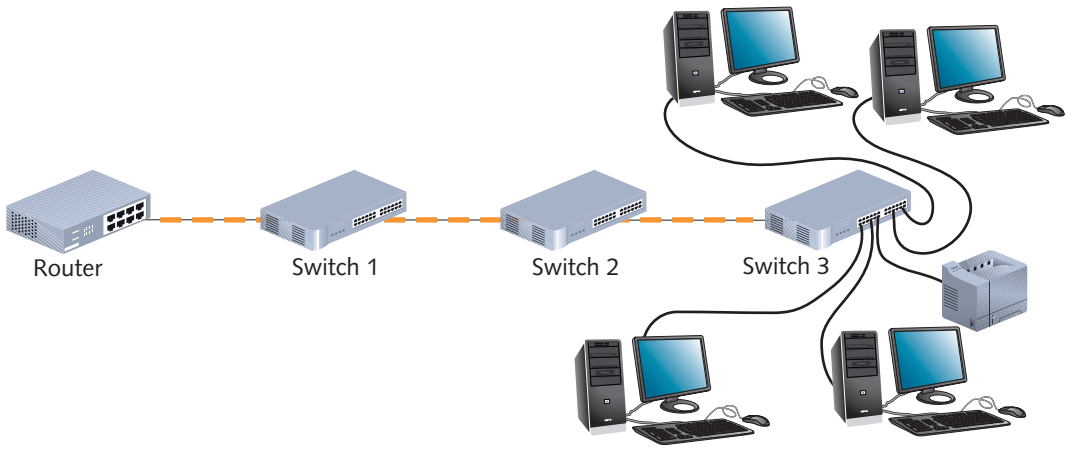


Figure 5-6 A serial backbone

about the maximum number of repeating devices and segments for each type of Ethernet network. Exceeding the maximum network length will adversely affect the performance of a LAN. If you extend a LAN beyond its recommended size, intermittent and unpredictable data transmission errors will result. Similarly, if you daisy-chain a topology with limited bandwidth, you risk overloading the channel and generating still more data errors.

Modern networks of any size don't depend on simple serial backbones. Instead, they use a more scalable and fault-tolerant framework such as a distributed backbone.

Distributed Backbone

A **distributed backbone** consists of a number of intermediate connectivity devices connected to one or more central connectivity devices, such as switches or routers, in a hierarchy, as shown in Figure 5-7. In Figure 5-7, the dashed lines represent the backbone. This kind of topology allows for simple expansion and limited capital outlay for growth because more layers of devices can be added to existing layers. For example, suppose that you are the network administrator for a small publisher's office. You might begin your network with a distributed backbone consisting of two switches that supply connectivity to your 20 users, 10 on each switch. When your company hires more staff, you can connect another switch to one of the existing switches, and use the new switch to connect the new staff to the network.

A more complicated distributed backbone connects multiple LANs or LAN segments using routers, as shown in Figure 5-8. In this example, the routers form the highest layer of the backbone to connect the LANs or LAN segments.

A distributed backbone also provides network administrators with the ability to segregate workgroups and, therefore, manage them more easily. For example, it adapts well to an enterprise-wide network confined to a single building, in which certain switches can be assigned according to the floor or department. Note that it's possible for distributed backbones to include repeating devices linked in a daisy-chain fashion. This arrangement requires the same length considerations that serial backbones demand. Another possible problem in this design relates to the potential single points of failure, such as the devices

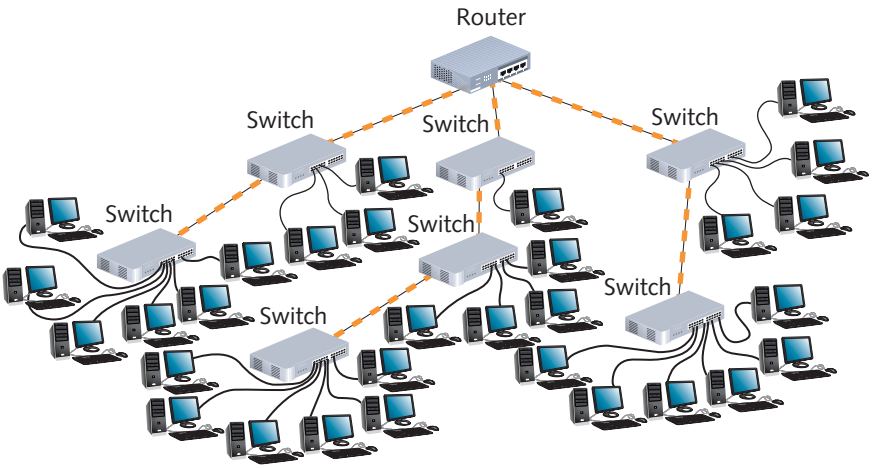


Figure 5-7 A simple distributed backbone

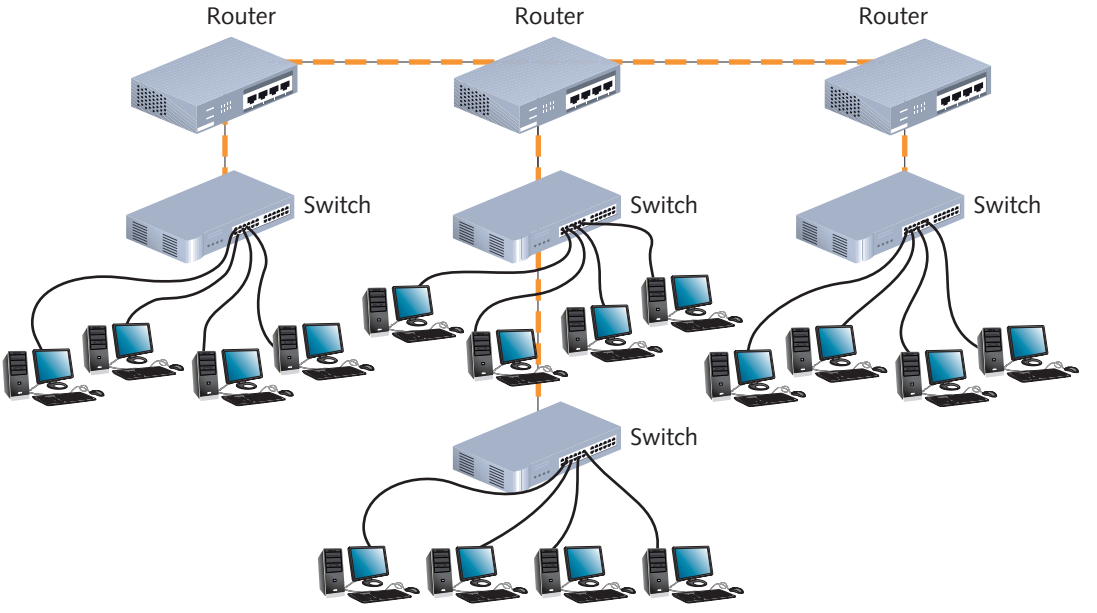


Figure 5-8 A distributed backbone connecting multiple LANs

at the uppermost layers. Despite these potential drawbacks, implementing a distributed backbone network can be relatively simple, quick, and inexpensive.

Collapsed Backbone

The **collapsed backbone** topology uses a router or switch as the single central connection point for multiple subnetworks, as shown in Figure 5-9. Contrast Figure 5-9 with Figure 5-8, in which multiple LANs are connected via a distributed backbone. In a collapsed backbone, a single

router or switch is the highest layer of the backbone. The router or switch that makes up the collapsed backbone must contain multiprocessors to handle the heavy traffic going through it. This is risky because a failure in the central router or switch can bring down the entire network. In addition, because routers cannot move traffic as quickly as switches, using a router may slow data transmission.

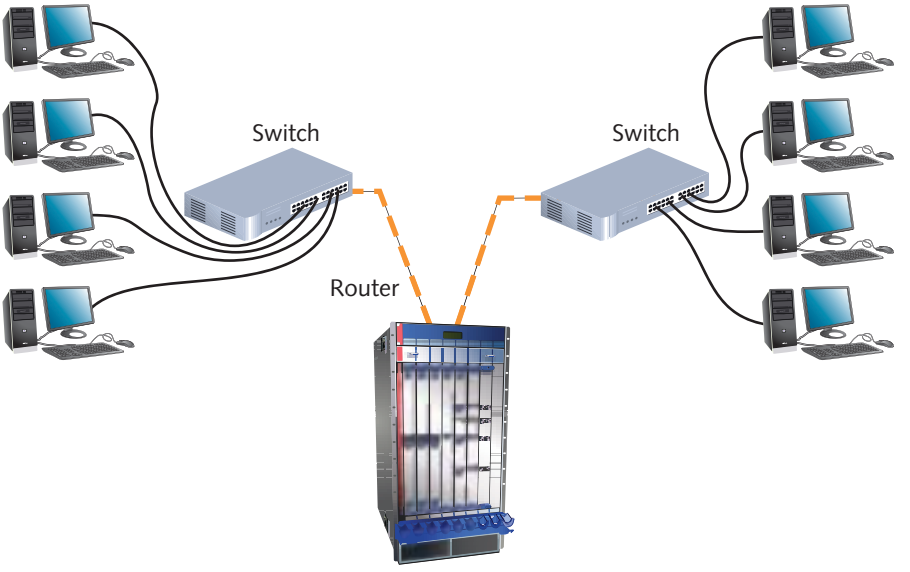


Figure 5-9 A collapsed backbone

Nevertheless, a collapsed backbone topology offers substantial advantages. Most significantly, this arrangement allows you to interconnect different types of subnetworks. You can also centrally manage maintenance and troubleshooting chores.

Parallel Backbone

A **parallel backbone** is the most robust type of network backbone. This variation of the collapsed backbone arrangement consists of more than one connection from the central router or switch to each network segment. In a network with more than one router or switch, the parallel backbone calls for duplicate connections between those connectivity devices as well. Figure 5-10 depicts a simple parallel backbone topology. As you can see, each switch is connected to the router by two cables, and the two routers are also connected by two cables.

The most significant advantage of using a parallel backbone is that its redundant (duplicate) links ensure network connectivity to any area of the enterprise. Parallel backbones are more expensive than other enterprise-wide topologies because they require much more cabling than the others. However, they make up for the additional cost by offering increased performance and better fault tolerance.

