Chapter 4

Network Topologies and Architectures

Networks come in a few standard forms, and each form is a complete system of compatible hardware, protocols, transmission media, and topologies. A *topology* is a map of the network. It is a plan for how the cabling will interconnect the nodes and how the nodes will function in relation to one another. Several factors shape the various network topologies, and one of the most important is the choice of an *access method*. An access method is a set of rules for sharing the transmission medium. This chapter describes two of the most important categories of access methods: *contention* and *token passing*. You learn about *CSMA/CD* and *CSMA/CA*, two contention-based access methods, and about some of the fundamental topology archetypes. This chapter then looks at Ethernet and Token Ring networks. Ethernet and Token Ring are network architectures designed around the contention and token-passing access methods, respectively.

Chapter 4 targets the following objective in the Planning section of the Networking Essentials exam:

Test Objectives

- Select the appropriate topology for various Token Ring and Ethernet networks

Test Yourself

Stop! Before reading this chapter, test yourself to determine how much study time you will need to devote to this section.

1. In the __________ access method, a computer signals a warning when it is about to transmit data.

   A. CSMA/CD

   B. CSMA/CA

   C. CSMA/BD

   D. Token passing

2. The __________ topology is most often associated with contention-based access methods.

   A. star

   B. mesh

   C. ring

   D. bus

3. Which two of the following are true of 10BASE-T networks?

   A. 10BASE-T uses UTP cable.

   B. 10BASE-T uses STP cable.

   C. 10BASE-T is a physical star but a logical bus.

   D. 10BASE-T is a physical bus but a logical star.

4. IBM specifications call for a maximum cabling distance of __________ for Type 3 cable in Token Ring.

   A. 45 meters

   B. 75 meters

   C. 185 meters

   D. 300 meters

Access Methods

An *access method* is a set of rules governing how the network nodes share the transmission medium. The rules for sharing among computers are similar to the rules for sharing among humans in that they both boil down to a pair of fundamental philosophies: 1) *first come, first serve* and 2) *take turns*. These philosophies are the principles defining the two most important types of media access methods:

- **Contention.** In its purest form, *contention* means that the computers are contending for use of the transmission medium. Any computer in the network can transmit at any time (first come, first serve).
- **Token passing.** The computers take turns using the transmission medium.

As you can imagine, contention-based access methods can give rise to situations in which two or more of the network nodes try to broadcast at the same time and the signals collide. Specifications for contention-based access methods include procedures for how to avoid collisions and what to do if a collision occurs. This section will introduce the CSMA/CD and CSMA/CA access methods.

On most contention-based networks, the nodes are basically equal. No node has a higher priority than other nodes. A new access method called *demand priority*, however, resolves contention and collisions and in so doing accounts for data type priorities. This section also describes demand priority access.

Contention

In pure contention-based access control, any computer can transmit at any time. This system breaks down when two computers attempt to transmit at the same time, in which case a collision occurs (see fig. 4.1). Eventually, when a network gets busy enough, most attempts to transmit result in collisions and little effective communication can take place.

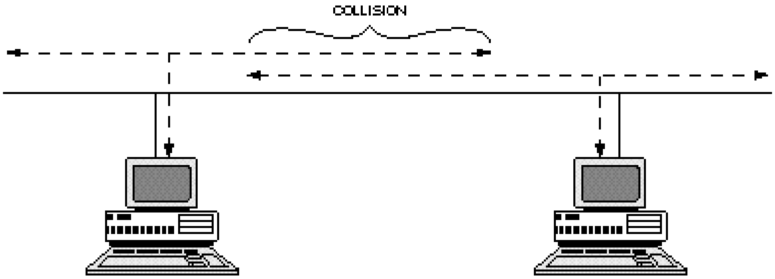


Figure 4.1

A collision on a contention-based network.

Mechanisms, therefore, usually are put into place to minimize the effects of collisions. One mechanism is *carrier sensing*, whereby each computer listens to the network before attempting to transmit. If the network is busy, the computer refrains from transmitting until the network quiets down. This simple "listen before talking" strategy can significantly reduce collisions.

Another mechanism is *carrier detection*. With this strategy, computers continue to listen to the network as they transmit. If a computer detects another signal that interferes with the signal it's sending, it stops transmitting. Both computers then wait a random amount of time and attempt to retransmit. Unless the network is extremely busy, carrier detection along with carrier sensing can manage a large volume of transmissions.

Carrier detection and carrier sensing used together form the protocol used in all types of Ethernet: *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*. CSMA/CD limits the size of the network to 2,500 meters. At longer distances, the broadcast-sensing mechanisms don't work—a node at one end can't sense when a node at the other end starts to broadcast.

Apple's LocalTalk network uses the protocol *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)*. Collision avoidance uses additional techniques to further reduce the likelihood of collisions. In CSMA/CA, each computer signals a warning that says it is *about* to transmit data, and then the other computers wait for the broadcast. CSMA/CA adds an extra layer of order, thereby reducing collisions, but the warning broadcasts increase network traffic, and the task of constantly listening for warnings increases system load.

Although it sounds as if contention methods are unworkable due to the damage caused by collisions, contention (in particular CSMA/CD in the form of Ethernet) is the most popular media access control method on LANs. (In fact, no currently employed LAN standards utilize pure contention access control without adding some mechanism to reduce the incidence of collisions.)

Contention is a simple protocol that can operate with simple network software and hardware. Unless traffic levels exceed about 30 percent of bandwidth, contention works quite well. Contention-based networks offer good performance at low cost.

Because collisions occur at unpredictable intervals, no computer is guaranteed the capability to transmit at any given time. Contention-based networks are called *probabilistic* because a computer's chance of being permitted to transmit cannot be predicted. Collisions increase in frequency as more computers use the network. When too many computers use the network, collisions dominate network traffic, and few frames are transmitted without error.

All computers on a contention-based network are equal. Consequently, it's impossible to assign certain computers higher priorities and, therefore, greater access to the network.

note

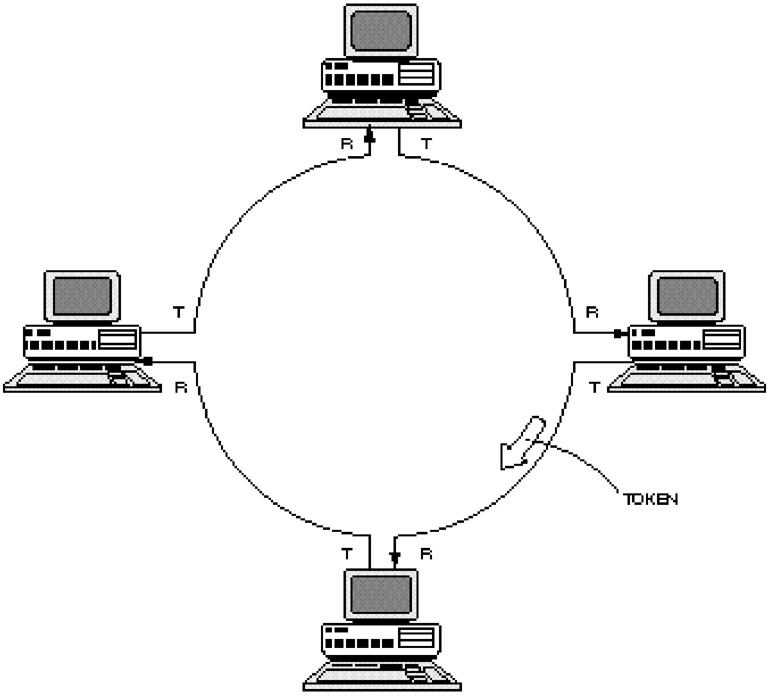
Contention access control is well-suited for networks that experience bursts in traffic—for instance, from large intermittent file transfers—and have relatively few computers.

