Part 2

Planning

Chapter 3
Transmission Media

On any network, the various entities must communicate through some form of media. Just as humans can communicate through telephone wires or sound waves in the air, computers can communicate through cables, light, and radio waves. Transmission media enable computers to send and receive messages but do not guarantee that the messages will be understood.

This chapter discusses some of the most common network transmission media, such as coaxial cable, shielded twisted-pair cable, and unshielded twisted-pair cable. You also learn about network fiber-optic cable and wireless communications. To lay the groundwork for these issues, the chapter begins with an introduction to radio frequency transmissions and a look at some important characteristics of transmission media.

This chapter targets one multipart objective in the Planning section of the Networking Essentials exam:

Test Objectives

- Select the appropriate media for various situations. Media choices include the following:
  - Twisted-pair cable
  - Coaxial cable
  - Fiber-optic cable
  - Wireless communications
- Situational elements include the following:
  - Cost
  - Distance limitations
  - Number of nodes

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

1. The maximum range for Thicknet cable is approximately _____.

   A. 100 m
   B. 185 m
   C. 500 m
   D. 1000 m

2. The _____ is commonly used to connect coaxial Thinnet cable.

   A. N-connector
   B. DB-15
   C. RJ-45
   D. BNC

3. Which of the following cabling types is most expensive to install?

   A. Fiber-optic
   B. Unshielded twisted-pair
   C. Shielded twisted-pair
   D. Coaxial Thicknet

4. _____ is a technique for systematically switching frequencies in the middle of a spread-spectrum transmission.

   A. Frequency shifting
   B. Frequency switching
   C. Frequency hopping
   D. Frequency shopping

Transmission Media Types

The most common type of media is copper cable. The most common types of copper cabling are twisted-pair and coaxial. *Twisted-pair* cabling used in a LAN is similar to the cabling used to connect your telephone to the wall outlet. Network *coaxial* cabling, on the other hand, is similar to the cable used to connect your television set to the cable TV outlet.

Another type of LAN connection media quickly gaining popularity is fiber-optic cable. Consisting of a number of glass or high-grade plastic optical strands surrounded by a tough cloth-and-plastic wrap, *fiber-optic cables* resemble coaxial cables from the outside. Fiber-optic network cabling is similar to the fiber-optic strand used in the fiber-optic lamps found in novelty stores, in which colored lights feed into optical strands to create the appearance of dozens of pinpoints of light.

Wireless media, which is, in a sense, no media at all, is also gaining popularity. Wireless transmissions use radio waves or infrared light to transmit data. Many major network vendors now offer wireless network adapters.