As a network administrator, you might choose to implement parallel connections to only some of the most critical devices on your network. For example, if the first and second switches in

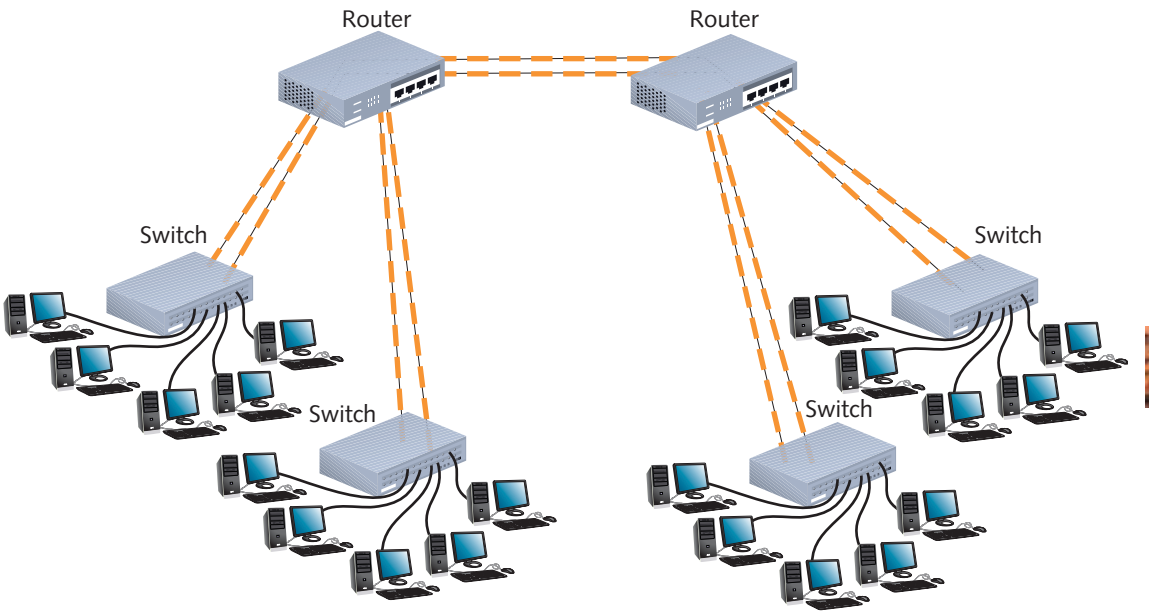


Figure 5-10 A parallel backbone

Figure 5-10 connected your Facilities and Payroll Departments to the rest of the network, and your organization could never afford to lose connectivity with those departments, you might use a parallel structure for those links. If the third and fourth switches in Figure 5-10 connected your organization's Recreation and Training Departments to the network, you might decide that parallel connections were unnecessary for these departments. By selectively implementing the parallel structure, you can lower connectivity costs and leave available additional ports on the connectivity devices.

Bear in mind that an enterprise-wide LAN or WAN may include different combinations of physical topologies and backbone designs. Now that you understand how networks may be arranged, both physically and logically, you are ready to learn more about how connections between nodes are established.

Switching

Net+ 3.4

Switching is a component of a network's logical topology that determines how connections are created between nodes. Three switching methods are used on modern networks: circuit switching, packet switching, and multiprotocol label switching.

Circuit Switching

In **circuit switching**, a connection is established between two network nodes before they begin transmitting data. Bandwidth is dedicated to this connection and remains available until the users terminate communication between the two nodes. While the nodes remain connected, all data follow the same path initially selected by the switch. Traditional telephone calls—that is, calls not carried over TCP/IP networks—for example, typically use a circuit-switched connection.

Net+ 3.4

Because circuit switching monopolizes its piece of bandwidth while the two stations remain connected, even when no actual communication is taking place, it can result in a waste of available resources. However, some network applications benefit from such a reserved path. For example, live audio or videoconferencing might not tolerate the time delay it would take to reorganize data packets that have taken separate paths through another switching method. Several WAN technologies, such as ISDN, T1 services, and ATM (described in Chapter 7), also use circuit switching.

Packet Switching

By far the most popular method for connecting nodes on a network is packet switching. **Packet switching** breaks data into packets before they are transported. Packets can travel any path on the network to their destination because, as you learned in Chapter 4, each packet contains the destination address and sequencing information. Consequently, packets can attempt to find the fastest circuit available at any instant. They need not follow each other along the same path, nor must they arrive at their destination in the same sequence as when they left their source.

To understand this technology, imagine that you work in Washington, D.C., and you organized a field trip for 50 colleagues to the National Air and Space Museum. You gave the museum's exact address to your colleagues and told them to leave precisely at 7:00 a.m. from your office building several blocks away. You did not tell your coworkers which route to take. Some might choose the subway, others might hail a taxicab, and still others might choose to drive their own cars or even walk. All of them will attempt to find the fastest route to the museum. But if a group of six decides to take a taxicab and only four people fit in that taxi, the next two people have to wait for another taxi. Or, a taxi might get caught in rush hour traffic and be forced to find an alternate route. Thus, the fastest route might not be obvious the moment everyone departs. But no matter which transportation method your colleagues choose, all will arrive at the museum and reassemble as a group. This analogy illustrates how packets travel in a packet-switched network.

When packets reach their destination node, the node reassembles them based on their control information. Because of the time it takes to reassemble the packets into a message, packet switching requires speedy connections if it's used for live audio or video transmission. Even connections as slow as a dial-up Internet service, however, are sufficiently fast to send and receive typical network data, such as e-mail messages, spreadsheet files, or even software programs from a server to a client. The greatest advantage to packet switching lies in the fact that it does not waste bandwidth by holding a connection open until a message reaches its destination, as circuit switching does. Ethernet networks and the Internet are the most common examples of packet-switched networks.

MPLS (Multiprotocol Label Switching)

Net+ 3.5

Another type of switching, **MPLS** (**multiprotocol label switching**), was introduced by the IETF in 1999. As its name implies, MPLS enables multiple types of Layer 3 protocols to travel over any one of several connection-oriented Layer 2 protocols. As you have learned, IP is the most commonly used Layer 3 protocol, and so MPLS most often supports IP. MPLS can operate over Ethernet frames, but is more often used with other Layer 2 protocols, like those designed for WANs. In fact, one of its benefits is the ability to use packet-switched technologies over

Net+ 3.5

traditionally circuit-switched networks. MPLS can also create end-to-end paths that act like circuit-switched connections.

In addition, MPLS addresses some limitations of traditional packet switching. For example, on an IP-based network, each router along the data's path must interpret the IP datagram's header to discover its destination address, and then perform a route lookup to determine where to forward the packet next. As you can imagine, stopping to process this information at every router slows transmission. In MPLS, the first router that receives a packet adds one or more labels to the Layer 3 datagram. (Collectively, the MPLS labels are sometimes called a shim because of their placement between Layer 3 and Layer 2 information. Also, MPLS is sometimes said to belong to "Layer 2.5.") Then the network's Layer 2 protocol header is added, as shown in Figure 5-11.

Labels added during MPLS include special addressing and, sometimes, prioritization information. Routers then need only interpret the MPLS labels, which can point to exclusive, predefined data paths. Network engineers have significant control in setting these paths. Consequently, MPLS offers potentially faster transmission than traditionally packet-switched or circuit-switched networks. Because it can add prioritization information, MPLS can also offer better **QoS (quality of service)**. QoS is a specification that guarantees delivery of data within a certain time frame. These advantages make MPLS especially well suited to WANs.

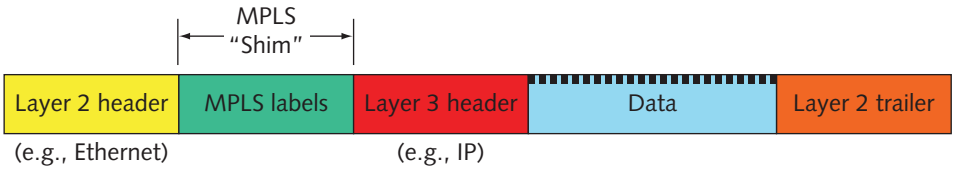


Figure 5-11 MPLS shim within a frame

Now that you are familiar with the various methods of establishing paths between nodes, you are ready to investigate Ethernet, a Layer 2 standard used on nearly every LAN.

Ethernet

Net+ 3.7

Ethernet is a flexible technology that can run on a variety of network media and offers excellent throughput at a reasonable cost. Because of its many advantages Ethernet is, by far, the most popular network technology used on modern LANs.

Ethernet has evolved through many variations, and its speed and reliability continue to improve. As a result of this history, it supports many different versions—so many, in fact, that you might find the many variations a little confusing. However, all Ethernet networks have at least one thing in common—their access method, which is known as CSMA/CD.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Net+ 3.7

A network's **access method** is its method of controlling how network nodes access the communications channel. In comparing a network with a highway, the on-ramps would be one part of the highway's access method. A busy highway might use stoplights at each on-ramp to allow only one person to merge into traffic every five seconds. After merging, cars must drive within lanes, and each lane is limited as to how many cars it can hold at one time. All of these highway controls are designed to avoid collisions and help drivers get to their destinations. On networks, similar restrictions apply to the way in which multiple computers share a finite amount of bandwidth on a network. These controls make up the network's access method.

All Ethernet networks, independent of their speed or frame type, use an access method called **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**. To understand Ethernet, you must first understand CSMA/CD. Take a minute to think about the full name *Carrier Sense Multiple Access with Collision Detection*. The term *Carrier Sense* refers to the fact that Ethernet NICs listen on the network and wait until they detect (or sense) that no other nodes are transmitting data over the signal (or carrier) on the communications channel before they begin to transmit. The term *Multiple Access* refers to the fact that several Ethernet nodes can be connected to a network and can monitor traffic, or access the media, simultaneously.

In CSMA/CD, when a node wants to transmit data it must first access the transmission media and determine whether the channel is free. If the channel is not free, it waits and checks again after a very brief amount of time. If the channel is free, the node transmits its data. Any node can transmit data after it determines that the channel is free. But what if two nodes simultaneously check the channel, determine that it's free, and begin to transmit? When this happens, their two transmissions interfere with each other; this is known as a **collision**.

The last part of CSMA/CD, the term *collision detection,* refers to the way nodes respond to a collision. In the event of a collision, the network performs a series of steps known as the collision detection routine. If a node's NIC determines that its data have been involved in a collision, it immediately stops transmitting. Next, in a process called **jamming**, the NIC issues a special 32-bit sequence that indicates to the rest of the network nodes that its previous transmission was faulty and that those data frames are invalid. After waiting, the NIC determines if the line is again available; if it is available, the NIC retransmits its data.

On heavily trafficked network segments, collisions are fairly common. It is not surprising that the more nodes there are transmitting data on a segment, the more collisions that will take place. (Although a collision rate greater than 5 percent of all traffic is unusual and may point to a problematic NIC or poor cabling on the network.) When an Ethernet segment grows to include a particularly large number of nodes, you may see performance suffer as a result of collisions. This "critical mass" number depends on the type and volume of data that the network regularly transmits. Collisions can corrupt data or truncate data frames, so it is important that the network detect and compensate for them. Figure 5-12 depicts the way CSMA/CD regulates data flow to avoid and, if necessary, detect collisions.

Net+ 1.4 3.7

On an Ethernet network, a **collision domain** is the portion of a network in which collisions occur if two nodes transmit data at the same time. When designing an Ethernet network, it's important to note that because repeaters simply regenerate any signal they receive, they repeat collisions just as they repeat data. Thus, connecting multiple parts of a network with

Net+ 1.4 3.7

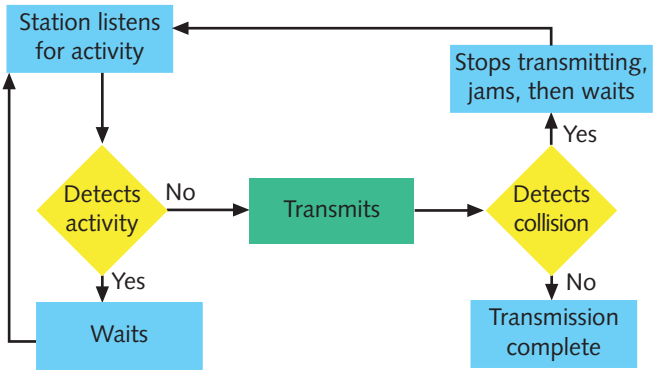


Figure 5-12 CSMA/CD process

repeaters or hubs results in a larger collision domain. Switches and routers, however, separate collision domains.

Collision domains differ from broadcast domains in that collision domains define a logically shared space for Layer 2 communications. Also, by default, switches do not separate broadcast domains. Figure 5-13 illustrates the difference between broadcast domains and collision domains.