Token Passing

Token passing utilizes a frame called a *token*, which circulates around the network. A computer that needs to transmit must wait until it receives the token, at which time the computer is permitted to transmit. When the computer is finished transmitting, it passes the token frame to the next station on the network. Figure 4.2 shows how token passing is implemented on a Token Ring network. Token Ring networks are discussed in greater detail later in this chapter in the section titled "Token Ring."

Figure 4.2

Token passing.



Several network standards employ token passing access control:

- **Token Ring.** The most common token-passing standard, embodied in IEEE standard 802.5
- **IEEE standard 802.4.** Implemented infrequently; defines a bus network that also employs token passing
- **FDDI.** A 100 Mbps fiber-optic network standard that uses token passing and rings in much the same manner as 802.5 Token Ring

Token-passing methods can use station priorities and other methods to prevent any one station from monopolizing the network. Because each computer has a chance to transmit each time the token travels around the network, each station is guaranteed a chance to transmit at some minimum time interval.

note

Token passing is more appropriate than contention under the following conditions:

- **When the network is carrying time-critical data.** Because token passing results in more predictable delivery, token passing is called *deterministic*.
- **When the network experiences heavy utilization.** Performance typically falls off more gracefully with a token-passing network than with a contention-based network. Token-passing networks cannot become gridlocked due to excessive numbers of collisions.
- **When some stations should have higher priority than others.** Some token-passing schemes support priority assignments.

Comparing Contention and Token Passing

As an access control mechanism, token passing appears to be clearly superior to contention. You find, however, that Ethernet, by far the dominant LAN standard, has achieved its prominence while firmly wedded to contention access control.

Token passing requires a variety of complex control mechanisms for it to work well. The necessary hardware is considerably more expensive than the hardware required to implement the much simpler contention mechanisms. The higher cost of token passing networks is difficult to justify unless the special features are required.

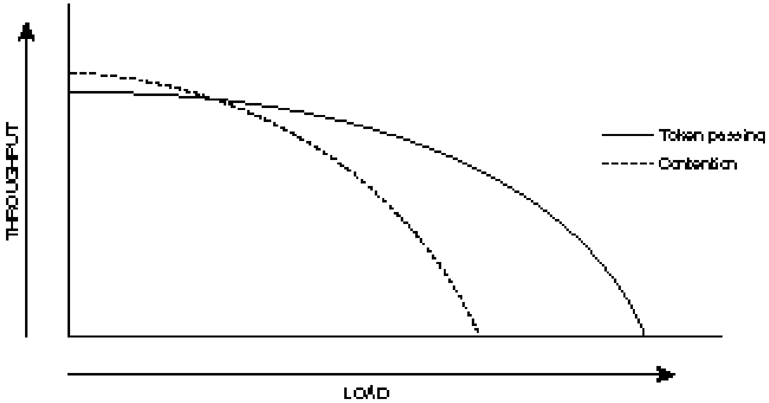
Because token-passing networks are designed for high reliability, building network diagnostic and troubleshooting capabilities into the network hardware is common. These capabilities increase the cost of token-passing networks. Organizations must decide whether this additional reliability is worth the extra cost.

Conversely, although token-passing networks perform better than contention-based networks when traffic levels are high, contention networks exhibit superior performance under lighter loading conditions. Passing the token around (and other maintenance operations) eats into the available bandwidth. As a result, a 10 Mbps Ethernet and a 16 Mbps Token Ring perform comparably well under light loading conditions, but the Ethernet costs considerably less.

Figure 4.3 illustrates the performance characteristics you can expect from each access control method. (This figure implies that token-passing throughput eventually reaches a zero level, which cannot happen, regardless of the loading conditions. Although a station's access to the network might be limited, access is guaranteed with each circuit of the token.)

Figure 4.3

Comparison of contention and token passing.



Demand Priority

Demand priority is an access method used with the new 100 Mbps 100VG-AnyLAN standard. Although demand priority is officially considered a contention-based access method, demand priority is considerably different from the basic CSMA/CD Ethernet. In demand priority, network nodes are connected to hubs, and those hubs are connected to other hubs. Contention, therefore, occurs at the hub. (100VG-AnyLAN cables can actually send and receive data at the same time.) Demand priority provides a mechanism for prioritizing data types. If contention occurs, data with a higher priority takes precedence.

note

100VG-AnyLAN cabling uses four twisted-pairs in a scheme called *quartet signaling*.

Physical and Logical Topologies

A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. Two basic categories form the basis for all discussions of topologies:

- **Physical topology.** Describes the actual layout of the network transmission media
- **Logical topology.** Describes the logical pathway a signal follows as it passes among the network nodes

Another way to think about this distinction is that a physical topology defines the way the network *looks*, and a logical topology defines the way the *data passes* among the nodes. At a glance this distinction may seem nit-picky, but as you learn in this chapter, the physical and logical topologies for a network can be very different. A network with a star physical topology, for example, may actually have a bus or a ring logical topology.

In common usage, the word "topology" applies to a complete network definition, which includes the physical and logical topologies and also specifications for elements such as the transmission medium. The term *topology* as used in Microsoft's test objectives for the Networking Essentials exam applies not to the physical and logical topology archetypes described in this section but to the complete network specifications (such as 10BASE-T or 10BASE5) described in the "Ethernet" and "Token Ring" sections of this chapter.

Physical and logical topologies can take several forms. The most common—and the most important for understanding the Ethernet and Token Ring topologies described later in this chapter—are the following:

- Bus topologies
- Ring topologies
- Star topologies

The following sections discuss each of these important topology types.

Bus Topologies

A *bus physical topology* is one in which all devices connect to a common, shared cable (sometimes called the *backbone*). A bus physical topology is shown in figure 4.4.

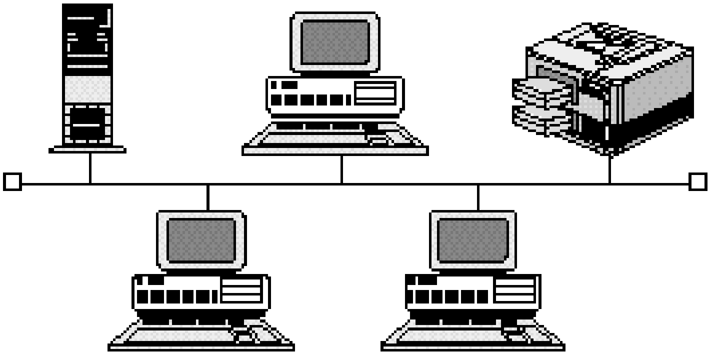


Figure 4.4

A bus physical topology.

