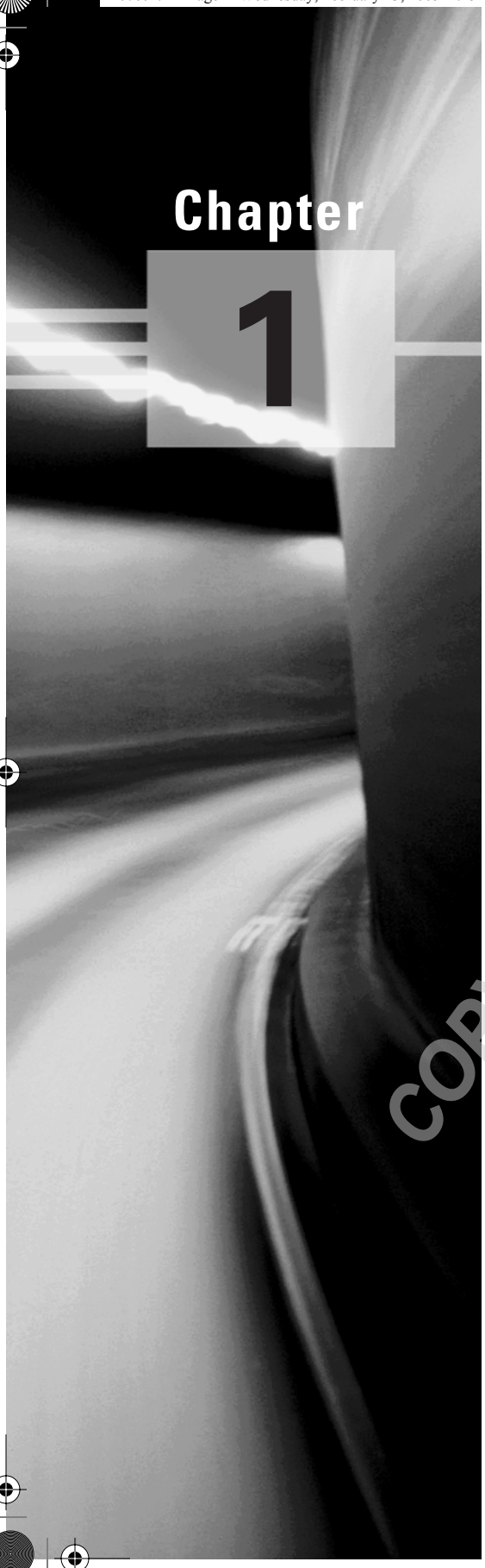
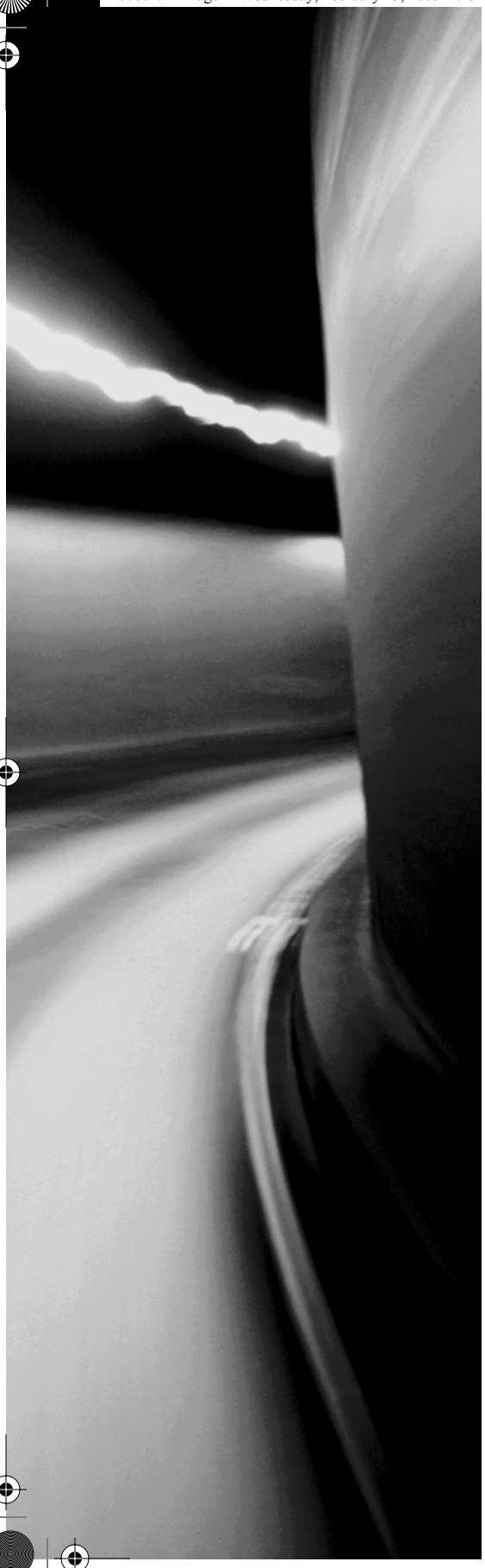


Chapter 1

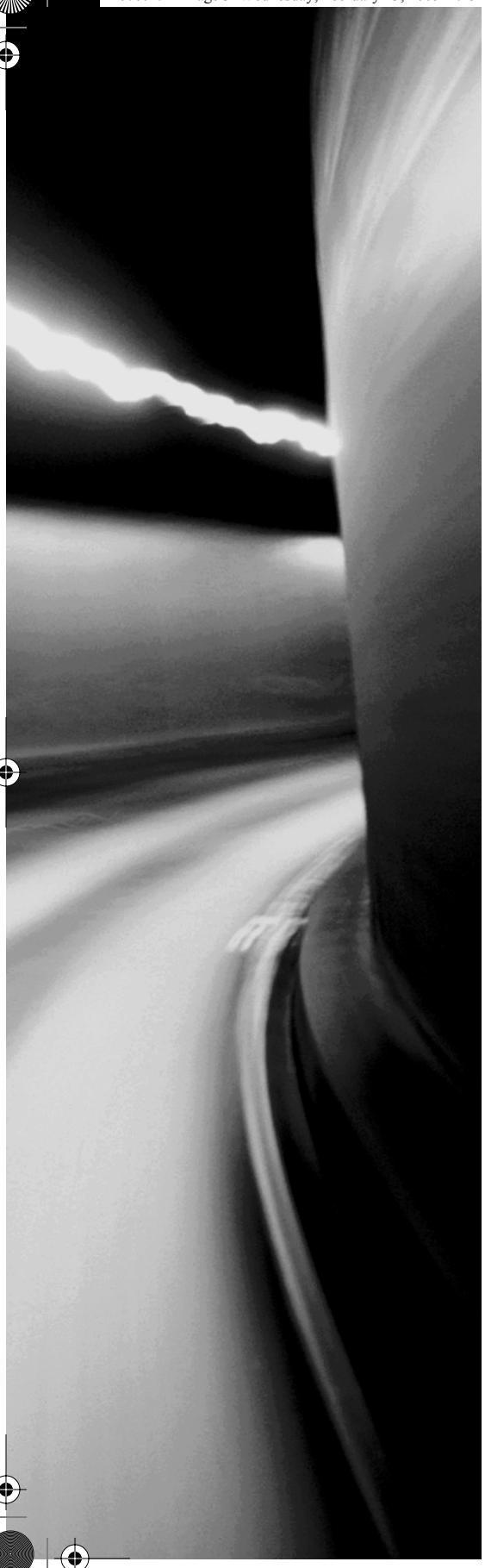
Domain 1 Media and Topologies

COMPTIA NETWORK+ EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description:**
  - Star
  - Bus
  - Mesh
  - Ring
- ✓ **1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including:**
  - Speed
  - Access method (CSMA / CA (Carrier Sense Multiple Access/Collision Avoidance) and CSMA / CD (Carrier Sense Multiple Access / Collision Detection))
  - Topology
  - Media
- ✓ **1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:**
  - 10BASE-T and 10BASE-FL
  - 100BASE-TX and 100BASE-FX
  - 1000BASE-TX, 1000BASE-CX, 1000BASE-SX and 1000BASE-LX
  - 10GBASE-SR, 10GBASE-LR and 10GBASE-ER



- ✓ **1.4 Recognize the following media connectors and describe their uses:**
  - RJ-11 (Registered Jack)
  - RJ-45 (Registered Jack)
  - F-Type
  - ST (Straight Tip)
  - SC (Standard Connector)1
  - IEEE1394 (FireWire)1
  - LC (Local Connector)1
  - MTRJ (Mechanical Transfer Registered Jack)1
- ✓ **1.5 Recognize the following media types and describe their uses:**
  - Category 3, 5, 5e, and 6
  - UTP (Unshielded Twisted Pair)
  - STP (Shielded Twisted Pair)
  - Coaxial cable
  - SMF (Single Mode Fiber) optic cable
  - MMF (Multimode Fiber) optic cable
- ✓ **1.6 Identify the purposes, features and functions of the following network components:**
  - Hubs
  - Switches
  - Bridges
  - Routers
  - Gateways
  - CSU / DSU (Channel Service Unit / Data Service Unit)
  - NICs (Network Interface Card)
  - ISDN (Integrated Services Digital Network) adapters
  - WAPs (Wireless Access Point)
  - Modems
  - Transceivers (media converters)
  - Firewalls



- ✓ **1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies:**
  - 802.11 (Frequency hopping spread spectrum) 802.11*x* (Direct sequence spread spectrum)
  - Infrared
  - Bluetooth
- ✓ **1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).**

A network is a group of computers that are connected to share hardware and software. In order for the computers to communicate with each other, they must share three elements: a network media and topology, a protocol, and a software client or service. In this chapter, we will focus on the first of these elements, the network media and topology.