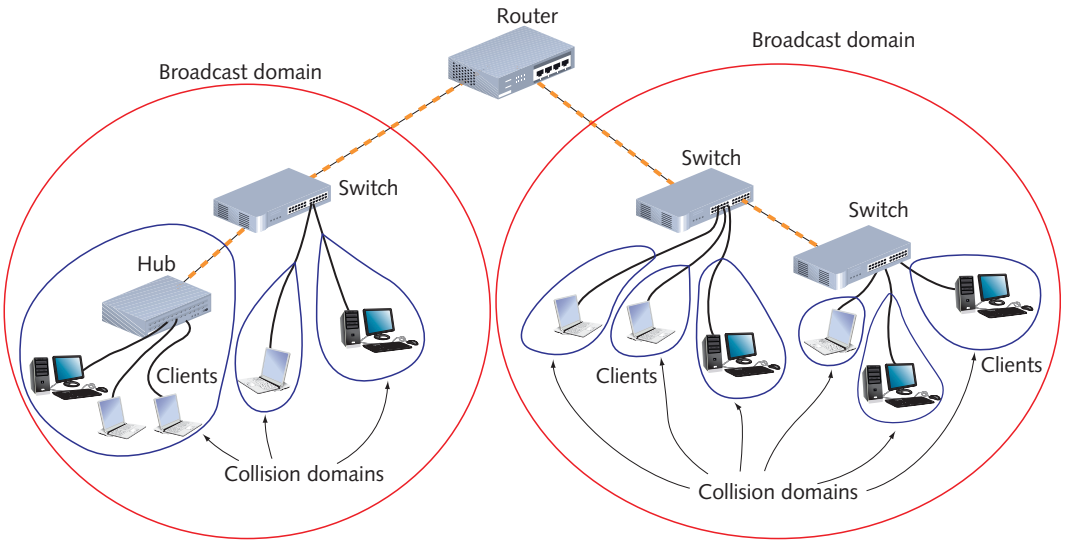


Figure 5-13 Broadcast domains and collision domains

Collision domains play a role in the Ethernet cabling distance limitations. For example, if two nodes on the same segment are positioned beyond the maximum recommended segment length, data propagation delays will be too long for CSMA/CD to be effective. A **data propagation**

Net+ 1.4 3.7

delay is the length of time data take to travel from one point on the segment to another point. When data take a long time, CSMA/CD's collision detection routine cannot identify collisions accurately. In other words, one node on the segment might begin its CSMA/CD routine and determine that the channel is free even though a second node has begun transmitting because the second node's data are taking so long to reach the first node.

At rates of 100 or 1000 Mbps, data travel so quickly that NICs can't always keep up with the collision detection and retransmission routines. For example, because of the speed employed on a 100-Mbps Ethernet network, the window of time for the NIC to both detect and compensate for the error is much less than that of a 10-Mbps network. To minimize undetected collisions, 100-Mbps networks can support only a maximum of three network segments connected with two repeating devices, such as hubs, whereas 10-Mbps buses can support a maximum of five network segments connected with four repeating devices. This shorter path reduces the highest potential propagation delay between nodes. Although it's important to know about limitations related to repeating devices, practically speaking, today's enterprise networks, which use switches and routers, will rarely be affected by these limitations.

Net+ Ethernet Standards for Copper Cable

3.7

Recall that IEEE Physical layer standards specify how signals are transmitted to the media. The following sections describe the standards for several types of Ethernet networks. Bear in mind that the technologies described by IEEE standards differ significantly in how they encode signals at the Physical layer. The specifics of encoding methods are beyond the scope of this book. However, encoding methods affect a standard's maximum throughput, segment length, and wiring requirements—and these are the details you need to understand for designing networks and installing cable.

In Ethernet technology, the most common theoretical maximum data transfer rates are 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps. Actual data transfer rates on a network will vary, just as you might average 22 miles per gallon (mpg) driving your car to work and back, even though the manufacturer rates the car's gas mileage at 28 mpg.

10Base-T

10Base-T was a popular Ethernet networking standard that replaced the older Thicknet and Thinnet technologies. In 10Base-T, the *10* represents its maximum throughput of *10 Mbps*, the *Base* indicates that it uses *baseband transmission*, and the *T* stands for *twisted pair,* the medium it uses. On a 10Base-T network, one pair of wires in the UTP cable is used for transmission, while a second pair of wires is used for reception. These two pairs of wires allow 10Base-T networks to provide full-duplex transmission. A 10Base-T network requires Cat 3 or better UTP.

Nodes on a 10Base-T Ethernet network connect to a central network device in a star fashion. As is typical of a star topology, a single network cable connects only two devices. This characteristic makes 10Base-T networks more fault tolerant than older networks that used the bus topology. Use of the star topology also makes 10Base-T networks easier to troubleshoot because you can isolate problems more readily when every device has a separate connection to the LAN.

Net+ 3.7

10Base-T follows the **5-4-3 rule** of networking. This rule says that, between two communicating nodes, the network cannot contain more than five network segments connected by four repeating devices, and no more than three of the segments may be populated (at least two must be unpopulated). The maximum distance that a 10Base-T segment can traverse is 100 meters. To go beyond that distance, Ethernet star segments must be connected by additional connectivity devices to form more complex topologies. This arrangement can connect a maximum of five sequential network segments, for an overall distance between communicating nodes of 500 meters. Figure 5-14 depicts a 10Base-T Ethernet network with maximum segment lengths.

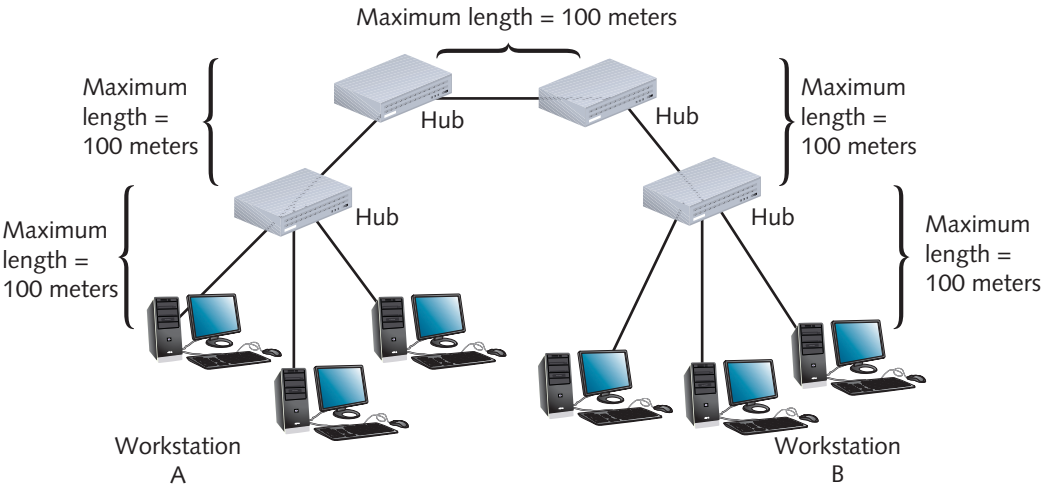


Figure 5-14 A 10Base-T network

100Base-T (Fast Ethernet) As networks expanded and handled heavier traffic, Ethernet's long-standing 10-Mbps limitation proved a bottleneck. The need for faster LANs that could use the same infrastructure as the popular 10Base-T technology was met by 100Base-T, also known as **Fast Ethernet**. 100Base-T, specified in the IEEE **802.3u** standard, enables LANs to run at a 100-Mbps data transfer rate, a tenfold increase from that provided by 10Base-T, without requiring a significant investment in new infrastructure. 100Base-T uses baseband transmission and the same star topology as 10Base-T. It also uses the same RJ-45 modular connectors. Depending on the type of 100Base-T technology used, it may require Cat 3, Cat 5, or better UTP.

As with 10Base-T, nodes on a 100Base-T network are configured in a star topology. However, unlike 10-Mbps Ethernet networks, 100Base-T networks do not follow the 5-4-3 rule. Because of their faster response requirements, to avoid data errors they require communicating nodes to be even closer. 100Base-T buses can support a maximum of three network segments connected with two repeating devices. Each segment length is limited to 100 meters. Thus, the overall maximum length between nodes is limited to 300 meters, as shown in Figure 5-15.

Net+ 3.7

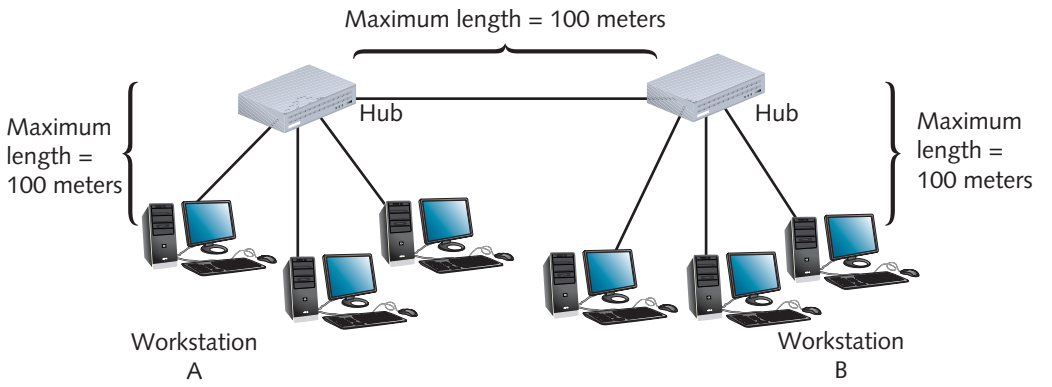


Figure 5-15 A 100Base-T network

The most common standard for achieving 100-Mbps throughput over twisted pair is **100Base-TX**. Compared with 10Base-T, it sends signals 10 times faster and condenses the time between digital pulses as well as the time a station must wait and listen for a signal. 100Base-TX requires Cat 5 or better unshielded twisted pair cabling. Within the cable, it uses the same two pairs of wire for transmitting and receiving data that 10Base-T uses. Therefore, like 10Base-T, 100Base-TX is also capable of full-duplex transmission. Full duplexing can potentially double the effective bandwidth of a 100Base-T network to 200 Mbps.

1000Base-T Because of increasing volumes of data and numbers of users who need to access this data quickly, even 100 Mbps has not met the throughput demands of many networks. Ethernet technologies designed to transmit data at 1 Gbps are collectively known as **Gigabit Ethernet**. **1000Base-T** is a standard for achieving throughputs 10 times faster than Fast Ethernet over copper cable, as described in IEEE's **802.3ab** standard. In *1000Base-TX, 1000* represents *1000 megabits per second (Mbps)*, or 1 gigabit per second (Gbps). *Base* indicates that it uses *baseband transmission*, and *T* indicates that it relies on *twisted pair wiring*.

1000Base-T achieves its higher throughput by using all four pairs of wires in a Cat 5 or better cable to both transmit and receive signals, whereas 100Base-T uses only two of the four pairs. 1000Base-T also uses a different data encoding scheme than 100Base-T networks use. However, the standards can be combined on the same network and you can purchase NICs that support 10 Mbps, 100 Mbps, and 1 Gbps via the same connector jack. Because of this compatibility, and the fact that 1000Base-T can use existing Cat 5 cabling, the 1-gigabit technology can be added gradually to an existing 100-Mbps network with minimal interruption of service. The maximum segment length on a 1000Base-T network is 100 meters. It allows for only one repeater. Therefore, the maximum distance between communicating nodes on a 1000Base-T network is 200 meters.