If you think the bus topology seems ideally suited for the networks that use contention-based access methods such as CSMA/CD, you are correct. Ethernet, the most common contention-based network architecture, typically uses bus as a physical topology. 10BASE-T Ethernet networks (described later in this chapter) use bus as a logical topology but are configured in a star physical topology.

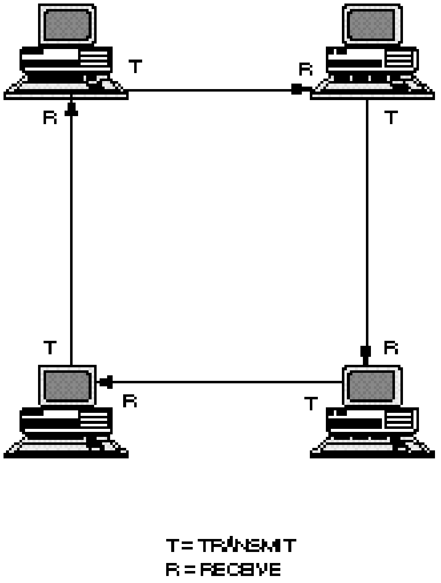
Most bus networks broadcast signals in both directions on the backbone cable, enabling all devices to directly receive the signal. Some buses, however, are unidirectional: signals travel in only one direction and can reach only downstream devices. Recall from Chapter 3, "Transmission Media," that a special connector called a *terminator* must be placed at the end of the backbone cable to prevent signals from reflecting back on the cable and causing interference. In the case of a *unidirectional bus*, the cable must be terminated in such a way that signals can reflect back on the cable and reach other devices without causing disruption.

Ring Topologies

Ring topologies are wired in a circle. Each node is connected to its neighbors on either side, and data passes around the ring in one direction only (see fig. 4.5). Each device incorporates a receiver and a transmitter and serves as a repeater that passes the signal on to the next device in the ring. Because the signal is regenerated at each device, signal degeneration is low.

Figure 4.5

A ring topology. (The ring topology is almost always implemented as a logical topology. See fig. 4.6.)

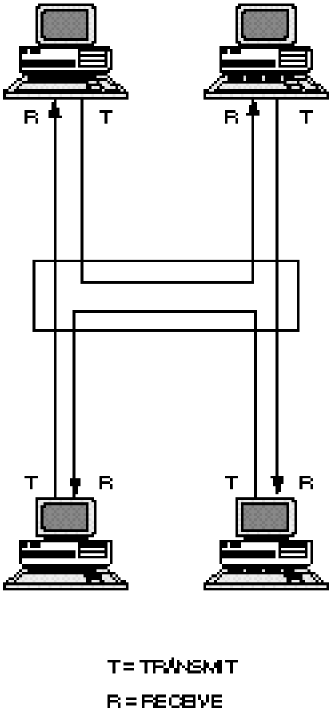


Ring topologies are ideally suited for token-passing access methods. The token passes around the ring, and only the node that holds the token can transmit data.

Ring physical topologies are quite rare. The ring topology is almost always implemented as a logical topology. Token Ring, for example—the most widespread token-passing network—always arranges the nodes in a physical star (with all nodes connecting to a central hub) but passes data in a logical ring (see fig. 4.6).

Figure 4.6

A logical ring configured in a physical star.



You get a closer look at Token Ring later in this chapter in the section titled "Token Ring."

Star Topologies

Star topologies require that all devices connect to a central hub (see fig. 4.7). The hub receives signals from other network devices and routes the signals to the proper destinations. Star hubs can be interconnected to form *tree* or *hierarchical* network topologies.

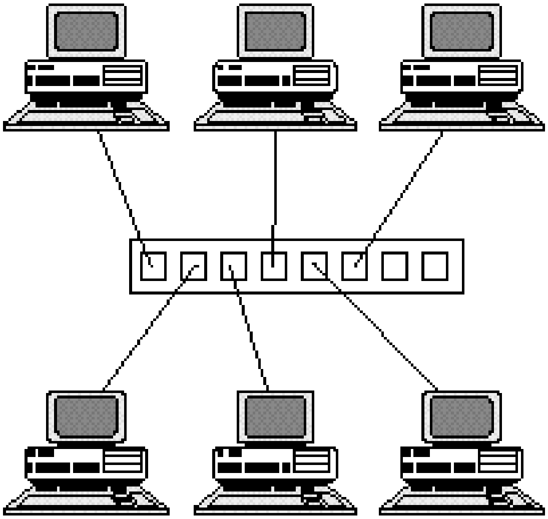


Figure 4.7

A star topology.

As mentioned earlier, a star physical topology is often used to implement a bus or ring logical topology (refer to fig. 4.6).

note

A *star physical topology* means that the nodes are all connected to a central hub. The path the data takes among the nodes and through that hub (the logical topology) depends on the design of the hub, the design of the cabling, and the hardware and software configuration of the nodes.

Ethernet

Ethernet is a very popular local area network architecture based on the CSMA/CD access method. The original Ethernet specification was the basis for the IEEE 802.3 specifications (see Chapter 2, "Networking Standards"). In present usage, the term Ethernet refers to original Ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of Ethernet networks are commonly referred to as *Ethernet topologies*. Typically, Ethernet networks use a bus physical topology, although, as mentioned earlier, some varieties of Ethernet such as 10BASE-T use a star physical topology and a bus logical topology. (Microsoft uses the term "star bus" topology to describe 10BASE-T.)

Ethernet networks, depending on the specification, operate at 10 or 100 Mbps using baseband transmission. Each of the IEEE 802.3 specifications (see Chapter 2) prescribes its own cable types.

The next sections in this chapter examine the following Ethernet topologies:

- 10BASE2
- 10BASE5
- 10BASE-T
- 10BASE-FL
- 100VG-AnyLAN
- 100BASE-X

Note that the name of each Ethernet topology begins with a number (10 or 100). That number specifies the transmission speed for the network. For instance, 10BASE5 is designed to operate at 10 Mbps, and 100BASE-X operates at 100 Mbps.

Ethernet networks transmit data in small units called *frames*. The size of an Ethernet frame can be anywhere between 64 and 1,518 bytes. Eighteen bytes of the total size are taken up by frame overhead, such as the source and destination addresses, protocol information, and error-checking information.

A typical Ethernet II frame has the following sections:

- **Preamble.** A field that Signifies the beginning of the frame
- **Addresses.** Source and destination addresses for the frame
- **Type.** A field that designates the Network layer protocol
- **Data.** The data being transmitted
- **CRC.** Cyclical Redundancy Check for error checking

note

> The origins of Ethernet are commemorated in the initials DIX, a 15-pin connector used to interface Ethernet components. The acronym "DIX" derives from the combination of leading letters of the founding Ethernet vendors: Digital, Intel, and Xerox.