While the basic concept of connecting computers hasn't changed much since the mid-1980s, the methods that we use to connect them have changed dramatically. Networking technologies have evolved dramatically over the last 20 years and will continue to evolve. The components that we use in our networks have also evolved because of these technologies.

When you connect computers, your main goal is to provide fast communication with as few errors as possible. You should understand that the type of media and topology you use in your network will largely determine your ability to reach this goal. In addition, you should know that the components that you choose for a network will also affect your capability to control network traffic. In this chapter, we will discuss several networking media and topologies and compare the features that they, and the components that use them, bring to your network design to help you control traffic within your network.

1.1 Recognizing Logical and Physical Network Topologies

Basically, a *topology* is a shape, so a network topology is the shape of a network. There is, however, a big difference between a physical network topology and a logical network topology. The physical network topology represents how the network looks to the naked eye—in other words, the way the components are arranged. The logical network topology represents how the flow of information works its way through the network. This may not be the same as it looks to the naked eye. You should understand the main network topologies as well as the difference between a physical network topology and a logical one. In this section, we discuss the most common network topologies.

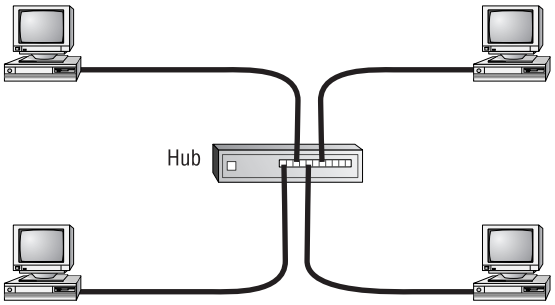
Critical Information

Recognizing the major differences in regard to the shape and the components that are used in the most common topologies is important. You should be able to recognize these differences given a diagram, schematic, or description. In the following paragraphs, we discuss each network topology in greater detail.

Star

A *star* topology is a group of computers that are connected to a central location such as a hub or a switch. This is the most common topology in use today. The computers may be physically located next to each other or spread throughout an entire building, but the flow of information from each computer to the other computers must go through the central location. In a star topology, each computer has its own cable or connection to the hub. Since each computer has its own connection, the failure of one computer will not affect the other computers in the network; however, if the hub or switch should fail, then all of the computers on that hub or switch will be affected. Figure 1.1 is an illustration of a star topology.

FIGURE 1.1 A star topology



Bus

The *bus* topology was commonly used in earlier networks but is not seen much today. In a bus topology, a single cable connects all the computers. A coaxial cable is used with special connectors called BNC and T connectors. (We will discuss cables and connectors in the next section.) The T connectors provide an independent connection for each computer on the bus. In addition, the bus only works if both ends of the cable have a special resistor installed called a terminator. Figure 1.2 shows a bus topology; Figure 1.3 shows the T connector used to connect the computers to the bus.

FIGURE 1.2 A bus topology

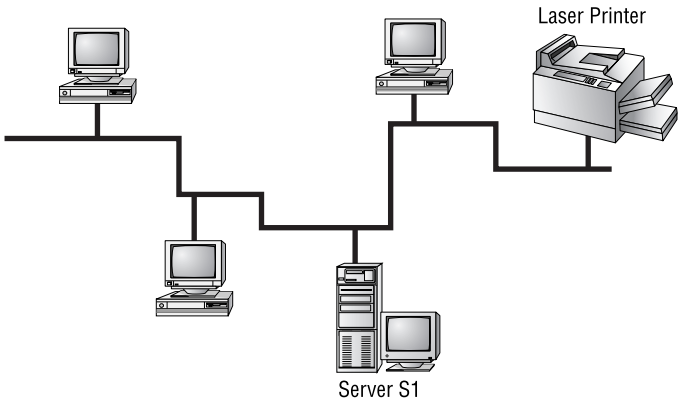
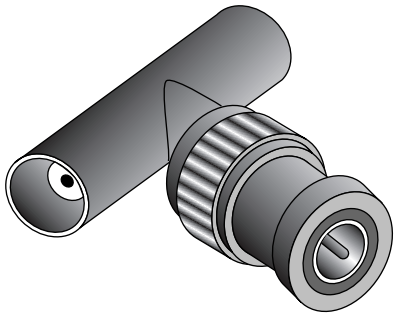


FIGURE 1.3 A T connector



Mesh

The *mesh* topology is not often used and is almost never used for individual computers. In a full-mesh topology, all of the components in the mesh have independent connections to all of the other components in the mesh. For example, if four computers are connected with a "full mesh," then the number of connections can be determined by the following formula:

n(n – 1) = total number of connections

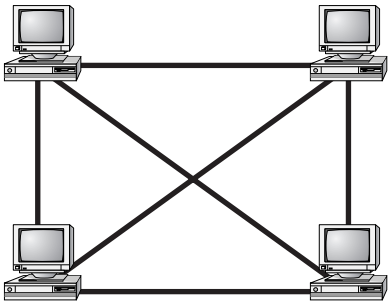
In this case:

4(4 – 1) = 12

In other words, there are a total of 12 connections and each computer has to contain three network interface cards.

Actually, any network with multiple or redundant connections to network components can be considered a mesh topology, but because of the expense involved in creating this type of network, they are rarely created for individual computers. A mesh, and even a full mesh, would most likely be found connecting multiple networks in an organization. In fact, the Internet is the best and biggest example of a mesh topology. Figure 1.4 shows a full-mesh topology with four computers.

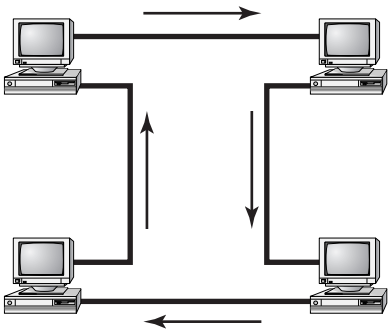
FIGURE 1.4 A mesh topology



Ring

A *ring* topology (see Figure 1.5) looks exactly like a star topology to the naked eye. The real difference between a ring topology and a star topology lies in the technology used. Computers in a ring topology generally use an IBM Token Ring technology. Other components can also be arranged in a ring topology and use different technologies. The computers involved in a ring topology are not generally arranged in a physical ring. In fact, just as with a star topology, they can be located next to each other or spread throughout a building. The difference is that the central component that connects them contains the logical ring that facilitates communication on the network using the ring technologies. (We will discuss ring technologies in the next section.)

FIGURE 1.5 A ring topology



Exam Essentials

Know the difference between a physical topology and a logical topology. The physical topology of the network is simply what it looks like or how the components are arranged. The logical topology, on the other hand, represents the flow of information in the network.

Be able to list the main features of a star topology. Be able to recognize a star topology from a diagram, schematic, or description. A star topology contains a central hub (or switch) and all information must flow through the hub. A star topology is considered fault tolerant, since each device has its own network connection.

Describe the main features of a bus topology. A bus topology uses a coaxial cable, and all computers are connected to the same cable. T connectors are used to attach the computers. Resistors called terminators must be used at both ends of a bus. Keep in mind that the failure of one computer will generally not affect the entire segment, but a break in the cable will.

Summarize the main features of a mesh topology. A mesh topology provides multiple connections for the devices in the mesh. A full mesh requires $n(n-1)$ connections, where n is the number of devices in the mesh. A mesh topology is most often used with networks and not with individual computers.

Describe the main features of a ring topology. A ring topology looks like a star topology; the real difference is in the way that the information is transferred through the network. The IBM Token Ring is the most common type of ring topology, but is quickly being replaced by the star topology and Ethernet.

1.2 Specifying the Main Features of Networking Technologies

Whereas the topology of a network is the shape of the network, the technology is the method of putting information onto the network and controlling it based on the physical components that are used and how they operate within the network. Some technologies have evolved over time, some have been all but discontinued, while others have been improved and refined.

In February 1980, the Institute of Electrical and Electronics Engineers (IEEE) developed a set of standards called the 802 project. Each of the standards was given a number beginning with 802 (the 80th year and the second month). These standards have been refined over the last two decades, but (in general) are still used to represent the main networking technologies of the past, present, and future. In this section, we discuss each of these technologies in detail.

Critical Information

Familiarize yourself with the new technologies as well as some of the older, less used technologies. You should be able to specify the main features of each technology, such as speed, access method, topology used, and media used. In the paragraphs that follow, we discuss each of the technologies with which you should be familiar.

Ethernet

Ethernet is by far the most common technology in use today. The Internet operates using Ethernet technology. It was first developed by Xerox at the Palo Alto Research Center (PARC) and was defined as 802.3 by the IEEE. Ethernet began production at a speed of only 3Mbps, but common speeds today include 10Mbps, 100Mbps, and 1000Mbps. The speed of the network is dependent on the devices that are used and on the slowest devices in the network. (We will discuss types of network devices later in this chapter.)

Ethernet uses an access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). This method of putting data "on the wire" works by first sensing the wire to determine whether there is currently any data flowing on it, indicated by a fluctuation in electrical current. If no data is flowing on the wire, then the Ethernet device can send its data. Sometimes two devices might try to send data at the same time, resulting in a collision. If this happens, then the network is "stalled" until the devices have sent their data again with no collision. One of the responsibilities of a network designer is to control traffic in order to reduce or eliminate collisions.