10GBase-T In 2006, IEEE released its **802.3an** standard for transmitting 10 Gbps over twisted pair, **10GBase-T**. This standard was a breakthrough in pushing the limits of the twisted pair medium. To achieve such dramatic data transmission rates, however, 10GBase-T segments require Cat 6, Cat 6a, or Cat 7 cabling. Still, as with other twisted pair Ethernet standards, the maximum segment length for 10GBase-T is 100 meters. The primary benefit of the 10GBase-T

Net+ 3.7

standard is that it makes very fast data transmission available at a much lower cost than using fiber-optic cable. 10GBase-T would probably not be used to connect two office locations across town because of its distance limitations. However, it could be used to connect network devices or to connect servers or workstations to a LAN. This type of implementation would easily allow the use of converged services, such as video and voice, at every desktop.

Yet long before IEEE developed a 10GBase-T standard for twisted pair cable, it had established standards for achieving high data rates over fiber-optic cable. In fact, fiber optic is the best medium for delivering high throughput. The following section details the IEEE standards that apply to these high-speed networks.

Ethernet Standards for Fiber-Optic Cable

100Base-FX The **100Base-FX** standard specifies a network capable of 100-Mbps throughput that uses baseband transmission and fiber-optic cabling. 100Base-FX requires multimode fiber containing at least two strands of fiber. In half-duplex mode, one strand is used for data transmission while the other strand is used for reception. In full-duplex implementations, both strands are used for both sending and receiving data. 100Base-FX has a maximum segment length of 412 meters if half-duplex transmission is used and 2000 meters if full-duplex is used. The standard allows for a maximum of one repeater to connect segments. The 100Base-FX standard uses a star topology, with its repeaters connected in a bus fashion.

100Base-FX, like 100Base-T, is also considered Fast Ethernet and is described in IEEE's 802.3u standard. Organizations switching, or migrating, from UTP to fiber media can combine 100Base-TX and 100Base-FX within one network. To do this, transceivers (for example, NICs) in computers and connectivity devices must have both RJ-45 and SC, ST, LC, or MT-RJ ports. Alternatively, a 100Base-TX to 100Base-FX media converter may be used at any point in the network to interconnect the different media and convert the signals of one standard to signals that work with the other standard.

1000Base-LX IEEE has specified three different types of 1000Base, or 1-gigabit, Ethernet technologies for use over fiber-optic cable in its **802.3z** standard.

Probably the most common 1-gigabit Ethernet standard in use today is **1000Base-LX**. The *1000* in 1000Base-LX stands for *1000-Mbps*—or 1-Gbps—throughput. *Base* stands for *baseband transmission,* and *LX* represents its reliance on *long* wavelengths of 1300 nanometers. (A nanometer equals 0.000000001 meters, or about the width of six carbon atoms in a row.) 1000Base-LX has a longer reach than any other 1-gigabit technology available today. It relies on either single-mode or multimode fiber. With multimode fiber (62.5 microns in diameter), the maximum segment length is 550 meters. When used with single-mode fiber (8 microns in diameter), 1000Base-LX can reach 5000 meters. 1000Base-LX networks can use one repeater between segments. Because of its potential length, 1000Base-LX is *an* excellent choice for long backbones—connecting buildings in a MAN, for example, or connecting an ISP with its telecommunications carrier.

1000Base-SX **1000Base-SX** is similar to 1000Base-LX in that it has a maximum throughput of 1 Gbps. However, it relies on only multimode fiber-optic cable as its medium. This makes it less expensive to install than 1000Base-LX. Another difference is that 1000Base-SX uses short wavelengths of 850 nanometers—thus, the *SX,* which stands for *short*. The maximum segment length for 1000Base-SX depends on two things: the diameter of the fiber and the modal bandwidth used to transmit signals. **Modal bandwidth** is a measure of the highest frequency of

Net+ 3.7

signal a multimode fiber can support over a specific distance and is measured in MHz-km. It is related to the distortion that occurs when multiple pulses of light, although issued at the same time, arrive at the end of a fiber at slightly different times. The higher the modal bandwidth, the longer a multimode fiber can carry a signal reliably.

When used with fibers whose diameters are 50 microns each, and with the highest possible modal bandwidth, the maximum segment length on a 1000Base-SX network is 550 meters. When used with fibers whose diameters are 62.5 microns each, and with the highest possible modal bandwidth, the maximum segment length is 275 meters. Only one repeater may be used between segments. Therefore, 1000Base-SX is best suited for shorter network runs than 1000Base-LX—for example, connecting a data center with a telecommunications closet in an office building.

10-Gigabit Fiber-Optic Standards

As you have learned, the throughput potential for fiber-optic cable is extraordinary, and engineers continue to push its limits. In 2002, IEEE published its **802.3ae** standard for fiber-optic Ethernet networks transmitting data at 10 Gbps. Several variations were described by the standard, but all share some characteristics in common. For example, all of the fiber-optic 10-gigabit options rely on a star topology and allow for only one repeater. (As you will learn in later chapters, however, switches, and not repeaters, are more commonly used with high-speed data links.) In addition, all 10-gigabit standards operate under full-duplex mode only. The 10-gigabit fiber-optic standards differ significantly in the wavelength of light each uses to issue signals and, as a result, their maximum allowable segment length differs also.

10GBase-SR and 10GBase-SW The 10-gigabit options with the shortest segment length are **10GBase-SR** and **10GBase-SW**. By now you can guess that the *10G* stands for the standard's maximum throughput of *10 gigabits per second* and *Base* stands for *baseband transmission. S* stands for *short reach*. The fact that one of the standards ends with *R* and the other ends with *W* reflects the type of Physical layer encoding each uses. Simply put, 10GBase-SR is designed to work with fiber connections on LANs, and 10GBase-SW is designed to work with WAN links that use a highly reliable fiber-optic ring technology called SONET. You'll learn more about SONET in Chapter 7.

10GBase-SR and 10GBase-SW rely on multimode fiber and transmit signals with wavelengths of 850 nanometers. As with the 1-gigabit standards, the maximum segment length on a 10GBase-SR or 10GBase-SW network depends on the diameter of the fibers used. It also depends on the modal bandwidth used. For example, if 50-micron fiber is used with the maximum possible modal bandwidth, the maximum segment length is 300 meters. If 62.5-micron fiber is used with the maximum possible modal bandwidth, a 10GBase-SR or 10GBase-SW segment can be *66* meters long. Either way, this 10-gigabit Ethernet technology is best suited for connections within a data center or building, as its distance is the most limited.

10GBase-LR and 10GBase-LW Another standard defined in IEEE 802.3ae is **10GBase-LR** and **10GBase-LW**, in which the *10G* stands for *10 gigabits per second, Base* stands for *baseband transmission,* and *L* stands for *long reach*. 10GBase-LR and 10GBase-LW networks carry signals with wavelengths of 1310 nanometers through single-mode fiber. Their maximum segment length is 10,000 meters. As is the case with the previously described 10-gigabit standard, in 10GBase-LW the *W* reflects its unique method of encoding that allows it to work over SONET WAN links. 10GBase-LR and 10GBase-LW technology is suited to WAN or MAN implementations.

Net+ 3.7

10GBase-ER and 10GBase-EW For the longest fiber-optic segments, network administrators choose **10GBase-ER** or **10GBase-EW**. In this standard, *E* stands for *extended reach*. 10GBase-ER and 10GBase-EW require single-mode fiber, through which they transmit signals with wavelengths of 1550 nanometers. These standards allow for segments up to 40,000 meters, or nearly 25 miles, long. The 10GBase-EW standard specifies encoding that makes it compatible with the SONET transmission format. Given their long-distance capabilities, 10GBase-ER and 10GBase-EW are best suited for use on WANs.

NSPs and ISPs use 10-gigabit Ethernet where traffic is aggregated and customers demand fast data transfer. As with any new technology, however, when 10-gigabit Ethernet becomes more economical, more organizations will adopt it for their WANs and LANs. Even faster Ethernet networks are on the way. IEEE has recently ratified standards for 40- and 100-gigabit Ethernet.

Net+ 3.7

Summary of Common Ethernet Standards

To obtain Network+ certification, you must be familiar with the different characteristics and limitations of each type of network discussed in this chapter. To put this information in context, Table 5-1 summarizes the characteristics and limitations for common Physical layer networking standards, including Ethernet networks that use twisted pair cable and fiber-optic cable. In addition to the varying specifications below, remember that all of these standards rely on a star or star-bus hybrid network topology.

Table 5-1 Common Ethernet standards

Standard	Maximum transmission speed (Mbps)	Maximum distance per segment (m)	Physical media
10Base-T	10	100	Cat 3 or better UTP
100Base-TX	100	100	Cat 5 or better UTP
1000Base-T	1000	100	Cat 5 or better UTP (Cat 5e is preferred)
10GBase-T	10,000	100	Cat 6 or Cat 7 (preferred)
100Base-FX	100	2000	MMF
1000Base-LX	1000	550 5000	MMF SMF
1000Base-SX	1000	Up to 550, depending on modal bandwidth and fiber core diameter	MMF
10GBase-SR and 10GBase-SW	10,000	Up to 300, depending on modal bandwidth and fiber core diameter	MMF
10GBase-LR and 10GBase-LW	10,000	10,000	SMF
10GBase-ER and 10GBase-EW	10,000	40,000	SMF

Net+ 3.7

In this chapter, you have learned about several varieties of Ethernet as well as their throughputs, distances, and media requirements. You should recognize that multiple Ethernet specifications may be found on a single LAN. For example, one switch might serve a number of clients with Fast Ethernet (100Base-T), while the routers that form the LAN's backbone might communicate over 1-gigabit Ethernet (1000Base-T). On a WAN, even more varieties might be used. For example, two NSPs might exchange a high volume of traffic using 10-gigabit Ethernet. That level of service, characterized by very high throughput and reliability, is commonly called **Carrier Ethernet**. Specifications for Carrier Ethernet include techniques for exceeding the normal 10-gigabit distance limitations shown in Table 5-1. Detailing these techniques is beyond the scope of this book, however.

Figure 5-16 provides a simplified example of how more than one type of Ethernet may be used on a network. Note that the connections between the company and its ISP and between the ISP and its NSP are identified, generically, as WAN links. After reading Chapter 7, you'll understand what type of links might fit there.

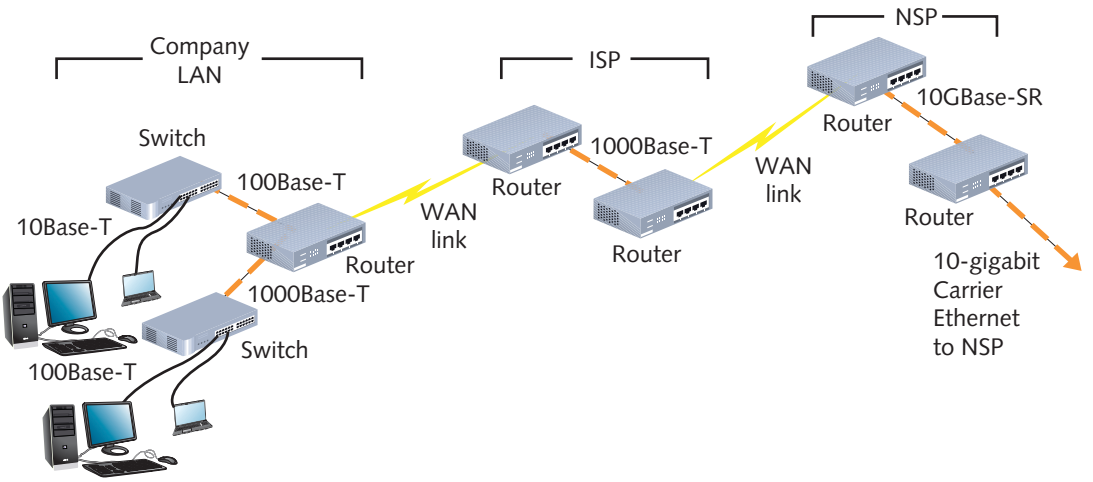


Figure 5-16 Multiple types of Ethernet on a WAN

Ethernet Frames

Chapter 2 introduced you to data frames, the packages that carry higher-layer data and control information that enable data to reach their destinations without errors and in the correct sequence. Ethernet networks may use any of four kinds of data frames: Ethernet_802.2 (Raw), Ethernet_802.3 (Novell proprietary), Ethernet II (DIX), and Ethernet_SNAP. This variety of Ethernet frame types came about as different organizations released and revised Ethernet standards during the 1980s, changing as LAN technology evolved. Each frame type differs slightly in the way it codes and decodes packets of data traveling from one device to another.