The term Ethernet commonly refers to original Ethernet (which has been updated to Ethernet II) as well as the IEEE 802.3 standards. Ethernet and the 802.3 standards differ in ways significant enough to make standards incompatible in terms of packet formats, however. At the Physical layer, Ethernet and 802.3 are generally compatible in terms of cables, connectors, and electronic devices.

Ethernet generally is used on light-to-medium traffic networks and performs best when a network's data traffic transmits in short bursts. Ethernet is the most commonly used network standard. It has become especially popular in many university and government installations.

One advantage of the linear bus topology used by most Ethernet networks (this doesn't apply to star bus networks such as 10BASE-T) is that the required cabling is minimized because each node doesn't require a separate cable run to the hub. One disadvantage is that a break in the cable or a streaming network adapter card can bring down the entire network. Streaming is more frequently referred to as a *broadcast storm.* A broadcast storm occurs when a network card fails and the transmitter floods the cable with traffic, like a faucet stuck open. At this point, the network becomes unusable. See Chapter 13, "Troubleshooting," for more on broadcast storms.

Ethernet Cabling

You can use a variety of cables to implement Ethernet networks. Many of these cable types—Thinnet, Thicknet, UTP—are described in Chapter 3. Ethernet networks traditionally have used coaxial cables of several different types. Fiber-optic cables now are frequently employed to extend the geographic range of Ethernet networks.

The contemporary interest in using twisted-pair wiring has resulted in a scheme for cabling that uses unshielded twisted-pair (UTP): the 10BASE-T cabling standard, which uses UTP in a star physical topology. (10BASE-T is discussed later in this chapter.)

Ethernet remains closely associated with coaxial cable. Two types of coaxial cable still used in small and large environments are Thinnet (10BASE2) and Thicknet (10BASE5). Thinnet and Thicknet Ethernet networks have different limitations that are based on the Thinnet and Thicknet cable specifications. The best way to remember the requirements is to use the 5-4-3 rule of thumb for each cable type.

The 5-4-3 rule (see fig. 4.8) states that the following can appear between any two nodes in the Ethernet network:

- Up to 5 segments in a series
- Up to 4 concentrators or repeaters
- 3 segments of (coaxial only) cable that contain nodes

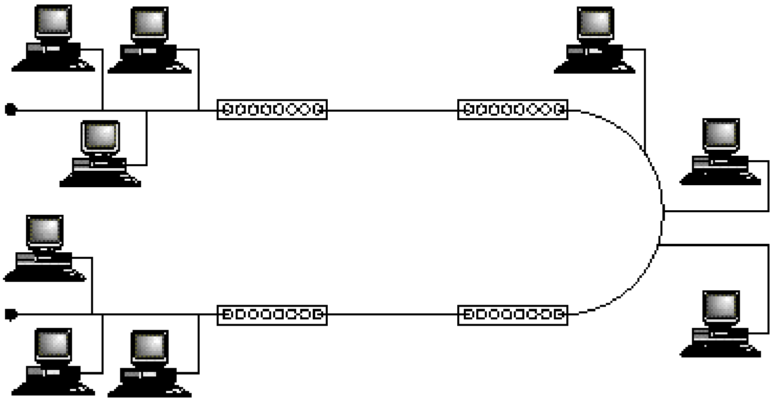


Figure 4.8

The 5-4-3 rule: 5 segments on a LAN, 4 repeaters, and 3 segments that contain nodes.

10BASE2

The 10BASE2 cabling topology (Thinnet) generally uses the onboard transceiver of the network interface card to translate the signals to and from the rest of the network. Thinnet cabling, described in Chapter 3, uses BNC T-connectors that directly attach to the network adapter. Each end of the cable should have a terminator, and you must use a grounded terminator on one end.

The main advantage of using 10BASE2 in your network is cost. When any given cable segment on the network doesn't have to be run further than 185 meters (607 feet), 10BASE2 is often the cheapest network cabling option.

10BASE2 is also relatively simple to connect. Each network node connects directly to the network cable by using a T-connector attached to the network adapter. For a successful installation, you must adhere to several rules in 10BASE2 Ethernet environments, including the following:

- The minimum cable distance between clients must be 0.5 meters (1.5 feet).
- *Pig tails*, also known as *drop cables*, from T-connectors shouldn't be used to connect to the BNC connector on the network adapter. The T-connector must be connected directly to the network adapter.
- You may not exceed the maximum network segment limitation of 185 meters (607 feet).
- The entire network cabling scheme cannot exceed 925 meters (3,035 feet).
- The maximum number of nodes per network segment is 30 (this includes clients and repeaters).
- A 50-ohm terminator must be used on each end of the bus with only one of the terminators having either a grounding strap or a grounding wire that attaches it to the screw holding an electrical outlet cover in place.
- You may not have more than five segments on a network. These segments may be connected with a maximum of four repeaters, and only three of the five segments may have network nodes.

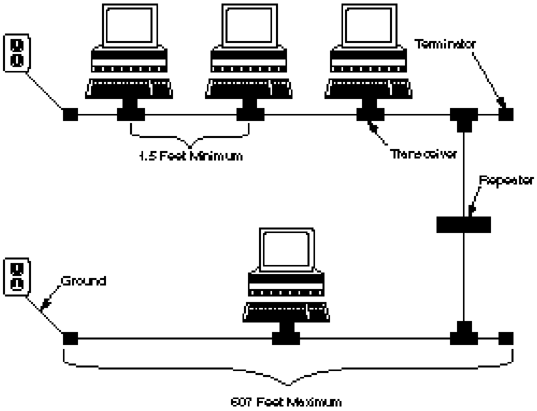
note

You should be able to translate cable segment lengths from feet to meters or from meters to feet. A meter is equivalent to 39.37 inches or 3.28 feet.

Figure 4.9 shows two network segments using 10BASE2 cabling. For more on 10BASE2's Thinnet cabling, see Chapter 3.

Figure 4.9

Two segments using 10BASE2 cabling.



10BASE5

The 10BASE5 cabling topology (Thicknet) uses an external transceiver to attach to the network adapter card (see fig. 4.10). The external transceiver clamps to the Thicknet cable (as described in Chapter 3). An Attachment Universal Interface (AUI) cable runs from the transceiver to a DIX connector on the back of the network adapter card. As with Thinnet, each network segment must be terminated at both ends, with one end using a grounded terminator. The components of a Thicknet network are shown in figure 4.11.

Figure 4.10

Two segments using 10BASE5 cabling.