Ethernet networks began as bus topologies that used coaxial cable. These networks used a large coaxial cable as a backbone and a smaller coaxial cable to connect the computers and hubs to the backbone. Today, Ethernet networks typically use unshielded twisted-pair (UTP) cable in a star topology. Some networks use wireless connections that require no cable at all. (We will discuss media types in greater detail later in this chapter.) Table 1.1 highlights the main features of the Ethernet topology.

TABLE 1.1 Ethernet Topology Features

Speed	10Mbps, 100Mbps (Fast Ethernet), 1000Mbps (Gigabit Ethernet), and 10,000Mbps (10G Ethernet)
Access Method	CSMA/CD
Topology	Star, bus (bus is not widely used today)
Media	Copper wire and fiber-optic cable

Logical Link Control (LLC)

Logical Link Control (LLC) is a networking technology defined by the IEEE as 802.2. It does not provide a complete networking model, but instead defines the standards for controlling the data sent and received by a system. LLC specifies the protocols, or rules, that perform flow control and error checking. These protocols are the essential foundation for all of the other networking standards.

Token Ring

Token Ring was introduced by IBM in the mid-1980s. Since it virtually eliminated collisions and thereby increased the speed of networks, it became the network topology of choice for those companies who could afford the best and most expensive networks. Defined by the IEEE as 802.5, Token Ring uses a token-passing access method. A token is a unique electronic signal that must be attached to a message in order for the message to enter the network or travel on it. Because there is only one token on each ring, only one message can travel on the network at any given point in time, thereby eliminating the possibility of collisions.

Token Ring uses a physical star topology but the logical topology is a ring. The ring is actually created inside special hubs called multiple-station access units (MSAUs). The media used in Token Ring is twisted-pair cable. Typically, Token Ring networks run at either 4Mbps or 16Mbps. While Token Ring had a huge following in the 1980s, it has been all but eliminated from modern network designs due to advancements in technology that increased the speed and reliability of Ethernet. Table 1.2 highlights the main features of the Token Ring topology.

Wireless

Today's networks have the capability to eliminate the cables for many of the computers. The IEEE 802.11 wireless standard was originally defined in the 1980s by the "forward-thinking" representatives of the IEEE. Nowadays, many individuals and companies are adopting the technology for portions of their networks. Because of the conveniences that they offer, wireless networks will likely continue to grow in popularity.

TABLE 1.2 Token Ring Topology Features

Speed	4Mbps, 16Mbps
Access Method	IBM token passing
Topology	Ring
Media	Copper wire

The 802.11 standard has two common levels: 802.11b and 802.11g. The 802.11b standard offers speeds up to 11Mbps, and the 802.11g standard increases the speed to 54Mbps. Both use an access method referred to as Carrier Sense Multiple Access with Collision Avoidance CSMA/CA. This access method is similar to CSMA/CD except that the device that wants to send its message must first send a very small message to make sure that the signal can be received without any collisions or other problems. If the short message is transmitted successfully, then the long message is sent next. The media that 802.11 wireless networks use is the 2.4GHz radio wave band. Table 1.3 highlights the main features of the wireless topology.

TABLE 1.3 Wireless Topology Features

Speed	11Mbps, 54Mbps
Access Method	CSMA/CA
Topology	Star (WAP is central point)
Media	2.4GHz radio band

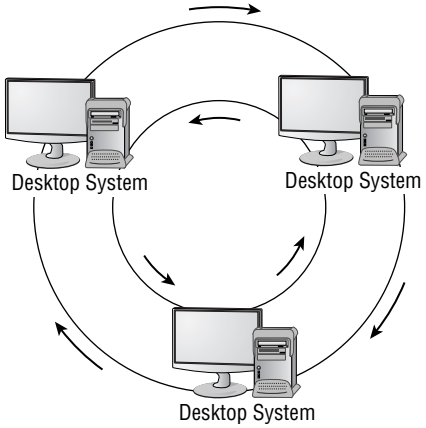
FDDI

Fiber Distributed Data Interface (FDDI) was developed by the American National Standards Institute (ANSI) in the mid-1980s. It uses a token-passing access method and a dual-ring topology. Figure 1.6 shows an example of an FDDI topology. The media used by FDDI is typically fiber-optic cable, but it can also use shielded twisted-pair (STP) or unshielded twisted-pair (UTP) cable. (We will discuss cable types in greater detail later in this chapter.) FDDI communicates at a speed of 100 Mbps on copper wire, but can communicate much faster on fiber-optic cable. (FDDI on copper wire is sometimes referred to as CDDI.) Table 1.4 highlights the main features of the FDDI topology.

TABLE 1.4 FDDI Topology Features

Speed	100Mbps–620Mbps
Access Method	Token passing
Topology	Dual-ring
Media	Copper wire and fiber-optic cable

FIGURE 1.6 An FDDI topology



Exam Essentials

Know the difference between a topology and a technology. A network's topology represents the way that it is shaped logically and physically, but its technology represents the methods that it uses to introduce data onto the media and transfer it to other computers.

List the characteristics of Ethernet. Ethernet, the most common technology in use today, uses the CSMA/CD access method to put data onto the wire. Ethernet has evolved over time and has many different speeds, including 10Mbps, 100Mbps, 1000Mbps, and 10,000Mbps. Ethernet is defined by the IEEE 802.3 specification.

Describe the characteristics of LLC. LLC is a standard defined by the IEEE 802.2 specification. It is not a complete networking model, but it does define the standards for controlling data sent and received by systems. LLC defines the rules and standard for flow control and error checking.

Know the characteristics of Token Ring. Token Ring is a technology developed by IBM and defined by the 802.5 specification standard. Token Ring uses a token-passing method of carrier access to eliminate the possibility of collisions. The two main speeds of Token Ring are 4Mbps and 16Mbps. Token Ring is used on copper wire for local area networks (LANs).

List the characteristics of the wireless topology. The wireless topology is defined by the 802.11 specification standard. The two most common standards of wireless communication are 802.11b and 802.11g; both use the 2.4GHz radio band. Keep in mind that 802.11b operates at 11Mbps and 802.11g operates at 54Mbps. Wireless communications use a CSMA/CA method of media access, which tests the communication channel before sending data onto it.

Describe the characteristics of FDDI. FDDI is a topology that is used in wide area networks (WANs) rather than LANs. FDDI uses a token-passing method similar to Token Ring, but its method is more advanced. It uses a dual-ring topology to provide for fault tolerance. The speed of FDDI is generally 100Mbps, but some forms of FDDI can transmit much faster.

1.3 Specifying the Characteristics of Cable Standards

The cables that connect our networks today have evolved from earlier standards. Although some of these standards are no longer in common use today, understanding them will assist you in appreciating the advantages of the cables that we use today. You should know the characteristics of these standards. In this section, we discuss each of these cable standards in detail.

Critical Information

You should know the speeds, maximum lengths, topology, and cable types associated with each of the main cable standards. In the paragraphs that follow, we discuss each of these characteristics in detail.

10BASE-T and 10BASE-FL

The most common cable standard used in the early 1990s was 10BASE-T. The "10" represents the maximum speed of 10Mbps; "BASE" represents a baseband type of transmission in which only one signal can be on the wire at any given time; "T" indicates that a twisted-pair cable was used. The maximum length of any network segment using 10BASE-T is 100 meters.

As you can imagine, some organizations needed to have a network segment that was longer than 100 meters. In the mid- to late 1990s, 10BASE-FL was developed to provide the solution. It used a fiber-optic cable to transmit the signal rather than the copper twisted-pair cable. The fiber-optic cable can transmit much further without suffering a loss of signal due to the media itself (a problem referred to as *attenuation*). The speed of 10BASE-FL was still 10Mbps, but the maximum transmission length could be up to 20 kilometers! Many of these networks are still in use today where speed is not a concern but maximum distance is a factor. Table 1.5 shows the characteristics of 10BASET and 10BASE-FL.

TABLE 1.5 Characteristics of 10BASE-T and 10BASE-FL

	Speed	Max. Length	Topology	Cable Type
10BASE-T	10Mbps	100 meters	Star	Copper wire Category 3+
10BASE-FL	10Mbps	20 kilometers	Star	Fiber-optic

100BASE-TX and 100BASE-FX

100BASE-TX is by far the most common networking standard in use today. The "100" represents the maximum speed of 100Mbps; "BASE" represents a baseband type of transmission; and "TX" represents twisted-pair cable of the type that will support 100Mbps transmission. (We will discuss cable types in greater detail later in this chapter.) Although 100BASE-TX is 10 times faster than 10BASE-T, it is still limited to 100 meters per network segment.

To provide a solution for longer network segments, 100BASE-FX was developed. It uses fiber-optic cable to increase the distance that the signal can be transmitted without suffering from attenuation. Some devices that use 100BASE-FX can transmit up to 20 kilometers! Table 1.6 shows the characteristics of 100BASE-TX and 100BASE-FX.

TABLE 1.6 Characteristics of 100BASE-T and 100BASE-FX

	Speed	Max. Length	Topology	Cable Type
100BASE-T	100Mbps	100 meters	Star	Copper wire Category 5+
100BASE-FX	100Mbps	20 kilometers	Star	Fiber-optic

1000BASE-TX, 1000BASE-CX, 1000BASE-SX, and 1000BASE-LX

The next fastest cable standard is 1000BASEX, Gigabit Ethernet. The "1000" represents 1000Mbps, or 1 Gbps, and "BASE" represents a baseband type of transmission in a star topology. While this standard is implemented in many forms, the only main difference is the cable type used and therefore the maximum distance. Table 1.7 shows the difference in cable types and maximum transmission distance possible for each form of 1000BASEX.