Physical layer standards, such as 100Base-T, have no effect on the type of framing that occurs in the Data Link layer. Thus, Ethernet frame types have no relation to the topology or cabling characteristics of the network. Framing also takes place independently of the higher-level layers. Theoretically, all frame types could carry any one of many higher-layer protocols. But as you'll learn in the following discussion, not all frame types are well suited to carrying all kinds of traffic.

Using and Configuring Frames

A node's Data Link layer services must be properly configured to expect the types of frames it might receive. You can use multiple frame types on a network, but a node configured to use only one frame type cannot communicate with another node that uses a different frame type. If a node receives an unfamiliar frame type, it will not be able to decode the data contained in the frame, nor will it be able to communicate with nodes configured to use that frame type. For this reason, it is important for LAN administrators to ensure that all devices use the same, correct frame type. These days, virtually all networks use the Ethernet II frame type. But in the 1990s, before this uniformity evolved, the use of different NOSs or legacy hardware often required managing devices to interpret multiple frame types.

Frame types can be specified through a device's NIC configuration software. To make matters easier, most NICs can automatically sense what types of frames are running on a network and adjust themselves to that specification. This feature is called autodetect, or autosense. Workstations, networked printers, and servers added to an existing network can all take advantage of autodetection. Even if your devices use the autodetect feature, you should nevertheless know what frame types are running on your network so that you can troubleshoot connectivity problems.

Frame Fields

All Ethernet frame types share many fields in common. For example, every Ethernet frame contains a 7-byte preamble and a 1-byte start-of-frame delimiter. The **preamble** signals to the receiving node that data are incoming and indicates when the data flow is about to begin. The **SFD (start-of-frame delimiter)** identifies where the data field begins. Preambles and SFDs are not included, however, when calculating a frame's total size.

Each Ethernet frame also contains a 14-byte header, which includes a destination address, a source address, and an additional field that varies in function and size, depending on the frame type. The destination address and source address fields are each 6 bytes long. The destination address identifies the recipient of the data frame, and the source address identifies the network node that originally sent the data. Recall that any network device can be identified by its physical address, also known as a hardware address or MAC (Media Access Control) address. The source address and destination address fields of an Ethernet frame use the MAC address to identify where data originated and where it should be delivered.

Also, all Ethernet frames contain a 4-byte FCS (frame check sequence) field. Recall that the function of the FCS field is to ensure that the data at the destination exactly match the data issued from the source using the CRC (cyclic redundancy check) algorithm. Together, the FCS and the header make up the 18-byte "frame" for the data. The data portion of an Ethernet frame may contain from 46 to 1500 bytes of information (and recall that this includes the Network layer datagram). If fewer than 46 bytes of data are supplied by the higher layers, the source node fills out the data portion with extra bytes until it totals 46 bytes. The extra bytes are known as **padding** and have no significance other than to fill out the frame. They do not affect the data being transmitted.

Adding the 18-byte framing portion plus the smallest possible data field of 46 bytes equals the minimum Ethernet frame size of 64 bytes. Adding the framing portion plus the largest possible data field of 1500 bytes equals the maximum Ethernet frame size of 1518 bytes. No matter what frame type is used, the size range of 64 to 1518 total bytes applies to all Ethernet frames.

Because of the overhead present in each frame and the time required to perform CSMA/CD, the use of larger frame sizes on a network generally results in faster throughput. To some extent, you cannot control your network's frame sizes. You can, however, help improve network performance by properly managing frames. For example, network administrators should strive to minimize the number of broadcast frames on their networks because broadcast frames tend to be very small and, therefore, inefficient. Also, running more than one frame type on the same network can result in inefficiencies because it requires devices to examine each incoming frame to determine its type. Given a choice, it's most efficient to support only one frame type on a network.

Ethernet II (DIX)

Ethernet II, used on virtually all modern networks, is an Ethernet frame type developed by DEC, Intel, and Xerox (abbreviated as DIX) before the IEEE began to standardize Ethernet. The Ethernet II frame type (or DIX, as it is sometimes called) is distinguished by other Ethernet frame types in that it contains a 2-byte type field. This type field identifies the Network layer protocol (such as IP or ARP) contained in the frame. For example, if a frame were carrying an IP datagram, its type field would contain 0x0800, the type code for IP.

Because of its support for multiple Network layer protocols and because it uses fewer bytes as overhead than other frame types, Ethernet II is the type most commonly used on contemporary Ethernet networks. Figure 5-17 depicts an Ethernet II frame.

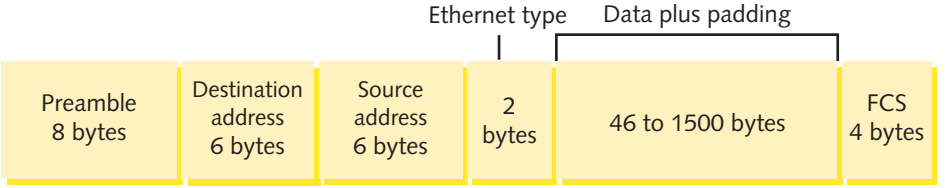


Figure 5-17 Ethernet II (DIX) frame

PoE (Power over Ethernet)

Net+ 2.1

In 2003, IEEE released its **802.3af** standard, which specifies a method for supplying electrical power over Ethernet connections, also known as **PoE** (**Power over Ethernet**). Although the standard is relatively new, the concept is not. In fact, your home telephone receives power from the telephone company over the lines that enter your residence. This power is necessary for dial tone and ringing. On an Ethernet network, carrying power over signaling connections can be useful for nodes that are far from traditional power receptacles or need a constant, reliable power source. For example, a wireless access point at an outdoor theater, a telephone used to receive digitized voice signals, an Internet gaming station in the center of a mall, or a critical router at the core of a network's backbone can all benefit from PoE.

The PoE standard specifies two types of devices: PSE (power sourcing equipment) and PDs (powered devices). **PSE** (**power sourcing equipment**) refers to the device that supplies the

Net+ 2.1

power; usually this device depends on backup power sources (in other words, not the electrical grid maintained by utilities). **PDs (powered devices)** are those that receive the power from the PSE. PoE requires Cat 5 or better copper cable. In the cable, electric current may run over an unused pair of wires or over the pair of wires used for data transmission in a 10Base-T, 100Base-TX, 1000Base-T, or 10GBase-T network. The standard allows for both approaches; however, on a single network, the choice of current-carrying pairs should be consistent between all PSE and PDs.

Not all connectivity devices are capable of issuing power. To use PoE, you must purchase a switch or router that supports it, like the switch shown in Figure 5-18. Also, not all end nodes are capable of receiving PoE. The IEEE standard has accounted for that possibility by requiring all PSE to first determine whether a node is PoE-capable before attempting to supply it with power. That means that PoE is compatible with current 802.3 installations.

Figure 5-18 PoE-capable switch

On networks that demand PoE but don't have PoE-capable equipment, you can add PoE adapters, like the ones shown in Figure 5-19. One type of adapter connects to a switch or router to allow it to supply power. The other adapter attaches to a client, such as an outdoor camera, to receive power over the Ethernet connection.

Figure 5-19 PoE adapters

Chapter Summary

- A physical topology is the basic physical layout of a network's media, nodes, and connectivity devices. Physical topologies are categorized into three fundamental shapes: bus, ring, and star.
- A bus topology consists of a single cable connecting all nodes on a network without intervening connectivity devices. At either end of a bus network, 50-ohm resistors (terminators) stop signals after they have reached their destination. Without terminators, signals on a bus network experience signal bounce and LAN performance suffers. Modern networks do not use a pure bus topology.
- In a ring topology, each node is connected to the two nearest nodes so that the entire network forms a circle. Data are transmitted in one direction around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring.
- In a star topology, every node on the network is connected through a central device, such as a switch or router. Any single cable on a star network connects only two devices, so a cabling problem will affect only two nodes. A source node transmits data to a connectivity device, which then retransmits the information to the rest of the network segment where the destination node can pick it up.
- Star topology networks are more fault tolerant than bus topology networks because a failure in one part of the network will not necessarily affect transmission on the entire network.
- Few LANs use the simple physical topologies in their pure form. More often, LANs employ a hybrid of more than one simple physical topology. The star-wired ring topology uses the physical layout of a star and the token-passing data transmission method. Data are sent around the star in a circular pattern. Token ring networks, as specified in IEEE 802.5, use this hybrid topology.
- In a star-wired bus topology, groups of workstations are star-connected to connectivity devices and then networked via a single bus. This design can cover longer distances than a simple star topology and easily interconnect or isolate different network segments. The star-wired bus topology commonly forms the basis for Ethernet and Fast Ethernet networks.
- Switches, routers, or hubs that service star-wired bus or star-wired ring topologies can be daisy-chained to form a more complex hybrid topology. However, daisy chains of repeating devices can only extend a network so far before data errors are apt to occur. In this case, maximum segment and network length limits must be carefully maintained.
- Network logical topologies describe how signals travel over a network. The two main types of logical topologies are bus and ring. Ethernet networks use a bus logical topology, and token ring networks use a ring logical topology.
- Network backbones may follow serial, distributed, collapsed, or parallel topologies. In a serial topology, two or more internetworking devices are connected to each other by a single cable in a daisy chain. This is the simplest type of backbone.

- A distributed backbone consists of a number of intermediate connectivity devices connected to one or more central devices in a hierarchy. This topology allows for easy network management and scalability.
- The collapsed backbone topology uses a router or switch as the single central connection point for multiple subnetworks. This is risky because an entire network could fail if the central device fails. Also, if the central connectivity device becomes overtaxed, performance on the entire network suffers.
- A parallel backbone is a variation of the collapsed backbone arrangement that consists of more than one connection from the central router or switch to each network segment and parallel connections between routers and switches, if more than one is present. Parallel backbones are the most expensive, but also the most fault-tolerant, type of backbone.
- Switching manages the filtering and forwarding of packets between nodes on a network. Every network relies on one or more types of switching, including circuit switching, packet switching, or MPLS (multiprotocol label switching).
- Packet switching separates data into packets before they are transported. Packets can travel any path on the network to their destination and attempt to find the fastest circuit available at any instant. They need not follow the same path, nor must they arrive at their destination in the same sequence as when they left their source.
- MPLS (multiprotocol label switching) enables multiple types of Layer 3 protocols to travel over any one of several connection-oriented Layer 2 protocols. In MPLS, the first router that receives a packet adds one or more labels to the Layer 3 datagram in a shim. Then the network's Layer 2 protocol header is added. MPLS offers potentially faster transmission with better quality of service guarantees.
- Ethernet employs a network access method called CSMA/CD (Carrier Sense Multiple Access with Collision Detection). All Ethernet networks, independent of their speed or frame type, use CSMA/CD.
- On heavily trafficked Ethernet segments, collisions are common. The more nodes that are transmitting data on a network segment, the more collisions will take place. When an Ethernet segment grows to a particular number of nodes, performance may suffer as a result of collisions.
- A collision domain is the portion of a network where collisions occur if two nodes transmit data at the same time. Repeaters, which simply regenerate signals they receive, repeat collisions, too. Thus, connecting multiple segments with repeaters results in a larger collision domain. Switches and routers, however, separate collision domains.
- Using switches enables network managers to separate a network segment into smaller logical segments, each independent of the other and supporting its own traffic. The use of switched Ethernet increases the effective bandwidth of a network segment because at any given time fewer workstations vie for the access to a shared channel.
- 10Base-T is a Physical layer specification for an Ethernet network that is capable of 10-Mbps throughput and uses baseband transmission and twisted pair media. It has a maximum segment length of 100 meters. It follows the 5-4-3 rule, which allows up to five segments between two communicating nodes, permits up to four repeating devices, and allows up to three of the segments to be populated.