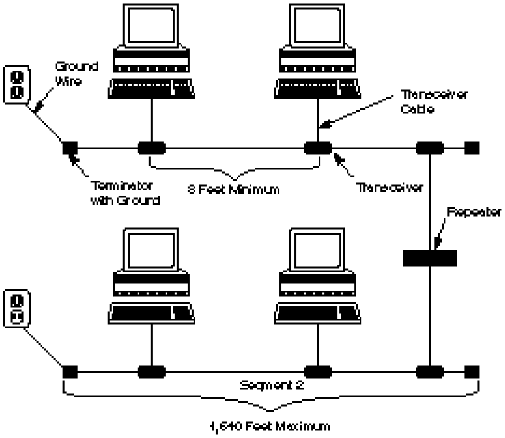
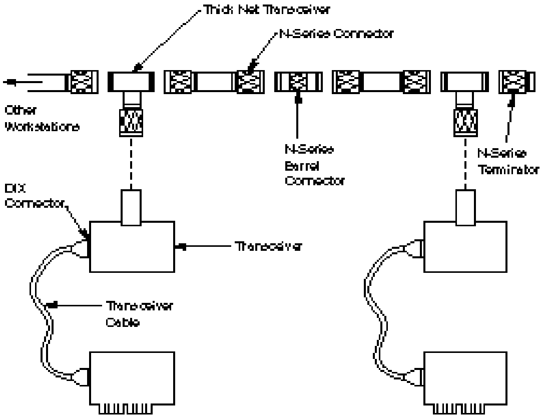


Figure 4.11

Components of a Thicknet network.



The primary advantage of 10BASE5 is its capability to exceed the cable restrictions that apply to 10BASE2. 10BASE5 does pose restrictions of its own, however, which you should consider when installing or troubleshooting a 10BASE5 network. As with 10BASE2 networks, the first consideration when troubleshooting a 10BASE5 network should be the established cabling rules and guidelines. You must follow several additional guidelines, along with the 5-4-3 rule, when configuring Thicknet networks, such as the following:

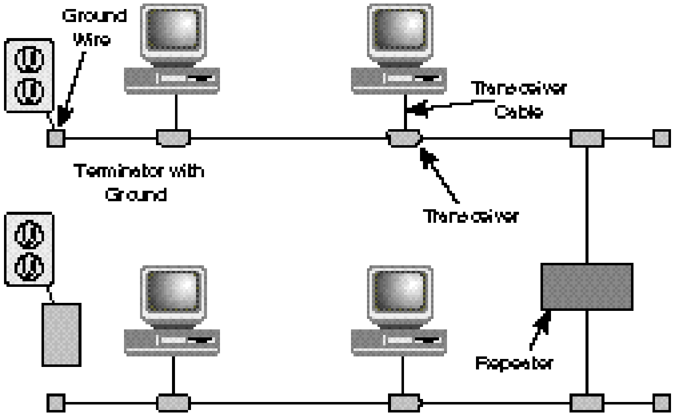
- The minimum cable distance between transceivers is 2.5 meters (8 feet).
- You may not go beyond the maximum network segment length of 500 meters (1,640 feet).
- The entire network cabling scheme cannot exceed 2,500 meters (8,200 feet).
- One end of the terminated network segment must be grounded.
- Drop cables (transceiver cables) can be as short as required but cannot be longer than 50 meters from transceiver to computer.
- The maximum number of nodes per network segment is 100. (This includes all repeaters.)

The length of the drop cables (from the transceiver to the computer) is not included in measurements of the network segment length and total network length. Figure 4.12 shows two segments using Thicknet and the appropriate hardware.

As Chapter 3 mentions, Thicknet and Thinnet networks are often combined, with a Thicknet backbone merging smaller Thinnet segments. (See Chapter 3 for more on 10BASE5's Thicknet cabling.)

Figure 4.12

Example of Thicknet network cabling.



10BASE-T

The trend in wiring Ethernet networks is to use unshielded twisted-pair (UTP) cable. 10BASE-T, which uses UTP cable, is one of the most popular implementations for Ethernet. It is based on the IEEE 802.3 standard. 10BASE-T supports a data rate of 10 Mbps using baseband.

10BASE-T cabling is wired in a star topology. The nodes are wired to a central hub, which serves as a multiport repeater (see fig. 4.13). A 10BASE-T network functions logically as a linear bus. The hub repeats the signal to all nodes, and the nodes contend for access to the transmission medium as if they were connected along a linear bus. The cable uses RJ-45 connectors, and the network adapter card can have RJ-45 jacks built into the back of the card.

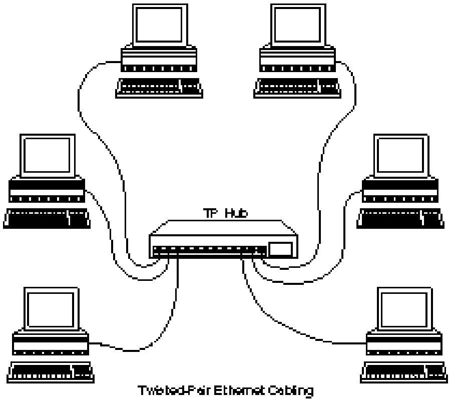


Figure 4.13

A 10BASE-T network.

10BASE-T segments can be connected by using coaxial or fiber-optic backbone segments. Some hubs provide connectors for Thinnet and Thicknet cables (in addition to 10BASE-T UTP-type connectors).

By attaching a 10BASE-T transceiver to the AUI port of the network adapter, you can use a computer set up for Thicknet on a 10BASE-T network.

The star wiring of 10BASE-T provides several advantages, particularly in larger networks. First, the network is more reliable and easier to manage because 10BASE-T networks use a concentrator (a centralized wiring hub). These hubs are “intelligent” in that they can detect defective cable segments and route network traffic around them. This capability makes locating and repairing bad cable segments easier.

10BASE-T enables you to design and build your LAN one segment at a time, growing as your network needs to grow. This capability makes 10BASE-T more flexible than other LAN cabling options.

10BASE-T is also relatively inexpensive to use compared to other cabling options. In some cases in which a data-grade phone system already has been used in an existing building, the data-grade phone cable can be used for the LAN.

> Networks with star wiring topologies can be significantly easier to troubleshoot and repair than bus-wired networks. With a star network, a problem node can be isolated from the rest of the network by disconnecting the cable and directly connecting it to the cable hub. If the hub is considered intelligent, management software developed for that hub type, as well as the hub itself, can disconnect the suspect port.

The rules for a 10BASE-T network are as follows:

- The maximum number of computers on a LAN is 1,024.
- The cabling should be UTP Category 3, 4, or 5. (Shielded twisted-pair cabling, STP, can be used in place of UTP.)
- The maximum unshielded cable segment length (hub to transceiver) is 100 meters (328 feet).
- The cable distance between computers is 2.5 meters (8 feet).

10BASE-FL

10BASE-FL is a specification for Ethernet over fiber-optic cables. The 10BASE-FL specification calls for a 10 Mbps data rate using baseband.

The advantages of fiber-optic cable (and hence, the advantages of 10BASE-FL) are discussed in Chapter 3. The most important advantages are long cabling runs (10BASE-FL supports a maximum cabling distance of about 2,000 meters) and the elimination of any potential electrical complications.