TABLE 1.7 1000BASEX Cable Standards

	1000 BASE-TX	1000 BASE-CX	1000BASE-SX	1000BASE-LX
Cable Type	Unshielded twisted-pair	Shielded copper (STP)	One fiber-optic cable	Two fiber-optic cables
Maximum Distance	100 meters	25 meters	550 meters	5000 meters

10GBASE-SR, 10GBASE-LR, and 10GBASE-ER

The newest and fastest cable standard is the 10G standard. As you may have guessed, the 10G standard allows a maximum transmission speed of 10Gbps, or 10 billion bits per second, in a star topology. The 10G standard is currently subdivided into three standards: 10GBASE-SR,

10GBASE-LR, and 10BASE-ER. All of these 10G standards use fiber-optic cable. The major difference between the standards is the maximum transmission distance. Table 1.8 shows the maximum transmission distance for each standard.

TABLE 1.8 10GBASEX Cable Standards

	10GBASE-SR	10GBASE-LR	10GBASE-ER
Maximum Distance	82 meters	10 kilometers	40 kilometers

Exam Essentials

Recognize the terminology used when identifying cable standards. You should be able to determine the speed and transmission type of a cable standard solely based on its name.

Know the characteristics of the 10BASE-T standard. The 10BASE-T standard indicates a 10Mbps baseband signal that uses a twisted-pair copper wire. This means that the maximum distance for this technology, without the use of repeaters, is 100 meters. 10BASE-T uses a star topology.

List the characteristics of the 10BASE-FL standard. The 10BASE-FL standard indicates a 10Mbps baseband signal that uses a fiber-optic cable. This means that the maximum distance for a run is about 20 kilometers. 10BASE-FL uses a star topology.

Describe the characteristics of the 100BASE-TX standard. The 100BASE-TX standard indicates a 100Mbps (Fast Ethernet) baseband signal that uses a twisted-pair copper cable. This means that the maximum distance for a run is 100 meters, without the use of repeaters. 100BASE-FX uses a star topology.

Know the characteristics of the 100BASE-FX standard. The 100BASE-FX standard indicates a 100Mbps (Fast Ethernet) baseband signal that uses a fiber-optic cable. This means that the maximum distance for a run is 20 kilometers. 100BASE-FX uses a star topology.

Be familiar with the characteristics of the 1000BASE-TX standard. The 1000BASE-TX standard indicates a 1000Mbps (1Gbps) baseband signal that uses unshielded twisted-pair cable. This means that the maximum distance for a run is 100 meters, without the use of repeaters. 1000BASE-TX uses a star topology.

List the characteristics of the 1000BASE-CX standard. The 1000BASE-CX standard indicates a 1000Mbps (1Gbps) baseband signal that uses Category 5 shielded twisted-pair cable. It is therefore more immune to electrical interference, but it has a maximum distance of only 25 meters. 1000BASE-CX uses a star topology.

Describe the characteristics of the 1000BASE-SX standard. The 1000BASE-SX standard indicates a 1000Mbps (1Gbps) baseband signal that uses one fiber-optic cable. This means that

it has a maximum distance of 550 meters, without the use of repeaters. 1000BASE-SX uses a star topology.

Know the characteristics of the 1000BASE-LX standard. The 1000BASE-LX standard indicates a 1000Mbps (1Gbps) baseband signal that uses two fiber-optic cables. This means that it has a maximum distance of 5000 meters, with the use of repeaters. 1000BASE-LX uses a star topology.

List the characteristics of the 10GBASE-SR standard. The 10GBASE-SR standard indicates a 10,000Mbps baseband signal that uses fiber-optic cable. Due to the type of fiber-optic cable that it uses, it has a maximum transmission distance of 82 meters. 10GBASE-SR uses a star topology.

Describe the characteristics of the 10GBASE-LR standard. The 10GBASE-LR standard indicates a 10,000Mbps baseband signal that uses fiber-optic cable. Due to the type of fiber-optic cable that it uses, it has a maximum transmission distance of 10 kilometers. 10GBASE-LR uses a star topology.

Know the characteristics of the 10GBASE-ER standard. The 10GBASE-ER standard indicates a 10,000Mbps baseband signal that uses fiber-optic cable. Due to the type of fiber-optic cable that it uses, it has a maximum transmission distance of 40 kilometers. 10GBASE-ER uses a star topology.

1.4 Recognizing Media Connectors

No matter what type of cable you are using, it won't be very effective unless it has the proper connectors on each end. The type of connectors that you use will depend on the cable as well as on your intended use for the cable. In other words, you need to have the proper connectors to plug into the devices that you are trying to use. In this section, we discuss the most common types of media connectors used in networks.

Critical Information

You should be able to recognize by sight the most common types of cable connectors and describe their main use. In this section, we will discuss the purpose of the major types of connectors and provide a photograph of each type.

RJ-11

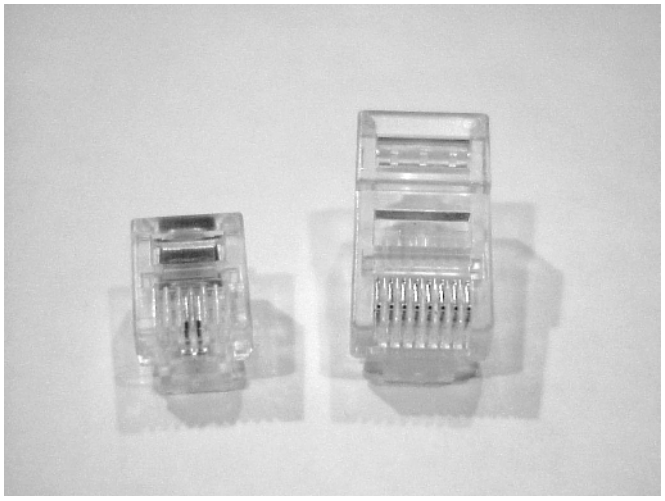
"RJ" stands for *registered jack*. Chances are good that you have held an RJ-11 connector in your hand, since they are used on all of the telephone connections in the United States and most other countries. An RJ-11 connector can contain and connect two pairs of wires. In regard to

computers, you are most likely to use an RJ-11 connector when you attach a modem to a telephone line. In fact, you plug an RJ-11 into the wall and another one into the modem. Figure 1.7 shows an RJ-11 connector on the left.

RJ-45

The RJ-45 connector is the most common network connector. It is used to connect network interface cards (NICs) to hubs and/or switches. RJ-45s can also be used to connect network devices together for communication as well as control. The RJ-45 connector can contain and connect four pairs of wires. For example, RJ-45 connectors are used to connect computer cables to a patch panel, a patch panel to a switch, and then to connect the switch to a router in order to supply a user connection to the Internet. Figure 1.7 shows an RJ-45 connector on the right.

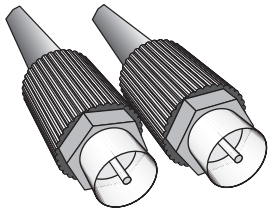
FIGURE 1.7 An RJ-11 connector (left) and an RJ-45 connector (right)



F-Type

Although coaxial cables are rarely used for computer network backbones, they have experienced a resurgence of growth because they are used to connect a cable modem to an NIC to provide a computer with a broadband Internet connection. Many of the newest coaxial cables use a new connector that slides onto the coaxial cable connection on a device with just one quick push. This new connector is referred to as an F-type connector. F-type connectors make connecting cable modems to the cable company's connections much easier than with previous connectors that had to be twisted many times to secure the connection. Figure 1.8 shows an F-type connector.

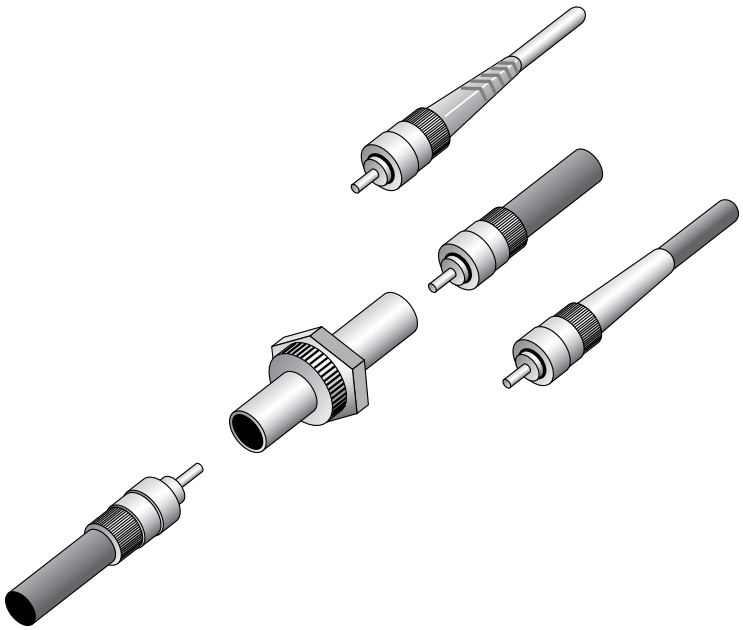
FIGURE 1.8 An F-type connector



ST

The ST (straight tip) connector is a type of fiber-optic cable connector. It uses a half-twist bayonet type of lock to hold it in place securely. ST connectors are most commonly used with single-mode fiber-optic cable that runs long distances. For example, an ST connector might be used on either side of a fiber backbone between two buildings on a corporate campus. Figure 1.9 shows an ST connector.