- 100Base-T (also called Fast Ethernet) is a Physical layer specification for an Ethernet network that is capable of 100-Mbps throughput and uses baseband transmission and twisted pair media. It has a maximum segment length of 100 meters and allows up to three segments connected by two repeating devices.
- 1000Base-T (also called Gigabit Ethernet) is a Physical layer specification for an Ethernet network that is capable of 1000-Mbps (1-Gbps) throughput and uses baseband transmission and twisted pair media. It has a maximum segment length of 100 meters and allows only one repeating device between segments.
- 10GBase-T is Physical layer specification for transmitting 10 Gbps over twisted pair cable. It relies on Cat 6 or better wiring and has a maximum segment length of 100 meters.
- 100Base-FX is a Physical layer specification for a network that can achieve 100-Mbps throughput using baseband transmission running on multimode fiber. Its maximum segment length is 2000 meters.
- 1-Gbps Physical layer standards for fiber-optic networks include 1000Base-SX and 1000Base-LX. Because 1000Base-LX reaches farther and uses a longer wavelength, it is the more popular of the two. 1000Base-LX can use either single-mode or multimode fiber-optic cable; its segments can be up to 550 or 5000 meters, respectively. 1000Base-SX uses only multimode fiber and can span up to 550 meters, depending on modal bandwidth and fiber core diameter.
- 10-Gbps Physical layer standards include 10GBase-SR and 10GBase-SW (short reach), which rely on multimode fiber-optic cable and can span a maximum of 300 meters; 10GBase-LR and 10GBase-LW (long reach), which rely on single-mode fiber and can span a maximum of 10,000 meters; and 10GBaseER and 10GBase-EW (extended reach), which also use single-mode fiber and can span up to 40,000 meters. Standards marked with a *W* mean they are specially encoded to operate over SONET links.
- Networks may use one (or a combination) of four kinds of Ethernet data frames. Each frame type differs slightly in the way it codes and decodes packets of data from one device to another. Most modern networks rely on Ethernet II (DIX) frames.

Key Terms

10Base-T A Physical layer standard for networks that specifies baseband transmission, twisted pair media, and 10-Mbps throughput. 10Base-T networks have a maximum segment length of 100 meters and rely on a star topology.

10GBase-ER A Physical layer standard for achieving 10-Gbps data transmission over single-mode, fiber-optic cable. In 10GBase-ER, the *ER* stands for *extended reach*. This standard specifies a star topology and segment lengths up to 40,000 meters.

10GBase-EW A variation of the 10GBase-ER standard that is specially encoded to operate over SONET links.

10GBase-LR A Physical layer standard for achieving 10-Gbps data transmission over single-mode, fiber-optic cable using wavelengths of 1310 nanometers. In 10GBase-LR, the *LR* stands for *long reach*. This standard specifies a star topology and segment lengths up to 10,000 meters.

10GBase-LW A variation of the 10GBase-LR standard that is specially encoded to operate over SONET links.

10GBase-SR A Physical layer standard for achieving 10-Gbps data transmission over multimode fiber using wavelengths of 850 nanometers. The maximum segment length for 10GBase-SR can reach up to 300 meters, depending on the fiber core diameter and modal bandwidth used.

10GBase-SW A variation of the 10GBase-SR standard that is specially encoded to operate over SONET links.

10GBase-T A Physical layer standard for achieving 10-Gbps data transmission over twisted pair cable. Described in its 2006 standard 802.3an, IEEE specifies Cat 6 or Cat 7 cable as the appropriate medium for 10GBase-T. The maximum segment length for 10GBase-T is 100 meters.

100Base-FX A Physical layer standard for networks that specifies baseband transmission, multimode fiber cabling, and 100-Mbps throughput. 100Base-FX networks have a maximum segment length of 2000 meters. 100Base-FX may also be called Fast Ethernet.

100Base-T A Physical layer standard for networks that specifies baseband transmission, twisted pair cabling, and 100-Mbps throughput. 100Base-T networks have a maximum segment length of 100 meters and use the star topology. 100Base-T is also known as Fast Ethernet.

100Base-TX A type of 100Base-T network that uses two wire pairs in a twisted pair cable, but uses faster signaling to achieve 100-Mbps throughput. It is capable of full-duplex transmission and requires Cat 5 or better twisted pair media.

1000Base-LX A Physical layer standard for networks that specifies 1-Gbps transmission over fiber-optic cable using baseband transmission. 1000Base-LX can run on either single-mode or multimode fiber. The *LX* represents its reliance on long wavelengths of 1300 nanometers. 1000Base-LX can extend to 5000-meter segment lengths using single-mode, fiber-optic cable. 1000Base-LX networks can use one repeater between segments.

1000Base-SX A Physical layer standard for networks that specifies 1-Gbps transmission over fiber-optic cable using baseband transmission. 1000Base-SX runs on multimode fiber. Its maximum segment length is 550 meters. The *SX* represents its reliance on short wavelengths of 850 nanometers. 1000Base-SX can use one repeater.

1000Base-T A Physical layer standard for achieving 1 Gbps over UTP. 1000Base-T achieves its higher throughput by using all four pairs of wires in a Cat 5 or better twisted pair cable to both transmit and receive signals. 1000Base-T also uses a different data encoding scheme than that used by other UTP Physical layer specifications.

5-4-3 rule A guideline for 10-Mbps Ethernet networks stating that between two communicating nodes, the network cannot contain more than five network segments connected by four repeating devices, and no more than three of the segments may be populated.

802.3ab The IEEE standard that describes 1000Base-T, a 1-gigabit Ethernet technology that runs over four pairs of Cat 5 or better cable.

802.3ae The IEEE standard that describes 10-gigabit Ethernet technologies, including 10GBase-SR, 10GBase-SW, 10GBase-LR, 10GBase-LW, 10GBase-ER, and 10GBase-EW.

802.3af The IEEE standard that specifies a way of supplying electrical Power over Ethernet (PoE). 802.3af requires Cat 5 or better UTP or STP cabling and uses power sourcing equipment to supply current over a wire pair to powered devices. PoE is compatible with existing 10Base-T, 100Base-TX, 1000Base-T, and 10GBase-T implementations.

802.3an The IEEE standard that describes 10GBase-T, a 10-Gbps Ethernet technology that runs on Cat 6 or Cat 7 twisted pair cable.

802.3u The IEEE standard that describes Fast Ethernet technologies, including 100Base-TX.

802.3z The IEEE standard that describes 1000Base (or 1-gigabit) Ethernet technologies, including 1000Base-LX and 1000Base-SX.

access method A network's method of controlling how nodes access the communications channel. For example, CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is the access method specified in the IEEE 802.3 (Ethernet) standard.

active topology A topology in which each workstation participates in transmitting data over the network. A ring topology is considered an active topology.

broadcast domain Logically grouped network nodes that can communicate directly via broadcast transmissions. By default, switches and repeating devices such as hubs extend broadcast domains. Routers and other Layer 3 devices separate broadcast domains.

bus The single cable connecting all devices in a bus topology.

bus topology A topology in which a single cable connects all nodes on a network without intervening connectivity devices.

Carrier Ethernet A level of Ethernet service that is characterized by very high throughput and reliability and is used between carriers, such as NSPs.

Carrier Sense Multiple Access with Collision Detection *See* CSMA/CD.

circuit switching A type of switching in which a connection is established between two network nodes before they begin transmitting data. Bandwidth is dedicated to this connection and remains available until users terminate the communication between the two nodes.

collapsed backbone A type of backbone that uses a router or switch as the single central connection point for multiple subnetworks.

collision In Ethernet networks, the interference of one node's data transmission with the data transmission of another node sharing the same segment.

collision domain The portion of an Ethernet network in which collisions could occur if two nodes transmit data at the same time. Switches and routers separate collision domains.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) A network access method specified for use by IEEE 802.3 (Ethernet) networks. In CSMA/CD, each node waits its turn before transmitting data to avoid interfering with other nodes' transmissions. If a node's NIC determines that its data have been involved in a collision, it immediately stops transmitting. Next, in a process called jamming, the NIC issues a special 32-bit sequence that indicates to the rest of the network nodes that its previous transmission was faulty and that those data frames are invalid. After waiting, the NIC determines if the line is again available; if it is available, the NIC retransmits its data.

daisy chain A group of connectivity devices linked together in a serial fashion.

data propagation delay The length of time data take to travel from one point on the segment to another point. On Ethernet networks, CSMA/CD's collision detection routine cannot operate accurately if the data propagation delay is too long.

distributed backbone A type of backbone in which a number of intermediate connectivity devices are connected to one or more central connectivity devices, such switches or routers, in a hierarchy.

enterprise An entire organization, including local and remote offices, a mixture of computer systems, and a number of departments. Enterprise-wide computing takes into account the breadth and diversity of a large organization's computer needs.

Ethernet II The original Ethernet frame type developed by Digital Equipment Corporation, Intel, and Xerox, before the IEEE began to standardize Ethernet. Ethernet II is distinguished from other Ethernet frame types in that it contains a 2-byte type field to identify the upper-layer protocol contained in the frame. It supports TCP/IP and other higher-layer protocols.

Fast Ethernet A type of Ethernet network that is capable of 100-Mbps throughput. 100Base-T and 100Base-FX are both examples of Fast Ethernet.

fault tolerance The capability for a component or system to continue functioning despite damage or malfunction.

Gigabit Ethernet A type of Ethernet network that is capable of 1000-Mbps, or 1-Gbps, throughput.

hybrid topology A physical topology that combines characteristics of more than one simple physical topology.

jamming A part of CSMA/CD in which, upon detecting a collision, a station issues a special 32-bit sequence to indicate to all nodes on an Ethernet segment that its previously transmitted frame has suffered a collision and should be considered faulty.

logical topology A characteristic of network transmission that reflects the way in which data are transmitted between nodes. A network's logical topology may differ from its physical topology. The most common logical topologies are bus and ring.

MPLS (multiprotocol label switching) A type of switching that enables any one of several Layer 2 protocols to carry multiple types of Layer 3 protocols. One of its benefits is the ability to use packet-switched technologies over traditionally circuit-switched networks. MPLS can also create end-to-end paths that act like circuit-switched connections.

modal bandwidth A measure of the highest frequency of signal a multimode fiber-optic cable can support over a specific distance. Modal bandwidth is measured in MHz-km.

multiprotocol label switching *See* MPLS.

packet switching A type of switching in which data are broken into packets before being transported. In packet switching, packets can travel any path on the network to their destination because each packet contains a destination address and sequencing information.

padding The bytes added to the data (or information) portion of an Ethernet frame to ensure this field is at least 46 bytes in size. Padding has no effect on the data carried by the frame.

parallel backbone A type of backbone that consists of more than one connection from the central router or switch to each network segment.

passive topology A network topology in which each node passively listens for, then accepts, data directed to it. A bus topology is considered a passive topology.