100VG-AnyLAN

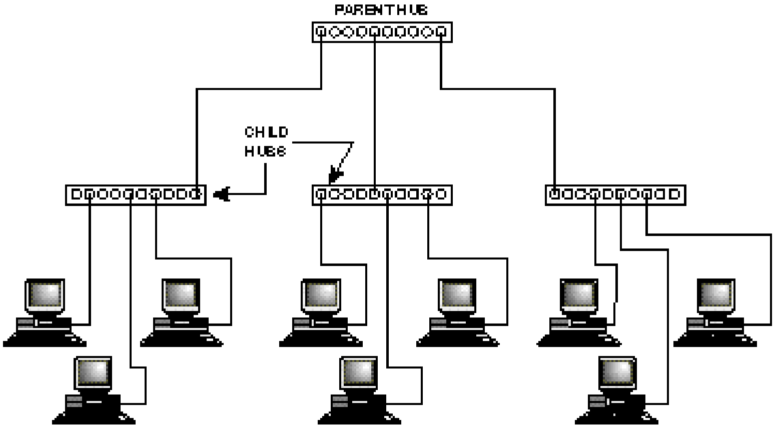
100VG-AnyLAN is defined in the IEEE 802.12 standard. *IEEE 802.12* is a standard for transmitting Ethernet and Token Ring packets (IEEE 802.3 and 802.5) at 100 Mbps. 100VG-AnyLAN is sometimes called 100BASE-VG. The “VG” in the name stands for voice grade.

The section titled “Demand Priority” earlier in this chapter, discussed 100VG-AnyLAN’s demand priority access method, which provides for two priority levels when resolving media access conflicts.

100VG-AnyLAN uses a *cascaded star* topology, which calls for a hierarchy of hubs. Computers are attached to *child hubs*, and the child hubs are connected to higher-level hubs called *parent hubs* (see fig. 4.14).

Figure 4.14

Cascaded star topology.



The maximum length for the two longest cables attached to a 100VG-AnyLAN hub is 250 meters (820 ft). The specified cabling is Category 3, 4, or 5 twisted-pair or fiber-optic. 100VG-AnyLAN is compatible with 10BASE-T cabling.

Both 100VG-AnyLAN and 100BASE-X (see the following section) can be installed as a plug-and-play upgrade to a 10BASE-T system.

100BASE-X

100BASE-X uses a star bus topology similar to 10BASE-T’s. 100BASE-X provides a data transmission speed of 100 Mbps using baseband.

The 100BASE-X standard provides the following cabling specifications:

- **100BASE-TX.** Two twisted-pairs of Category 5 UTP or STP
- **100BASE-FX.** Fiber-optic cabling using 2-strand cable
- **100BASE-T4.** Four twisted-pairs of Category 3, 4, or 5 UTP

100BASE-X is sometimes referred to as “Fast Ethernet.”
Like 100VG-AnyLAN, 100BASE-X provides compatibility with existing 10BASE-T systems and thus enables plug-and-play upgrades from 10BASE-T.

Token Ring

Token Ring uses a token-passing architecture that adheres to the IEEE 802.5 standard, as described earlier. The topology is physically a star, but Token Ring uses a logical ring to pass the token from station to station. Each node must be attached to a concentrator called a *multistation access unit (MSAU or MAU)*.

In the earlier discussion of token passing, it may have occurred to you that if one computer crashes, the others will be left waiting forever for the token. MSAUs add fault tolerance to the network, so that a single failure doesn’t stop the whole network. The MSAU can determine when the network adapter of a PC fails to transmit and can bypass it.

Token Ring network interface cards can run at 4 Mbps or 16 Mbps. Although 4 Mbps cards can run only at that data rate, 16-Mbps cards can be configured to run at 4 or 16 Mbps. All cards on a given network ring must run at the same rate.

As shown in figure 4.15, each node acts as a repeater that receives tokens and data frames from its nearest active upstream neighbor (NAUN). After the node processes a frame, the frame transmits downstream to the next attached node. Each token makes at least one trip around the entire ring and then returns to the originating node. Workstations that indicate problems send a *beacon* to identify an address of the potential failure.

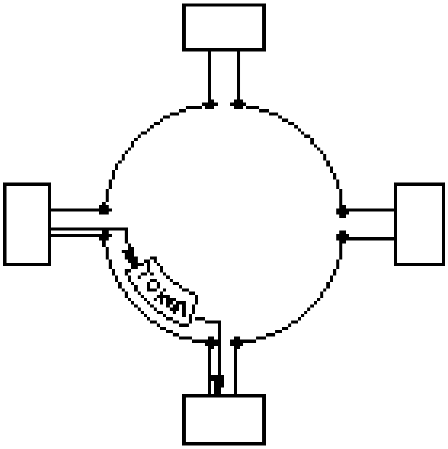


Figure 4.15

Operation of a Token Ring.

Token Ring Cabling

Traditional Token Ring networks use twisted-pair cable. The following are standard IBM cable types for Token Ring:

- **Type 1.** A braided shield surrounds two twisted-pairs of solid copper wire. Type 1 is used to connect terminals and distribution panels or to connect between different wiring closets that are located in the same building. Type 1 uses two STPs of solid-core 22 AWG wire for long, high data-grade transmissions within the building's walls. The maximum cabling distance is 101 meters (331 feet).

- **Type 2.** Type 2 uses a total of six twisted-pairs: two are STPs (for networking) and four are UTPs (for telephone systems). This cable is used for the same purposes as Type 1, but enables both voice and data cables to be included in a single cable run. The maximum cabling distance is 100 meters (328 feet).

- **Type 3.** Used as an alternative to Type 1 and Type 2 cable because of its reduced cost, Type 3 has unshielded twisted-pair copper with a minimum of two twists per inch. Type 3 has four UTPs of 22 or 24 AWG solid-core wire for networks or telephone systems. Type 3 cannot be used for 16 Mbps Token Ring networks. It is used primarily for long, low data-grade transmissions within walls. Signals don't travel as fast as with Type 1 cable because Type 3 doesn't have the shielding that Type 1 uses. The maximum cabling distance (according to IBM) is 45 meters (about 148 feet). Some vendors specify cabling distances of up to 150 meters (500 feet).

Type 3 cabling (UTP) is the most popular transmission medium for Token Ring. A Token Ring network using Type 3 (UTP) cabling can support up to 72 computers. A Token Ring network using STP cabling can support up to 260 computers.

The minimum distance between computers or between MSAUs is 2.5 meters (8 feet).

A patch cable is a cable that connects MSAUs. Patch cables are typically IBM Type 6 cables that come in standard lengths of 8, 30, 75, or 150 feet. (A Type 6 cable consists of two shielded 26-AWG twisted-pairs.) You can also get patch cables in custom lengths. You can use patch cables to extend the length of Type 3 cables or to connect computers to MSAUs. Patch cables have an IBM connector at each end.