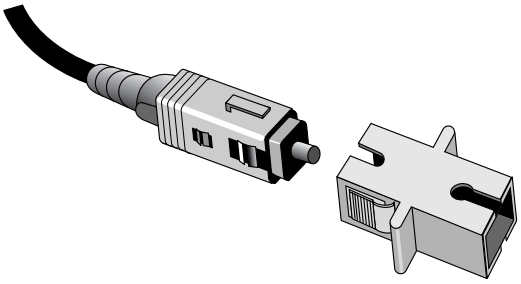
FIGURE 1.9 An ST connector



SC

The SC (standard connector) connector is a type of fiber-optic cable connector. It uses a push-pull connector mechanism that is similar to common audio and video plugs. SC connectors are most often used with multimode fiber-optic cable that is providing a backbone segment for a LAN. For example, SC connectors might be used on either side of a fiber backbone that runs between the floors of a single building. (We will discuss single-mode and multimode fiber-optic cable later in this chapter.) Figure 1.10 shows an SC connector.

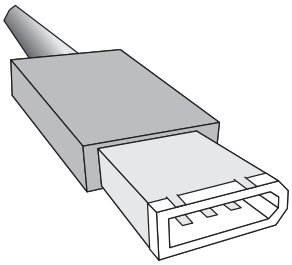
FIGURE 1.10 An SC connector



IEEE 1394

Specially developed for transferring pictures and video, the IEEE 1394 standard (also known as FireWire) has its own type of connector. You can recognize an IEEE 1394 connector by its small and distinctive "D" shape. This type of connector is now found on many types of video and multimedia devices. For example, you might use an IEEE 1394 connector to connect a digital video recorder to a computer to download pictures. Figure 1.11 shows an IEEE 1394 connector cable.

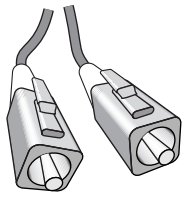
FIGURE 1.11 An IEEE 1394 connector cable



LC

The LC (local connector) connector is a fiber connector that is built into the body of an RJ-style jack. The LC connector is used for local connections. This type of connector is generally found on a fiber-optic patch cord that is used to connect fiber-optic equipment within the network closet itself. Figure 1.12 shows an LC connector.

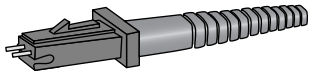
FIGURE 1.12 An LC connector



MTRJ

The MTRJ connector is one of the newest designs for connecting fiber-optic cable. The new connector is easier to use and smaller that the older types of connectors. Due to their rugged and durable design, they are becoming the connector of choice for use in the network and telecom closet of an organization. Figure 1.13 shows an MTRJ connector.

FIGURE 1.13 An MTRJ connector



Exam Essentials

Be able to recognize the main types of connectors used in networks. Be able to recognize a photo of the most common media connectors that we described in this chapter and discuss its normal use.

Know the characteristics of the RJ-11 connector. RJ stands for registered jack, and the RJ-11 connector is the connector that is commonly used with regular telephone lines. The RJ-11 connector contains four wires to be used as two pairs of wires. RJ-11 connectors are used to connect modems to telephone lines for communication on the Internet.

Describe the characteristics of the RJ-45 connector. The RJ-45 connector is the most common network connector. It is used to connect various types of network equipment, including patch panels, hubs, switches, and routers. The RJ-45 connector contains eight wires, or four pairs of wires.

List the characteristics of the F-type connector. The F-type connector is a new connector developed for use with coaxial cable connections. It provides a faster connection than the older type (BNC) connectors that were used for coaxial cable. The main use for coaxial cable these days is to connect cable modems to the cable company's outlet to create a connection to the Internet.

Know the characteristics of ST connectors. The ST connector is a type of fiber-optic cable connector that uses a half-twist bayonet type of lock. The ST connector is typically used with single-mode fiber-optic cable that runs long distances.

List the characteristics of SC connectors. The SC connector is a type of fiber-optic connector. It is a push-pull connector that is similar to audio and video plugs. The SC connector is most often used to connect a fiber-optic backbone segment within a LAN.

Be familiar with the characteristics of IEEE 1394 connectors. IEEE 1394 is a video and multimedia connector that is commonly referred to as FireWire. The IEEE 1394 connector has a distinctive "D" shape. The main purpose of the IEEE 1394 standard is increased speed of data transfer for video and multimedia applications.

Know the characteristics of LC connectors. The LC connector is a type of fiber connector. It is used to connect fiber-optic equipment within the network closet. This type of connector is generally found on patch cords that are used to connect fiber-optic equipment for short distances.

Describe the characteristics of MTRJ connectors. The MTRJ connector is a type of fiber connector. It is typically used to connect fiber-optic equipment for short distances in the network and telecom closet, as is the LC connector. The MTRJ connector is beginning to replace the LC connector because of its rugged design and durability.

1.5 Recognizing Media Types

The *media* is the wired or wireless connection that allows one computer to communicate with another computer. When you choose a cable standard and a connector type, you are also choosing a media type. It's important that you understand your choices in regard to connector type and media type.

Critical Information

You should be able to recognize the most common media types and describe their use. In this section we discuss each media type and its most common use.

Category 3, 5, 5e, and 6 Twisted-Pair Cables

The category of a twisted-pair cable indicates the tightness of the twist applied to the wire pairs in the cable. The twist in wire pairs prevents an electrical interference called crosstalk from affecting the communication. Crosstalk occurs when a signal bleeds over from one wire to

another (even through the insulation of the wire). The tighter the twist, the faster you can transmit information through a cable without suffering from crosstalk. Table 1.9 shows the maximum speed of the main cable categories.

Category 5e (enhanced) is the cable type that is currently recommended as a minimum for all new installations. Cable is generally used to connect each computer to a central point, typically a hub or a switch, that is contained in a network closet. Ensuring that each computer has its own cable creates redundancy in the network and thereby provides fault tolerance.

TABLE 1.9 Cable Categories and Speeds

	Category 3	Category 5	Category 5e	Category 6
Maximum Speed	10Mbps	100Mbps	1000Mbps	1000Mbps

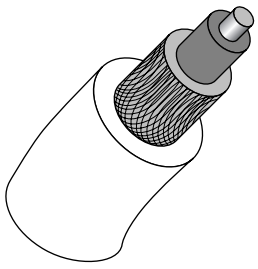
UTP

Unshielded twisted-pair (UTP) cable is the most common type of cable used today. UTP is offered for all of the categories of cable that we have discussed. It is most often used because it is far easier to install than STP (which we will discuss next). The only protection from electrical interference provided by UTP is the fact that the pairs of wires within the cable are twisted, which is usually enough.

STP

Shielded twisted-pair (STP) resembles UTP except that it includes a foil shield that covers the wires and adds another layer of protection against outside magnetic interference. In order for this protection to be effective, the connections have to be properly grounded. This adds to the complexity of installations, so most organizations have opted to use fiber-optic cable instead of STP when electromagnetic interference is a problem. For example, if a cable is passing by a large electrical motor or fluorescent light ballast, STP might be used to provide greater resistance from electromagnetic interference (EMI). STP cable was often used for communication connections through elevator shafts, prior to fiber-optic cable. Figure 1.14 shows an STP cable.

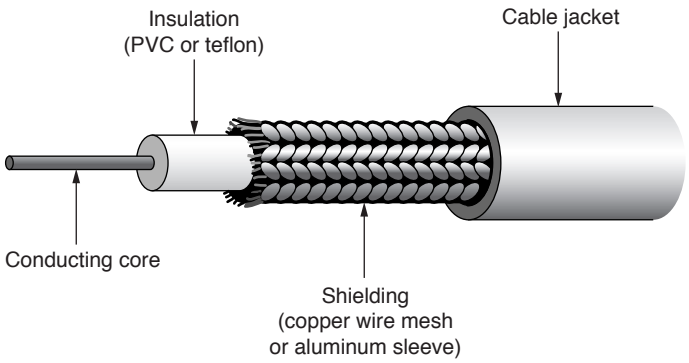
FIGURE 1.14 An STP cable



Coaxial Cable

In the late 1980s, coaxial cable was used as the backbone of network segments and to connect computers to the bus topology that made up the network. Coaxial cable is rarely used anymore for network backbones or to connect computers, but it is being used today to connect cable modems to the cable provider's connection to provide a computer with a broadband Internet connection. Coaxial cable consists of an inner core wire and an outer braid of insulating wire. The entire signal is carried by the inner core wire. Figure 1.15 shows the components that make up a coaxial cable.