PD (powered device) On a network using Power over Ethernet, a node that receives power from power sourcing equipment.

physical topology The physical layout of the media, nodes, and devices on a network. A physical topology does not specify device types, connectivity methods, or addressing schemes. Physical topologies are categorized into three fundamental shapes: bus, ring, and star. These shapes can be mixed to create hybrid topologies.

PoE (Power over Ethernet) A method of delivering current to devices using Ethernet connection cables.

Power over Ethernet *See* PoE.

power sourcing equipment *See* PSE.

powered device *See* PD.

preamble The field in an Ethernet frame that signals to the receiving node that data are incoming and indicates when the data flow is about to begin.

PSE (power sourcing equipment) On a network using Power over Ethernet, the device that supplies power to end nodes.

QoS (quality of service) The result of specifications for guaranteeing data delivery within a certain period of time after their transmission.

quality of service *See* QoS.

ring topology A network layout in which each node is connected to the two nearest nodes so that the entire network forms a circle. Data are transmitted in one direction around the ring. Each workstation accepts and responds to packets addressed to it, then forwards the other packets to the next workstation in the ring.

serial backbone A type of backbone that consists of two or more internetworking devices connected to each other by a single cable in a daisy chain.

SFD (start-of-frame delimiter) A 1-byte field that indicates where the data field begins in an Ethernet frame.

signal bounce A phenomenon, caused by improper termination on a bus-topology network, in which signals travel endlessly between the two ends of the network, preventing new signals from getting through.

star topology A physical topology in which every node on the network is connected through a central connectivity device. Any single physical wire on a star network connects only two devices, so a cabling problem will affect only two nodes. Nodes transmit data to the device, which then retransmits the data to the rest of the network segment where the destination node can pick it up.

star-wired bus topology A hybrid topology in which groups of workstations are connected in a star fashion to connectivity devices that are networked via a single bus.

star-wired ring topology A hybrid topology that uses the physical layout of a star and the token-passing data transmission method.

start-of-frame delimiter *See* SFD.

switching A component of a network's logical topology that manages how packets are filtered and forwarded between nodes on the network.

terminator A resistor that is attached to each end of a bus-topology network and that causes the signal to stop rather than reflect back toward its source.

Review Questions

1. Which of the following topologies is susceptible to signal bounce?
   a. Partial-mesh
   b. Bus
   c. Ring
   d. Full-mesh
2. What type of topology is required for use with a 100Base-TX network?
   a. Bus
   b. Star
   c. Mesh
   d. Ring
3. Your school's network has outgrown its designated telco rooms, so you decide to house a few routers in an old janitor's closet temporarily. However, because the closet has no power outlets, you will have to supply the routers power over the network. If you're lucky, your LAN already uses which of the following Ethernet standards that will allow you to do that?
   a. 100Base-FX
   b. 1000Base-T
   c. 1000Base-LX
   d. 10GBase-LR
4. What is the minimum cabling standard required for 10GBase-T Ethernet?
   a. MMF
   b. Cat 3
   c. Cat 5
   d. Cat 6
5. Why is packet switching more efficient than circuit switching?
   a. In packet switching, packets are synchronized according to a timing mechanism in the switch.
   b. In packet switching, two communicating nodes establish a channel first, then begin transmitting, thus ensuring a reliable connection and eliminating the need to retransmit.
   c. In packet switching, small pieces of data are sent to an intermediate node and reassembled before being transmitted, en masse, to the destination node.
   d. In packet switching, packets can take the quickest route between nodes and arrive independently of when other packets in their data stream arrive.

6. You are part of a team of engineers who work for an ISP that connects large data centers, telephone companies, and their customers throughout California and Oregon. Management has decided that the company can make large profits by promising the utmost QoS to certain high-profile customers. Which of the following switching methods will best guarantee the promised QoS?
   a. Circuit switching
   b. MPLS
   c. Packet switching
   d. Message switching
7. What happens in CSMA/CD when a node detects that its data have suffered a collision?
   a. It immediately retransmits the data.
   b. It signals to the other nodes that it is about to retransmit the data, and then does so.
   c. It waits for a random period of time before checking the network for activity, and then retransmits the data.
   d. It signals to the network that its data were damaged in a collision, waits a brief period of time before checking the network for activity, and then retransmits the data.
8. Which of the following backbone types is the most fault tolerant?
   a. Parallel backbone
   b. Collapsed backbone
   c. Distributed backbone
   d. Serial backbone
9. What is the purpose of padding in an Ethernet frame?
   a. Ensuring that the frame and data arrive without error
   b. Ensuring that the frame arrives in sequence
   c. Ensuring that the data portion of the frame totals at least 46 bytes
   d. Indicating the length of the frame
10. You are designing a 100Base-T network to connect groups of workstations in two different offices in your building. The offices are approximately 250 meters apart. If you only use repeating devices to connect the workstation groups, how many hubs will you need?
    a. One
    b. Two
    c. Three
    d. Four

11. On a 10Base-T network, which of the following best describes how the wires of a UTP cable are used to transmit and receive information?
    a. One wire pair handles data transmission, while another wire pair handles data reception.
    b. One wire in one pair handles data transmission, while the other wire in the same pair handles data reception.
    c. Three wires of two wire pairs handle both data transmission and reception, while the fourth wire acts as a ground.
    d. All four wires of two wire pairs handle both data transmission and reception.
12. What technique is used to achieve 1-Gbps throughput over a Cat 5 cable?
    a. All four wire pairs are used for both transmission and reception.
    b. The cable is encased in a special conduit to prevent signal degradation due to noise.
    c. Signals are issued as pulses of light, rather than pulses of electric current.
    d. Data are encapsulated by a unique type of frame that allows rapid data compression.
13. Which of the following Ethernet standards is specially encoded for transmission over WANs using SONET technology?
    a. 100Base-T
    b. 10GBase-ER
    c. 100Base-FX
    d. 10GBase-SW
14. Which two of the following might cause excessive data collisions on an Ethernet network?
    a. A server on the network contains a faulty NIC.
    b. A router on the network is mistakenly forwarding packets to the wrong segment.
    c. The overall network length exceeds IEEE 802.3 standards for that network type.
    d. A switch on the network has established multiple circuits for a single path between two nodes.
    e. The network attempts to use two incompatible frame types.
15. In which of the following examples do the workstations necessarily share a collision domain?
    a. Two computers connected to the same hub
    b. Two computers connected to the same switch
    c. Two computers connected to the same router
    d. Two computers connected to the same access server
16. What are the minimum and maximum sizes for an Ethernet frame?
    a. 46 and 64 bytes
    b. 46 and 128 bytes
    c. 64 and 1518 bytes
    d. 64 and 1600 bytes

17. Which of the following network technologies does not use circuit switching?
    a. ATM
    b. Ethernet
    c. T1
    d. ISDN
18. Which of the following is the type of 10-gigabit Ethernet that can carry signals the farthest, nearly 25 miles?
    a. 10GBase-T
    b. 10GBase-ER
    c. 10GBase-LR
    d. 10GBase-SR
19. The maximum segment length for a 1000Base-FX network depends on which two of the following?
    a. Voltage
    b. Wavelength
    c. Frame type
    d. Priority labeling
    e. Fiber core diameter
20. The data services company you work for has decided to become an ISP and supply high-capacity Internet connections from its data center. Currently, the data center relies on a 100Base-FX backbone, but your boss demands that the backbone be upgraded to 10GBase-LR. What kind of infrastructure changes would this require?
    a. None, because fiber-optic cabling and connectivity devices, including multiplexers, are already in place.
    b. The fiber-optic cabling will need to be upgraded, but the same connectivity devices and multiplexers can be used.
    c. The fiber-optic cabling can be reused, but the connectivity devices and multiplexers must be replaced.
    d. The fiber-optic cabling, connectivity devices, and multiplexers must be replaced.

Hands-On Projects

Project 5-1

In this project, you will use a software program called Wireshark to view frames and datagrams traveling through a computer's NIC. Network managers may use Wireshark to aid in troubleshooting. For example, if a network suddenly acts sluggish, viewing its traffic could uncover where excessive frames are being generated. The Wireshark program is available at no cost from the Wireshark Web site, *www.wireshark.org*. It works with recent versions of the Windows operating system, as well as Mac OS X, and most

versions of Linux and UNIX. This project guides you through installing Wireshark on a Windows 7 workstation. However, beginning with Step 19, the Windows 7 steps are very similar to steps required by Wireshark running on any operating system.

Your Windows 7 workstation should have at least 100 MB free on its hard disk, TCP/IP installed and properly configured, modern Web browser software, and an Internet connection. Furthermore, you should be logged on to the workstation as a user with administrator-equivalent privileges. Note that directions for obtaining and installing Wireshark were current as of this writing; however, some steps might have changed since then.

1. To obtain the Wireshark software, open your browser and go to the following Web site: **www.wireshark.org**. The Wireshark home page appears.
2. In the menu bar at the top of the page, click **Download Wireshark**. The Wireshark Download page appears.
3. Under the "Get Wireshark – Stable Release" heading, click **Windows Installer (64 bit)** if your computer has a 64-bit operating system, or click **Windows Installer (32 bit)** if your computer has a 32-bit operating system.
4. A dialog box appears asking you to confirm that you want to save the file. Click **Save File**.
5. A dialog box opens, prompting you to enter a name for the file. Choose a folder and filename, and then click **Save**.
6. Navigate to the folder where you saved the file and double-click the filename to run the executable.
7. A User Account Control window opens asking you whether you want to allow the program to make changes to your computer. Click **Yes** to continue.
8. The Wireshark Setup Wizard window opens. Click **Next** to continue.
9. The Wireshark Setup: License Agreement window opens. If you agree with the license agreement's terms, click **I Agree** to continue.
10. The Wireshark Setup: Choose Components window opens, prompting you to select from a group of optional components. Click **Next** to accept the default selections.
11. The Wireshark Setup: Select Additional Tasks window opens. Click **Next** to continue.
12. The Wireshark Setup: Choose Install Location window opens. Click **Next** to install the program in your default program file folder.
13. The Wireshark Setup: Install WinPcap? window opens. Because this program is required for capturing data with Wireshark on Windows-based computers, click **Install**.
14. After the Wireshark program and its components begin to install, the WinPcap Setup window opens. Click **Next** twice to continue, and then click **I Agree**. The Setup program will install the Wireshark files on your computer.
15. When prompted, click **Install**, and then click **Finish**.
16. The Installation Complete window opens. Click **Next** to continue.
17. Click **Finish** to complete the Wireshark installation.
18. To start the Wireshark application, click the **Start** button, then select **Wireshark**. The Wireshark Network Analyzer window opens.