Token Ring adapter cables have an IBM data connector at one end and a nine-pin connector at the other end. Adapter cables connect client and server network adapters to other network components that use IBM data connectors. The type of connectors you'll need for a Token Ring network depends on the type of cabling you're using. Type 3 cabling uses RJ-11 or RJ-45 connectors. (Media filters, if necessary, can convert the network adapter to RJ-11 or RJ-45 format.) Meanwhile, Type 1 and 2 cabling use IBM Type A connectors.

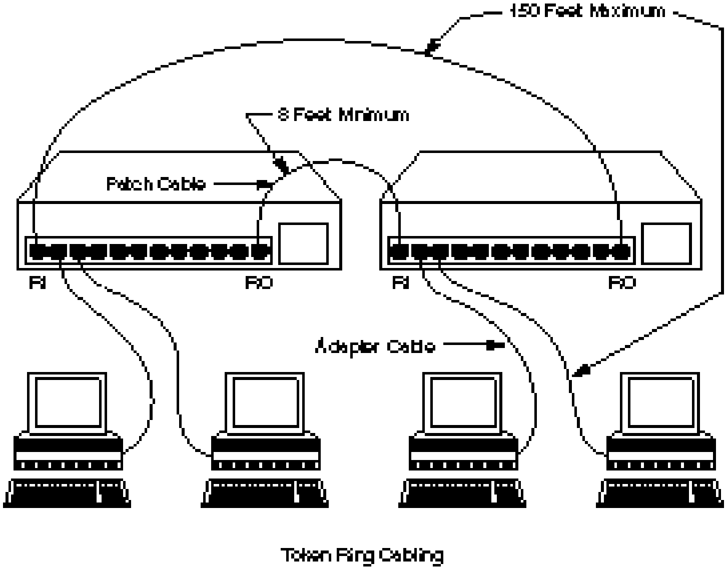
Token Ring networks come in a few sizes and designs. A *small movable* Token Ring system supports up to 12 MSAUs and uses Type 6 cable to attach clients and servers to IBM Model 8228 MSAUs. Type 6 is flexible but has limited distance capabilities. The characteristics of Type 6 cable make it suitable for small networks and for patch cords.

A *large nonmovable* system supports up to 260 clients and file servers with up to 33 MSAUs. This network configuration uses IBM Type 1 or Type 2 cable. The large nonmovable system also involves other wiring needs, such as punch panels or distribution panels, equipment racks for MSAUs, and wiring closets to contain the previously listed components.

The MSAU is the central cabling component for IBM Token Ring networks. The 8228 MSAU was the original wiring hub developed by IBM for Token Ring networks. Figure 4.16 shows 8228 MSAUs. Each 8228 has ten connectors, eight of which accept cables to clients or servers. The other connectors are labeled RI (ring in) and RO (ring out). The RI and RO connectors are used to connect multiple 8228s to form larger networks.

Figure 4.16

An example of Token Ring cabling using MSAUs.



8228s are mechanical devices that consist of relays and connectors. Their purpose is to switch clients in and out of the network. Each port is controlled by a relay powered by a voltage sent to the MSAU from the client. When an 8228 is first set up, each of these relays must be initialized with the setup tool that is shipped with the unit. Insert the setup tool into each port and hold it there until a light indicates that the port is properly initialized.

Figure 4.16 shows an example of a network cabling several clients and MSAUs. The distances noted in the figure are based on the rules for the small movable cabling system.

When you connect a Token Ring network, make sure you do the following:

1. Initialize each port in the 8228 MSAU by using the setup tool shipped with the MSAU.
2. If you're using more than one MSAU, connect the RO port of each MSAU with the RI port of the next MSAU in the loop. Complete the loop so that the MSAUs form a circle or ring.

Passing Data on Token Rings

As this chapter has already described, a frame called a token perpetually circulates around a Token Ring. The computer that holds the token has control of the transmission medium. The actual process is:

1. A computer in the ring captures the token.
2. If the computer has data to transmit, it holds the token and transmits a data frame. A Token Ring data frame contains the fields listed in table 4.1.
3. Each computer in the ring checks to see if it is the intended recipient of the frame.
4. When the frame reaches the destination address, the destination PC copies the frame to a receive buffer, updates the frame status field of the data frame (see step 2), and puts the frame back on the ring.
5. When the computer that originally sent the frame receives it from the ring, it acknowledges a successful transmission, takes the frame off the ring, and places the token back on the ring.

Table 4.1

Token Ring Data Frame Fields

Field	Description
Start delimiter	Marks the start of the frame
Access control	Specifies priority of the frame; also specifies whether the frame is a token or a data frame
Frame control	Media Access Control information
Destination address	Address of receiving computer
Source address	Address of sending computer
Data	Data being transmitted
Frame check sequence	Error-checking information (CRC)
End delimiter	Marks the end of the frame
Frame status	Tells whether the destination address was located and whether the frame was recognized

The Beaconing Process

Generally, the first station that is powered-up on a Token Ring network automatically becomes what is called the *active monitor* station. The responsibility of the active monitor station is to announce itself to the next active downstream station as the active monitor station and request that station to announce itself to its next active downstream station. The active monitor station sends this beacon announcement every seven seconds.

After each station announces itself to its next active downstream neighbor, the announcing station becomes the nearest active upstream neighbor (NAUN) to the downstream station. Each station on a Token Ring network has an upstream neighbor as well as a downstream neighbor.

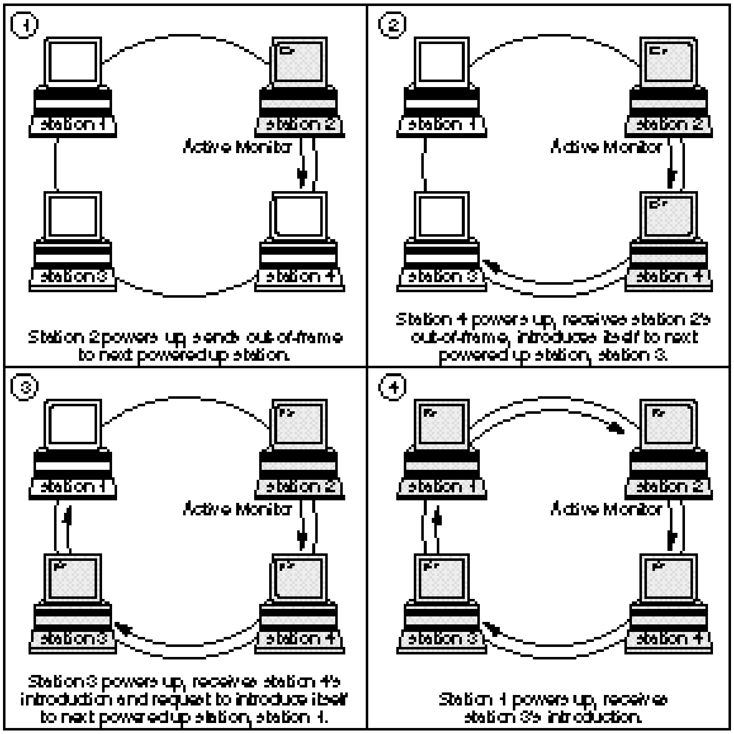
After each station becomes aware of its NAUN, the beaconing process continues every seven seconds. If, for some reason, a station doesn't receive one of its expected seven-second beaconed announcements from its upstream neighbor, it attempts to notify the network of the lack of contact from the upstream neighbor. It sends a message out onto the network ring, which includes the following:

- The sending station's network address
- The receiving NAUN's network address
- The beacon type

From this information, the ring can determine which station might be having a problem and then attempt to fix the problem without disrupting the entire network. This process is known as *autoreconfiguration.* If autoreconfiguration proves unsuccessful, manual correction becomes necessary. Figure 4.17 shows a Token Ring network utilizing the beaconing process.