FIGURE 1.15 A coaxial cable



Single-Mode Fiber

Single-mode fiber-optic cable (SMF) is a very high speed and very high distance media. It consists of a single strand of fiberglass that carries the signals. The light source that is generally used with single-mode fiber is a laser, although light-emitting diodes (LEDs) might also be used. With single-mode fiber, a single light source is transmitted from end to end and pulsed to create communication. Single-mode fiber is used for long runs because it can transmit data 50 times further than multimode fiber and at a faster rate. For example, single-mode fiber might be used on an organization's corporate campus between buildings. Since the transmission media is glass, the installation of single-mode fiber can be a bit tricky. There are other layers protecting the glass core, but the cable still should not be crimped or pinched around any tight turns. It is, however, completely immune to electrical interference since light is used instead of electrical signals. Figure 1.16 illustrates the layers included in single-mode fiber-optic cable

Multimode Fiber

Multimode fiber-optic cable (MMF) also uses light to communicate a signal, but the light is dispersed into numerous paths as it travels through the core and is reflected back by cladding that lines the core. Multimode fiber provides high bandwidth at high speeds over medium distances (up to about 3000 feet) but can be inconsistent for very long runs. Because of this, multimode fiber is generally used within a smaller area of a building whereas single mode might be used

between buildings. Multimode fiber is available in glass or in a plastic version that makes installation easier and increases installation flexibility. As with single-mode fiber, multimode fiber can be used when electrical interference is present, since it is completely immune to that interference. For example, multimode fiber might be used today to provide communication connections in a building that go through an elevator shaft. Figure 1.17 shows the how light is split into multiple paths in a multimode fiber-optic cable.

FIGURE 1.16 Single-mode fiber-optic cable

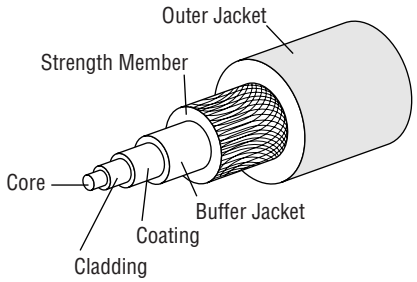
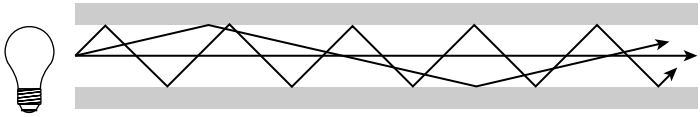


FIGURE 1.17 A multimode fiber-optic cable



Exam Essentials

Know and be able to recognize common media types. The most common media types are twisted-pair cable, coaxial cable, and fiber optic cable. You should be able to recognize the most common media types given a picture or description.

Describe how common media types are used. You should know how the most common media types are used to transfer data throughout the network. You should be able to differentiate between copper based twisted-pair cables and fiber-optic cables. You should also know how each type might be used in a network.

Know the characteristics of Category 3 cable. Category 3 cable is a copper twisted-pair cable that can carry signal at a maximum of 10Mbps without suffering from crosstalk. This type of cable is rarely used in networks today.

Describe the characteristics of Category 5 cable. Category 5 cable, the most common cable type today, is a copper twisted-pair cable that can carry signals at a maximum rate of 100Mbps without suffering from crosstalk. Category 5 cable is used to connect computers and many other devices within a LAN.

List the characteristics of Category 5e cable. Category 5e cable is a copper twisted-pair cable that can carry signals at a maximum rate of 1000Mbps without suffering from crosstalk. This is one of the most commonly installed cables today.

Know the characteristics of Category 6 cable. Category 6 cable is a copper twisted-pair cable that can carry signals at maximum rate of 1000Mbps without suffering from crosstalk. This is also one of the most commonly installed cables today.

Describe the characteristics of UTP. Unshielded twisted-pair (UTP) cable is the most common type of cable used today. It does not provide any shielding other than the fact that the wires are twisted. Most of the cable standards include the UTP type of cable.

Know the characteristics of STP. Shielded twisted-pair (STP) cable is used to reduce the effect of EMI on cables in environments that contain large sources of EMI, such as electric motors or fluorescent light ballasts. STP includes a foil shield that provides that added protection. STP is rarely used in today's networks because it has been replaced by fiber-optic cable.

List the characteristics of coaxial cable. Coaxial cable was used for backbone segments and for bus topology networks in the late 1980s. The entire signal on a coaxial cable is transmitted through the core wire in the center of the cable. The main use for coaxial cable today is to connect cable modems to the cable provider's connection.

Know the characteristics of single-mode fiber. Single-mode fiber optic cable is a very high speed and high distance media. It generally uses a laser beam to concentrate and pulse light on a single strand of fiber. Single-mode fiber is typically used to provide a backbone for buildings on an organization's campus.

List the characteristics of multimode fiber. Multimode fiber-optic cable also uses light to transmit a signal, but the light is dispersed within the cable, causing it to travel numerous paths called modes. Each of these modes is part of the communication process that is used. Multimode fiber can provide very high bandwidth for short distances, but it can become inconsistent for very long runs, over 3000 feet. This fiber is most often used as a backbone for a LAN within a single building.

1.6 Identifying Network Components

As we said, the components that are used in a network have a tremendous effect on the capabilities of the network and on your ability to control traffic within the network. Network components have evolved with time because of the need to create fast, efficient network designs for many computers. In this section we discuss the major types of network components and their effect on your network design.

Critical Information

You should be able to identify the purpose, features, and functions of each of the main network components. In this section, we discuss each of these components in detail.

Hubs

A *hub* is a device that has multiple ports into which connections can be made. All connections made to a hub are also connected to each other. A hub does not filter any communication or provide any intelligence in regard to the data stream; it simply lets all of the information flow through it and connects anything and everything that is connected to it. Hubs are generally used to connect network segments of computers that are physically close to each other, such as all of the computers on one floor of a building or in a computer classroom. There are two major types of hubs: active and passive. An *active* hub is generally plugged into a power source so that it can amplify signals as well as connect them. A *passive* hub provides connectivity but no power. An example of a passive hub is a patch panel in a network closet.

Switches

A *switch* (also called a LAN switch) resembles a hub from the outside, but that is where the resemblance stops. Switches are considerably more expensive than hubs because of the advantages they offer. Whereas a hub simply lets traffic flow through it, a switch controls traffic through it to automatically optimize traffic flow on your network. A switch learns the physical address (MAC address) of all of the devices that are connected to it and then uses it to control traffic flow. Rather than forwarding all data to all of the connected ports, a switch can forward data only to the port where the computer with the destination address actually exists. This process automatically segments the network and dramatically decreases the traffic in the segments that are less used. Because of this, switches are often used to connect departments of a company so that communication between departments does not affect the other departments that are not involved in the communication. Also, large files can be transferred within in the same department without affecting the traffic in any of the other departments. In addition, switches can be used to create virtual local area networks (VLANs), which improve the flexibility of a network design. (We will discuss VLANs in Chapter 3, "Domain 3 Network Implementation.")

Bridges

Bridges are similar to switches in that they can provide some intelligence to segment a network. Bridges, like switches, can learn the MAC address of each of the hosts connected to them and use that address to control traffic to each of the host's ports. Bridges, however, are slower than switches, so they have been largely replaced by switches as a device that is used to segment traffic. You should be aware of two main types of Ethernet bridges:

Transparent bridge A transparent bridge can connect two dissimilar networks but is "invisible" to both networks and does not provide translation of any kind. For example, if your network contained two Ethernet segments with one Token Ring segment between them, a transparent bridge could connect communication from one of the Ethernet segments, through the Token Ring segment, to the other Ethernet segment. The Ethernet traffic would not be interpreted by the Token Ring segment.

Translational bridge A translational bridge, as you might expect, actually performs a translation between two dissimilar networks. For example, if you wanted to translate data from an Ethernet segment to a Token Ring segment, you could use a translational bridge.

Routers

Routers are devices that forward traffic from one network (or subnet) to another. Routers first determine whether the traffic belongs on their network; then they deliver the traffic that belongs on their network to the appropriate network hosts and forward the traffic that does not belong on their network to another router. Routers determine where to forward traffic by consulting a routing table. The routing table can be manually entered by an administrator, or it can be learned by the router by using routing protocols. Routers are the devices that connect the Internet and make the World Wide Web possible. They use a higher level of intelligence than that of bridges or switches. (We will discuss routing in greater detail in Chapter 2, "Domain 2 Protocols and Standards.")

Gateways

Actually, the term *gateway* refers more to a network role than a network device. Any device that is used to translate data from one format to another can be called a gateway. For example, a router that can route data from an Internetwork Package Exchange (IPX) network to an Internet Protocol (IP) network so that it can be understood by the IP network can be considered a gateway. Gateways can also be special servers whose main job is to translate protocols between two networks, such as a Systems Network Architecture (SNA) gateway between an IBM mainframe network and a Microsoft Windows network. The gateway is always positioned logically between the two networks that it will translate.

CSU/DSU

Channel Service Unit/Data Service Unit (CSU/DSU) is a converter used between a LAN and a WAN. Conversion of information is necessary because the technologies that are used in the WAN environment are very different from those used in a LAN environment. The CSU/DSU changes signal from one digital format to another. Originally, the CSU/DSU was always a separate component, but now many routers have this function built into them.

NICs

Network interface cards (NICs) are used to connect a computer to the network. A network interface card is like a small computer in itself. Its job is to translate a stream serial data (one bit at a time) into several streams of parallel data that will be used by the computer. The network interface card also examines every packet on the network cable to determine if the packet

has a destination MAC address that matches its MAC address. If it does not, then the NIC does nothing more with the packet, but if the address does match then the NIC will forward the packet to the appropriate port of the computer based on the information contained in the packet. (We will discuss ports in greater detail in Chapter 2.)

ISDN Adapters

Integrated Services Digital Network (ISDN) is a service that was developed by telephone companies in the early 1990s. It was originally intended to provide individuals with a type of simultaneous voice and data communications capability. Since the Internet was in its infancy, and the World Wide Web did not exist, ISDN was ahead of its time. Today's networks use ISDN as a backup line for other communication lines that provide greater bandwidth. The device that connects an organization's equipment to the telephone company's ISDN line and converts the signal so that it can be sent over the line is called an ISDN terminal adapter. These devices are often built into the latest network equipment.