19. The first step in examining frames on a network is to enable the capture feature. To do so, click **Capture**, then **Interfaces** from the main menu. The Wireshark: Capture Interfaces window opens. It should list your NIC(s) and the IP addresses associated with each. For example, if you have a wireless network card and a Gigabit Ethernet card, both will appear.
20. Click the **Options** button that corresponds to the NIC for which you want to capture data. The Wireshark: Capture Options window opens.
21. Notice that the "Capture packets in promiscuous mode" option is checked by default. This means that anything passing through your NIC will be captured. In other words, no type of traffic will be filtered out.
22. For now, leave all the options at their defaults and click **Start** to begin capturing traffic.
23. Before you can examine the frames and datagrams on a network, you must first generate traffic. To generate traffic, open your Web browser and connect to a Web page, and then connect to a different Web page. Watch Wireshark's capture window to see how many frames it has captured. Notice how many of these frames rely on TCP, UDP, or ARP in the Transport layer.
24. Next you'll generate a different type of traffic. To open a Command Prompt window, click the **Start** button, select **All Programs**, select **Accessories**, and then select **Command Prompt**.
25. At the command prompt, type **ping www.cengage.com** and then press **Enter**. The `ping` command should generate replies from that Web site.
26. Now that you've generated different types of traffic, return to the Wireshark window, click **Capture** on the main menu and then click **Stop**.
27. The Wireshark window displays a list of all traffic captured on the top third of the screen and more detailed information about the selected frame in the middle and bottom thirds of the screen, as shown in Figure 5-20. Notice that data are differentiated by

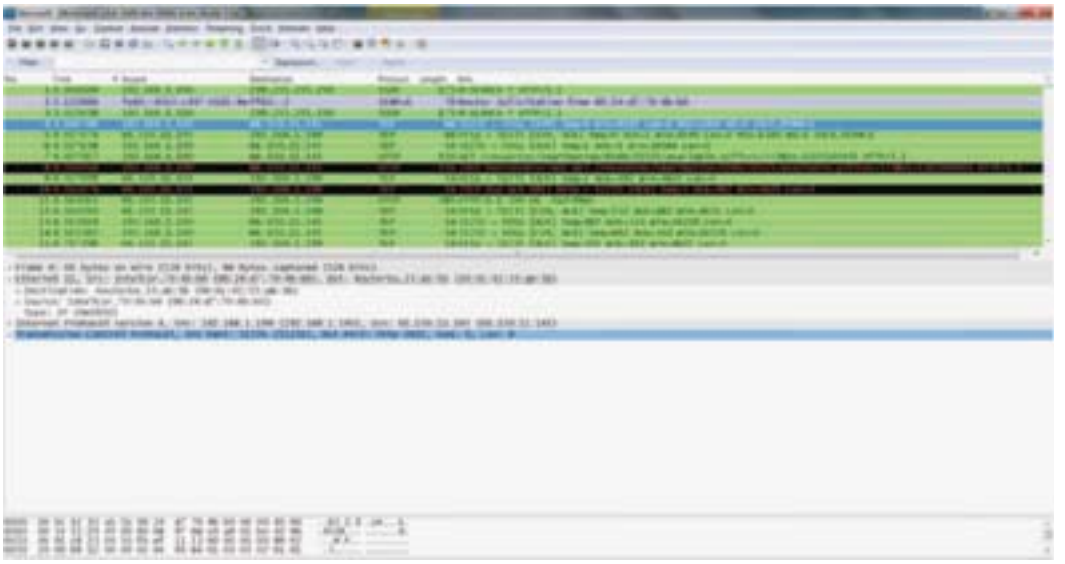


Figure 5-20 Wireshark capture window

color according to protocol type and appear in the order in which they were transmitted or received during the capture period. Click the **Protocol** column heading to sort the frames according to their Transport or Application layer protocols.

28. How much of the traffic you generated used TCP? How much used HTTP?
29. One by one, click on lines that represent different frames to view their details. According to the details provided in the middle third of the page, what Ethernet frame type do these frames follow? What Network layer protocol do the frames support?
30. From the list of frames in the top third of the screen, select a frame that uses the HTTP protocol.
31. In the middle third of the screen, notice the plus sign next to every line of information. (In the Linux version of Wireshark, a right-facing arrow takes the place of the plus sign.) Click the small **plus sign** next to the Ethernet II line. Assuming you're connecting to the Internet via a router, the details will reveal the MAC addresses of your router and workstation.
32. Click the small **minus sign** (or the downward-facing arrow, if you're running Wireshark on Linux) next to the line to hide the Ethernet frame details.
33. Click the small **plus sign** next to the Internet Protocol line. Details about the datagram will reveal the IP address of the packet's source and destination. What version of IP is the datagram using? What was the outcome of the datagram's header checksum?
34. Click the small **minus sign** to hide the Internet Protocol datagram details.
35. Locate the bar separating the bottom third of the screen from the middle third, and then drag this bar upward, so you can better view the packet's data contents.
36. In the middle third of the screen, click the small **plus sign** next to the Hypertext Transfer Protocol line. In the bottom third of the screen, the HTTP data are highlighted, with the total number of bytes displayed below. How much of this frame's bulk consisted of HTTP data? Compare this number with the total size of the frame, listed in the top line in the middle third of the screen that begins with *Frame X*, where X is the frame number.
37. Subtract the number of HTTP data bytes from the total frame size. How many bytes of overhead were used to send this frame?
38. Wireshark offers many more options for reviewing network data, including the ability to filter out certain types of frames either before or after capturing. Continue to Project 5-2 to experiment further with this program.

Project 5-2

In the previous Hands-On Project, you learned how to view traffic in Wireshark. In this project (which assumes you have already completed Hands-On Project 5-1), you'll analyze additional characteristics of your network's traffic. As with Project 5-1, this project is written to work with a Windows 7 workstation; however, the steps are very similar for versions of Wireshark running on other operating systems. Again, your workstation should have TCP/IP properly installed and configured and be connected to the Internet. You should also be logged on as a user with administrator-equivalent privileges.

1. Begin with an existing capture session—that is, keep the session you generated from Project 5-1 or create a new group of data by generating and capturing about two minutes of traffic over the Web and via the command-line interface.
2. Wireshark provides several methods for analyzing a group of data. To begin, click **Statistics** in the main menu and then click **Summary**. The Wireshark: Summary window opens.
3. How many packets did you capture? What was their average size?
4. Close the Wireshark: Summary window.
5. Click **Statistics** in the main menu and then click **Protocol Hierarchy**. The Wireshark: Protocol Hierarchy Statistics window opens, revealing, for example, the percentage of your traffic that used Ethernet frames, the percentage that used IP and TCP, and so on. Did any of your traffic use a type of frame that was not Ethernet? What percentage of your traffic relied on IP? How many and what percentage of your packets, if any, used IPv6?
6. Close the Wireshark: Protocol Hierarchy Statistics window.
7. Click **Statistics** on the main menu and then click **Endpoints**. The Endpoints window opens, with the Ethernet tab selected by default. Wireshark defines endpoints as a logical end of any transmission, such as a node, and identifies each endpoint with an IP address or MAC address.
8. In the Ethernet tab, nodes are listed in order of the highest volume of traffic generated and received, cumulatively. What node sits at the top of this list, and what kind of equipment does it represent?
9. Click the **IPv4** tab. A list of endpoints appears. As with the endpoints listed in the Ethernet tab, the one responsible for the greatest number of bytes transmitted and received (cumulatively) is listed first. Which IP address is at the top of this list? To what node does it belong?
10. Click the **IPv6** tab. How many endpoints and transmissions were using this protocol?
11. Close the **Endpoints** window.
12. When network engineers are diagnosing a problem with a particular connection, it often helps to filter out unrelated traffic and follow the data through the troubled connection. There are several ways to do this in Wireshark. As an example, right-click on a line that represents a frame carrying HTTP data, then choose **Follow TCP Stream**.
13. The Follow TCP Stream window opens, displaying frames belonging to each endpoint highlighted with different colors. Meanwhile, the main capture display has changed to include only traffic involved in the same data exchange. From what you can tell, what happened during this exchange?
14. Click **Close** to leave the Follow TCP Stream window.
15. Continue exploring the features of Wireshark if you like, or click **File** on the main menu and then click **Quit** to close the program.
16. You will be asked whether you want to save your capture file before quitting. Click **Quit without Saving**.

Net+ 1.4 3.7

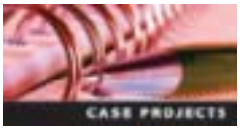
Project 5-3

In this project, you will sketch an Ethernet LAN that uses more than one version of the 802.3 standard and includes some legacy equipment. You'll also label each broadcast domain, collision domain, and Ethernet type. For this project, you need only a pen or pencil and paper.

1. On the left side of your paper, draw a hub and label it "Hub A."
2. Draw lines connecting Hub A to three older workstations. Label the three lines "10Base-T."
3. Draw a switch and label it "Switch A." Then draw a line connecting Hub A to Switch A. Label this line "10Base-T."
4. In the middle of your sheet of paper, draw a router. Label this router "Router A."
5. Draw a line connecting the switch to Router A. Label this line "100Base-T."
6. Draw several clients—three tower desktops, two printers, three laptops, and a server—and lines connecting each client to the switch you drew in Step 2. Label each of these lines "100Base-T."
7. Draw a second router just to the right of Router A and label it "Router B."
8. Draw a line connecting the two routers and label this line "1000Base-T."
9. On the right side of the page, draw a mirror image of the portion of the LAN on the left side of the page so the right side includes "Switch B" and its nine clients and "Hub B" and its three clients, with the same type of Ethernet connections.
10. On your drawing, circle and label each separate collision domain. How many are there?
11. On your drawing, circle and label each separate broadcast domain. How many are there?
12. Based on what you know about Ethernet and CSMA/CD, and assuming all workstations and servers on the network are generating approximately equal amounts of traffic while printers generate less traffic, what portions of the network you've drawn will likely experience the highest number of collisions? Which will experience the least?
13. What type of backbone does this LAN use?
14. If you were designing a new LAN, what pieces of the network you drew would you change or replace? What equipment and wiring upgrades would your recommendations require?
15. Redraw the LAN to include the recommendations you made in Step 14.

Net+ 2.6

Case Projects



Case Project 5-1

You have been asked to assess the LAN at a popular, but cash-strapped children's museum. Visitors have complained that the video kiosk exhibits, which obtain their content from a server on the local network, are slow to respond and sometimes stall out. Meanwhile, museum staff members often wait several minutes to access large files or retrieve Web pages. The museum's IT manager confesses that he hasn't had the time or money to redesign the LAN, which was installed in 1999. It uses small, outdated switches and routers and only

Net+ 2.6

delivers 10-Mbps throughput to each client. The IT manager feels confident that he can convince management to support a network upgrade because it's critical to continuing operations. He says the most important parts of the network are the 10 workstations that supply multimedia content to the exhibits, though it's also important for the seven office employees to perform their jobs efficiently. He adds that the museum's connection to its ISP was just upgraded, so it's only the LAN that needs to be changed. What kind of LAN will you design for this company? Describe its backbone, its physical and logical topologies, what access method it will use, and what media and throughputs you recommend.

Net+ 2.6

Case Project 5-2

Fortunately, the children's museum director recently received a $20,000 government grant for infrastructure upgrades, and half of this could be spent on networking equipment. She asks you and the IT manager to list the components necessary for your recommended network upgrade. She also stipulates that equipment should be high quality and obtained only from reputable suppliers, such as a device's manufacturer. What is the total cost of brand-new connectivity devices, NICs, and cabling (if necessary) for the solution you suggested? Can you purchase everything with half the grant? If not, what elements are you willing to sacrifice? How else could you save money?

Net+ 2.6

Case Project 5-3

The museum director is delighted with your LAN upgrade proposal, and she approves the equipment purchase right away. In fact, she asks if you can implement the solution over the week long holiday break, which is only two weeks from now. Her ulterior motive, she confesses, is that a patron will be visiting town during that time, and she would like to give him a private tour of the museum. If he's impressed, he might make a significant donation to the museum. But if the displays don't work well, the potential income could be lost. You tell her you'll do your best and begin researching how long it will take to order and receive the equipment you've specified. What kind of lead times do the vendors commit to? Based on what you've learned and your experience with network installation, do you promise the museum director you'll upgrade the network in two weeks? If not, how do you justify your reluctance to meet her demands? If so, what is your plan in case the equipment doesn't arrive on time or in case something goes wrong with the work?