Figure 4.17

Token Ring beaconing.


1
station 1
station 2
Active Monitor
station 3
station 4
Station 2 powers up, sends out-of-frame to next powered up station.
2
station 1
station 2
Active Monitor
station 3
station 4
Station 4 powers up, receives station 2's out-of-frame, introduces itself to next powered up station, station 3.
3
station 1
station 2
Active Monitor
station 3
station 4
Station 3 powers up, receives station 4's introduction and request to introduce itself to next powered up station, station 1.
4
station 1
station 2
Active Monitor
station 3
station 4
Station 1 powers up, receives station 3's introduction.

Summary

This chapter examined some common network topologies. You learned about the basic access methods, such as contention and token passing. This chapter then described some fundamental topology archetypes (bus, ring, and star) and discussed the differences between physical and logical topologies. Lastly, the chapter described the common varieties of Ethernet and Token Ring networks.

Exercises

Exercise 4.1: Matching Topologies to Applications

Objective: Practice associating network topologies with appropriate uses.

Time estimate: 10 minutes.

Match the topology to the application. For this exercise, you should be familiar with the material in this chapter and also in Chapter 3.

1. 10BASE2

A. You are looking for an inexpensive network with the maximum flexibility for future expansion. You want to utilize existing data-grade phone lines for some segments.

2. 10BASE5

B. Your network encompasses three buildings. The longest segment length is 450 meters. You want to minimize cost. Differences in electrical ground potential between the buildings is not a problem.

3. 10BASE-T

C. Your company encompasses three buildings. The longest segment length is 1,800 meters. In previous networking attempts, you have experienced problems with the ground potential differences between the buildings.

4. 10BASE-FL

D. You are designing a network for an airline ticket office. Employees query the database constantly, so the network utilization rate is extremely high. The network must be very reliable and capable of self-corrective action to isolate a malfunctioning PC.

5. 100BASE-X

E. You work in a small office with 12 PCs. You are looking for an inexpensive networking

continues

Exercise 4.1: Continued

	solution. The computers are spaced evenly throughout the office (approximately 3–5 meters between workstations). You want to minimize the total amount of cabling.
6. Token Ring	F. Your company colorizes Hollywood movies. Huge, digitized movie files, such as *Bringing Up Baby* or *The Jazz Singer,* must pass quickly through the network so they will arrive with extreme dispatch at colorizing workstations. Very high transmission speeds are required. Your company is reaping huge profits, so the cost of cabling is no concern.

The correct responses are as follows:

1. E
2. B
3. A
4. C
5. F
6. D

Review Questions

The following questions test your knowledge of the information in this chapter. For additional questions, see MCP Endeavor and the Microsoft Roadmap/Assessment Exam on the CD-ROM that accompanies this book.

1. CSMA/CD uses which two of the following techniques to control collisions?

   A. Nodes broadcast a warning before they transmit.

   B. Nodes listen for a clear line before they transmit.

   C. Nodes request and are given control of the medium before transmitting.

   D. Nodes listen while they transmit and stop transmitting if another signal interferes with the transmission.

2. The maximum size of a CSMA/CD network is __________.

   A. 100 meters

   B. 300 meters

   C. 1,500 meters

   D. 2,500 meters

3. CSMA/CA is commonly used by __________.

   A. Microsoft networks

   B. LocalTalk networks

   C. Fast Ethernet networks

   D. 10BASE5 networks.

4. Which three of the following network architectures use the token passing access method?

   A. IEEE 802.4

   B. FDDI

C. Token Ring

D. IEEE 802.3

5. If you see a group of networked computers connected to a central hub, you know that the network has a __________ physical topology.

A. ring

B. star

C. bus

D. can't tell

6. If you see a group of networked computers connected to a central hub, you know that the network has a __________ logical topology.

A. ring

B. star

C. bus

D. can't tell

7. The __________ topology uses fiber-optic cable.

A. 10BASE2

B. 10BASE5

C. 10BASE-T

D. none of the above

8. The __________ topology uses Thicknet cable.

A. 10BASE2

B. 10BASE5

C. 10BASE-T

D. none of the above

9. The __________ topology uses UTP cable.

   A. 10BASE2

   B. 10BASE5

   C. 10BASE-T

   D. none of the above

10. The __________ topology uses Thinnet cable.

   A. 10BASE2

   B. 10BASE5

   C. 10BASE-T

   D. none of the above

11. 10BASE5 networks cannot exceed a maximum length of __________.

   A. 185 meters

   B. 300 meters

   C. 500 meters

   D. 1,000 meters

12. Which two of the following are characteristics of a 10BASE-T network but not a 10BASE2 network?

   A. CSMA/CD

   B. central hub

   C. UTP

   D. BNC

13 __________ is sometimes called "Fast Ethernet."

   A. 10BASE-T

   B. 10BASE5

   C. 100VG-AnyLAN

   D. 100BASE-X

14. A Token Ring network using STP cabling can support _________ computers.

    A. 60

    B. 260

    C. 500

    D. 1,024

15. The _________ field of a Token Ring frame is updated by the destination PC.

    A. destination address

    B. frame check sequence

    C. end delimiter

    D. frame status

16. Which two of the following statements are true?

    A. Coax Ethernet is a physical bus and a logical bus.

    B. 10BASE-T Ethernet is a physical bus and a logical bus.

    C. Coax Ethernet is a physical star and a logical bus.

    D. 10BASE-T Ethernet is a physical star and a logical bus.

17. What is the main advantage of using 10BASE2 when network segments don't have to exceed 185 meters?

    A. It is relatively simple to connect.

    B. Drop cables can be used, making it easier to troubleshoot.

    C. Each node connects directly to the cable.

    D. It is the least expensive of the cabling options.

18. Which two of the Ethernet topologies require that each end of the bus be terminated?

    A. 10BASE2

    B. 10BASE5

    C. 10BASE-T

    D. Thinnet

19. Which of the following isn't an advantage of using 10BASE-T for cabling a network?

    A. It is easier and more reliable to manage.

    B. Centralized hubs make it easier to detect bad cable segments.

    C. Beaconing helps to isolate cable breaks.

    D. It is relatively inexpensive to use.