Wireless Access Point

A *wireless access point (WAP)* is a hub that is used by wireless devices. Typically, a WAP looks just like any other hub except that it has an antenna. The WAP is connected to the wired network of an organization so that any devices that can make a wireless connection to it will also be connected to the wired network. Wireless devices typically connect to the WAP using the 2.4GHz radio frequency. Since wireless networks are continuing to grow in popularity, you're likely to see many more WAPs. (We will discuss wireless connectivity in greater detail later in this chapter.)

Modems

The term *modem* stands for modulator/demodulator. Modulation is the process of converting digital data into analog data, usually in the form of sound. Demodulation is the reverse of this process, whereby the transmitted sounds are converted back into digital data on the other side of the connection. Modems are typically used to communicate on normal telephone wires using computers. The most common types of modems used on standard telephone lines can communicate at a maximum speed of 56Kbps. It is also possible to use multiple telephone lines simultaneously to increase the speed of communication. A simple 56K modem is built into most of the computers sold today.

Transceivers

The term *transceiver* stands for transmitter/receiver. The transceiver is more of a role in a network than a specific device. Any device that receives data, converts it, and then sends it to

another location can be called a transceiver. For example, an NIC is a type of transceiver since it converts serial data into parallel data and then sends it to a port.

Firewalls

A *firewall* is a hardware or software system that is used to separate one computer or network from another one. The most common type of firewall is used to protect a computer or an entire network from unauthorized access from the Internet. Firewalls can also be used to control the flow of data to and from multiple networks within the same organization. Firewalls can be programmed to filter data packets based on the information that is contained in the packets.

Exam Essentials

Know the major network components. The major components in today's networks include hubs, switches, bridges, routers, gateways, CSU/DSUs, NICs, ISDN Adapters, WAPs, modems, transceivers, and firewalls. You should be able to describe the purpose of each network component and its role in the network.

Be able to describe the functionality of each network component. You should know how each of the major network components function. For example, you should know whether a component has any intelligence or makes any decisions about the traffic flow within a network. You should be able to differentiate between the types of network components and their capability to control network traffic.

List the characteristics of a hub. A hub is a device with multiple ports that is used to connect devices on a network. A hub only connects devices and does not provide any intelligence or filtering. Two types of hubs are generally used in networks: active hubs (which also serve as multiport repeaters) and passive hubs (which are generally called patch panels).

Know the characteristics of a switch. Switches (also called LAN switches) resemble hubs on the outside but perform filtering that hubs cannot handle. The filtering that is performed by the switches is based on the MAC address of the devices that are connected through the switch. The switches build a table of the MAC addresses and then use it to segment network traffic. Switches can be used to create VLANs, which can improve the flexibility of network design.

Describe the characteristics of a bridge. Bridges are similar to switches in that they filter network traffic based on the MAC addresses of devices that are connected through them. Bridges can be used to connect dissimilar networks. The two main types of bridges are transparent and translational.

List the characteristics of a router. Routers are devices that forward traffic from one network to another. Routers use a logical address and a routing table to determine whether network traffic belongs on their network or on another network. The routing table can be entered by an administrator or it can be learned by using routing protocols.

Describe the characteristics of a gateway. The term *gateway* refers to a network role of translating data from one format or protocol to another. The gateway can be only one of many roles on a device, or the device can be dedicated to that one role. One of the most common gateways is the IBM SNA gateway, which connects a mainframe or mini-mainframe computer to a network environment.

Know the characteristics of a CSU/DSU. A CSU/DSU is a converter used between a LAN and a WAN environment. This conversion is necessary because of the difference in the technologies that are used in the two environments. The CSU/DSU was originally a separate device, but now many routers have this function built into them.

List the characteristics of an NIC. A network interface card (NIC) is used to connect a computer to the network and facilitate communication. The NIC converts serial and parallel data to and from the computer and is also responsible for examining every packet of a data stream to determine whether that packet has a destination address that matches its own address. If the address matches, then the NIC receives the information and sends it to the correct port in the computer. If it does not match, then the NIC simply ignores the packet and does not process it any further.

Know the characteristics of an ISDN adapter. ISDN adapters were originally developed by the telephone company to convert signals so that telephone and computer equipment could use their ISDN lines. Today's networks sometimes use ISDN but the adapters are often built into the network equipment.

Describe the characteristics of a wireless access point. A wireless access point (WAP) is a hub that is used by wireless devices to connect them to a wired network. Wireless devices generally use a wireless NIC to connect to the WAP, which in turn provides a connection to a network or to the Internet. Wireless technology is growing in popularity.

Know the characteristics of a modem. You should know that the term *modem* stands for modulator/demodulator because the purpose of a modem is to convert digital signals to analog signal in the form of sounds (modulation) and to convert the sounds into the form of digital signals on the other end (demodulation). The 56K modem is the most commonly used modem on regular telephone lines today. A 56K modem in generally built into most desktop and laptop computers that are sold today.

List the characteristics of a transceiver. The term *transceiver* stands for transmitter/receiver. A transceiver is more of a role for a device than a device itself. Any device that can receive data, convert it, and then transmit it can be considered a transceiver.

Identify the characteristics of a firewall. A firewall is a hardware or software system that is used to separate one computer network from another. Firewalls are often used to protect a computer network from the Internet and can be programmed to filter packets based on the information that is contained in the packets.

1.7 Specifying the Characteristics of Wireless Technologies

One of the newest and most exciting forms of communication is *wireless* communication. This type of communication is still in its infancy, and many competing standards exist. Wireless networks, if properly installed, can add to the flexibility on your network. To properly install a wireless network you must be familiar with wireless networking standards. In this section, we discuss wireless networking standards and their effect on your network design.

Critical Information

You should know about the most common wireless standards used in today's networks. Specifically, you should be familiar with their carrier speed, frequency, transmission type, and topology. In this section, we discuss these characteristics in regard to each of the most common wireless technologies.

802.11

802.11 is the IEEE specification created for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. The original 802.11 standard used a frequency hopping spread spectrum radio (FHSS) signal. There have been many revisions to the standard since then. The following are the major 802.11 standards in use today. 802.11x represents the family of standards that use the direct sequence spread spectrum (DSSS) radio signal. Table 1.10 compares the characteristics of 802.11 wireless technologies.

802.11a Uses orthogonal frequency division multiplexing to increase bandwidth. This standard uses the 5GHz radio band and can transmit at up to 54Mbps. It is not widely used today.

802.11b Uses DSSS in the 2.4GHz radio band. This standard can transmit at up to 11Mbps with fallback rates of 5.5Mbps, 2Mbps, and 1Mbps. It is one of the most commonly used standards today.

802.11g Uses DSSS and the 2.4GHz radio band. This standard enhances the 802.11b standard and can transmit at speeds up to 54Mbps.

Infrared

The term *infrared* means "below red." In other words, infrared communication is communication made possible by light that is below red in the color spectrum of light. Human beings cannot see this light, but we can build devices that can transmit and receive it. To make use of this light, a group of manufacturers known as the Infrared Data Association (IrDA) developed

a standard in the late 1990s. Many manufacturers have adopted this standard for use with the devices that they manufacture. Because of this, many devices now have the distinctive infrared port that allows them to communicate with other devices without the use of wires. The biggest difference between infrared and other wireless technologies is that infrared requires "line of sight" communications between devices. Also, infrared does not work well in bright sunlight.

Bluetooth

Bluetooth is a short-range radio technology that was developed by Ericsson, IBM, Intel, Nokia, and Toshiba. Many products sold today use Bluetooth technology, including printers, mice, keyboards, scanners, and many more. All products must pass interoperability testing by the Bluetooth Special Interest Group prior to their release.

Exam Essentials

Be familiar with the main types of wireless networks. The main types of wireless networks are 802.11, Infrared, and Bluetooth. You should be familiar with the each of these types of networks and where they might be used.

Know the main characteristics of the main types of wireless networks. You should know the main characteristics such as carrier speed, frequency, transmission type, and topology for the main types of wireless networks.

List the characteristics of 802.11x components. The 802.11x specification refers to the family of standards that use DSSS, usually on the 2.4GHz radio band. The most common of these are the 802.11b and 802.11g standards.

Know the characteristics of 802.11a. 802.11a is a standard for wireless communication that uses OFDM on the 5GHz radio band. 802.11a, which can communicate at a maximum rate of 54Mbps, is rarely used in today's networks.

Describe the characteristics of 802.11b. 802.11b is a standard for wireless communication that uses DSSS on the 2.4GHz radio band. 802.11b, which can communicate at a maximum rate of 11Mbps, is in common use in many networks today.

List the characteristics of 802.11g. 802.11g is a standard for wireless communication that uses DSSS on the 2.4GHz radio band. 802.11g, which can communicate at a maximum rate of 54Mbps, is in common use in many networks today.

Know the characteristics of infrared. The term *infrared* means "below red." Infrared light is light that humans cannot see, but we can use it to control devices and to communicate to them. The standards for the use of infrared light have been developed by the Infrared Data Association (IrDA). Infrared devices require a line-of-sight connection with a device in order to communicate effectively. Many devices are now including infrared capability.

1.8 Identifying Wireless Service Performance Factors

Since wireless services are continuing to grow in popularity, we are beginning to see wireless devices used in many different types of environments. While most wireless protocols work properly in the "perfect environment," most of them also become challenged in the real world. In this section, we discuss the real-world factors that affect wireless communications.

Critical Information

You should know the factors that might affect the range and speed of wireless device that you use. In this section, we discuss the most common of these factors.

Radio Interference

To understand how radio interference can be a problem in a wireless network, you have to consider the access method that the wireless network uses: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This means that a device will wait until no other device appears to be using the frequency before it sends its data over the frequency. If the network is close to an operating 2.4GHz phone, a microwave oven, or a Bluetooth device, it might sense that the network is in use and wait for the offending interference to subside before it sends its data. Also, if the interference is sporadic, the communication might be interrupted during a transmission. This would cause the data to become corrupted and would force the device to resend the data. In this case, the device might still operate but much more slowly than normal. To keep radio interference from affecting your networks, identify the sources and try to eliminate them wherever possible. Also, keeping devices in close proximity to the WAP will help to reduce the effects of interference, since the true signal will overpower the interference.

Antenna Type

Because your wireless network operates using radio waves, the sensitivity of the antenna that is used in your network can increase the range and speed of the communication. A huge variety of antennas are available from commercial sources. These include directional and omni-directional models for indoor and outdoor use. Network enthusiasts have even developed operational antennae from common household objects such as a tin can or an emptied potato chip can. The type of antenna that you use in your network will depend on the placement of the computers that require connectivity to the network. Often, the antenna that is built into the WAP is the only antenna that you will need.

Environmental Factors

While radio waves do not require line of sight in order to communicate properly, they are affected by some environmental factors. Simple factors such as the materials with which the

building was constructed can affect the range and speed of your wireless network. Since you cannot see the radio waves, you have to experiment a little to determine the best method of deploying your WAPs.

You can begin experimenting by placing WAPs in "best guess" locations and then walking around your network with a laptop equipped with a wireless NIC to determine where the signal is strongest and where it becomes weak. You can then change the location of a WAP or add another WAP as you begin to get a sense of the network's tendencies within your building.

Another way to optimize your network is to purchase equipment that will provide a spread spectrum analysis of radio transmissions in your building in a graphical format that allows you to "see" the radio waves as they travel through your building. This type of equipment can also identify and isolate other types of radio waves that might cause interference in your network. In either case, your goal is to eliminate as much interference as possible and keep signal strength to a maximum wherever possible.

Exam Essentials

Know the factors that might affect the range and speed of your wireless network communications. The range and speed of the network might be affected by interference, antenna types, and environmental conditions. You should be able to identify options that might improve these characteristics within your network.

Describe how wireless networks are affected. Wireless networks might be affected by such factors as interference, antenna type, and environmental factors. Be familiar with the methods of troubleshooting these factors to provide for the maximum range and speed of your wireless network.

Understand how radio interference can affect computer communication. Radio interference can keep wireless devices from communicating effectively. Part of the reason for this is the fact that the wireless devices use a CSMA/CA access method, which ensures that a medium is clear before trying to send information onto it. Know how to diagnose a problem caused by another wireless device, such as a Bluetooth device, and how to solve the problem by either removing the false signal or strengthening the real signal.

Know how antenna type can affect wireless communications. The type of antenna used in a wireless network can dramatically affect the range and direction of signal. Some antennas are designed to be very sensitive to signals in one direction only (directional), while others are designed to receive signals in the same manner in all directions (omni-directional). The antenna that is included on the WAP is often the only antenna needed for a wireless network.

Understand how environmental factors can affect wireless communications. Environmental factors such as the type of building or the construction of walls in a building can have a dramatic effect on a wireless network. You can optimize your network by experimenting with the best placement of WAPs in the building so as to avoid the pitfalls caused by the environmental factors. In addition, you can purchase special software that will give you a graphical representation of radio wave behavior in your building and assist you in finding other sources of interference.

Review Questions

1. Which logical network topology uses a hub as a central point of communication for all of the devices on a segment?
   - **A.** Ring
   - **B.** Star
   - **C.** Mesh
   - **D.** All of the above
2. Which network technology uses the CSMA/CD carrier access method to communicate?
   - **A.** Ethernet
   - **B.** Token Ring
   - **C.** FDDI
   - **D.** Bus
3. Which wireless standard uses the 2.4GHz radio band to communicate at speeds up to 54Mbps?
   - **A.** 802.11a
   - **B.** 802.11b
   - **C.** 802.11x
   - **D.** 802.11g
4. What is the maximum distance that a device can transmit a signal if it uses a 100BASE-FX standard?
   - **A.** 2000 meters
   - **B.** 2 kilometers
   - **C.** 20 kilometers
   - **D.** 200 kilometers
5. What is the name of the registered jack connector that is used on most network devices?
   - **A.** RJ-11
   - **B.** Category 5
   - **C.** ST
   - **D.** RJ-45
6. What IEEE specification is assigned to the FireWire cable standard?
   - **A.** 802.11x
   - **B.** Category 5e
   - **C.** 1394
   - **D.** 802.5

7. What is the maximum data transmission speed for Category 5e cable?
   - **A.** 100Mbps
   - **B.** 1000Mbps
   - **C.** 10,000Mbps
   - **D.** 100,000Mbps

8. Which type of device can be used to segment a network *and to* create VLANs?
   - **A.** Bridge
   - **B.** Router
   - **C.** Hub
   - **D.** Switch

9. Which type of wireless communication uses light and requires line of sight to operate properly?
   - **A.** Infrared
   - **B.** 802.11x
   - **C.** DSSS
   - **D.** 802.11g

10. Which type of carrier access method is used by 802.11 devices?
    - **A.** CSMA/CD
    - **B.** Token passing
    - **C.** WAP
    - **D.** CSMA/CA

11. In which of the following technologies would MSAUs be used?
    - **A.** FDDI
    - **B.** IBM Token Ring
    - **C.** Ethernet
    - **D.** Wireless

12. Which of the following are the principle speeds of the IBM Token Ring technology? (Choose all that apply.)
    - **A.** 4Kbps
    - **B.** 16Mbps
    - **C.** 4Mbps
    - **D.** 8Mbps

13. In the term 100BASE-TX, the "T" represents which of the following?

A. Transmission speed

B. Terminal adapter

C. Twisted-pair cable

D. Twin direction signals

14. Which of following media types uses twisted-pair cable with an extra foil shield to guard against EMI?

A. Thinnet

B. Thicknet

C. UTP

D. STP

15. Which of the following devices converts LAN technologies to WAN technologies, and vice versa?

A. Router

B. Switch

C. Bridge

D. CSU/DSU

Answers to Review Questions

1. B. A star topology uses a hub as a central point of communication. A ring topology uses a multiple station access unit. A mesh topology does not have a central hub.

2. A. Ethernet uses the CSMA/CD carrier access method to communicate. Token Ring and FDDI use a token-passing method. Bus is a topology, not a technology.

3. D. The IEEE 802.11g wireless standard uses the 2.4GHz radio band to communicate at 54Mbps. The 802.11a standard uses the 5Ghz band to communicate at 54Mbps, but is not widely used. The 802.11b standard uses the 2.4GHz band to communicate at 11Mbps. 802.11x is the general name for the widely used family that uses DSSS on the 2.4GHz band.

4. C. The maximum distance the 100BASE-FX can transmit is 20 kilometers.

5. D. The registered jack that is used on most network devices is called RJ-45. An RJ-11 is used for normal telephone connections. Category 5 is a cable standard, not a registered jack. ST is a connector used for fiber-optic connections, and is not a registered jack connector.

6. C. IEEE 1394 is widely known as FireWire. 802.11x is the family of wireless standards that use 2.4GHz radio band and a DSSS method of transmission. Category 5e is a cable standard used for Gigabit Ethernet. 802.5 is the IEEE standard used for IBM Token Ring networks.

7. B. The maximum transmission speed for Category 5e cable is 1000Mbps (1Gbps).

8. D. A switch is the only device listed that can be used to segment a network and create VLANs. A bridge can be used to segment a network, but it cannot be used to create VLANs. A router can be used to segment a network, but also cannot be used to create VLANs. A hub can neither segment a network nor create VLANs.

9. A. Infrared wireless communication uses light and requires line of sight to operate properly. 802.11x uses the 2.4Ghz radio band. DSSS is a signaling method used by most 802.11x devices. 802.11g uses the 2.4GHz radio band.

10. D. 802.11 devices use the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method of carrier access. This means that they send a small signal to check media before they send the main signal. Token passing is used by ring networks. A wireless access point (WAP) is a transceiver device that is used with 802.11.

11. B. Multiple-station access units (MSAUs) are special hubs that are used in the Token Ring technology.

12. B, C. The two principle speeds of Token Ring are 4Mbps and 16Mbps. You must set the network card for the appropriate speed when you install it on a Token Ring network.

13. C. In terms such as 100BASE-TX the "T" always represents that twisted-pair cable is being used.

14. D. Shielded twisted-pair (STP) cable uses twisted-pair wires (as the name implies) with an extra foil shield to guard against electromagnetic interference (EMI). Thinnet and thicknet are coaxial cable types. Unshielded twisted pair (UTP) does not use a foil shield.

15. D. A CSU/DSU is a device that converts local area network (LAN) technologies to wide area network (WAN) technologies, and vice versa. Routers are used in LAN and WAN environments, but are not converters. Switches and bridges are primarily used in a LAN environment and are not converters.