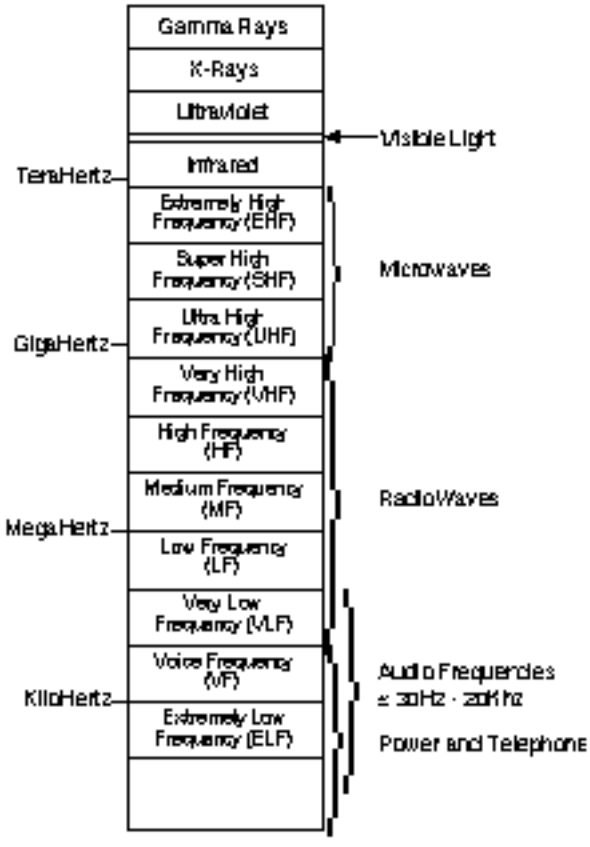
Transmission Frequencies

Transmission media make possible the transmission of the electronic signals from one computer to another computer. These electronic signals express data values in the form of binary (on/off) impulses. The signals are transmitted through the network using a combination of electronic devices (such as network boards and hubs) and transmission media (such as cables and radio) until they reach the desired destination computer.

All signals transmitted between computers consist of some form of electromagnetic (EM) waveform, ranging from radio frequencies through microwave and infrared light. Different media are used to transmit the signals, depending on the frequency of the EM waveform. Figure 3.1 illustrates the range of electromagnetic waveforms (known as the electromagnetic spectrum) and their associated frequencies.

Figure 3.1

The electromagnetic spectrum.



The electromagnetic spectrum consists of several categories of waveforms, including radio frequency waves, microwave transmissions, and infrared light.

Radio frequency waves often are used for LAN signaling. Radio frequencies can be transmitted across electrical cables (twisted-pair or coaxial) or by using radio broadcast transmission.

Microwave transmissions can be used for tightly focused transmissions between two points. Microwaves are used to communicate between Earth stations and satellites, for example, and they also are used for line-of-sight transmissions on the earth's surface. In addition, microwaves can be used in low-power forms to broadcast signals from a transmitter to many receivers. Cellular phone networks are examples of systems that use low-power microwave signals to broadcast signals.

Infrared light is ideal for many types of network communications. Infrared light can be transmitted across relatively short distances and can be either beamed between two points or broadcast from one point to many receivers. Infrared and higher frequencies of light also can be transmitted through fiber-optic cables.

The next sections examine examples of network transmission media and describe the advantages and disadvantages of each media type.

Characteristics of Transmission Media

Each type of transmission media has special characteristics that make it suitable for a specific type of service. You should be familiar with these characteristics:

- Cost
- Installation requirements
- Bandwidth
- Band Usage (Baseband or Broadband)
- Attenuation
- Immunity from electromagnetic interference

The last four characteristics require some explanation. The following sections introduce you to bandwidth, transmission type, attenuation, and electromagnetic interference.

Bandwidth

In computer networking, the term *bandwidth* refers to the measure of the capacity of a medium to transmit data. A medium that has a high capacity, for example, has a high bandwidth, whereas a medium that has limited capacity has a low bandwidth.

Bandwidth can be best understood by using an analogy to water hoses. If a half-inch garden hose can carry waterflow from a trickle up to two gallons per minute, then that hose can be said to

have a bandwidth of two gallons per minute. A four-inch fire hose, however, might have a bandwidth that exceeds 100 gallons per minute.

Data transmission rates frequently are stated in terms of the bits that can be transmitted per second. An Ethernet LAN theoretically can transmit 10 million bits per second and has a bandwidth of 10 megabits per second (Mbps).

The bandwidth that a cable can accommodate is determined in part by the cable's length. A short cable generally can accommodate greater bandwidth than a long cable, which is one reason all cable designs specify maximum lengths for cable runs. Beyond those limits, the highest-frequency signals can deteriorate, and errors begin to occur in data signals.

The term *bandwidth* also has another meaning. In the communications industry, bandwidth refers to the range of available frequencies between the lower frequency limit and the upper frequency limit. Frequencies are measured in Hertz (Hz), or cycles per second. The bandwidth of a voice telephone line is 400–4,000 Hz, which means that the line can transmit signals with frequencies ranging from 400 to 4,000 cycles per second.

Band Usage (Baseband or Broadband)

The two ways to allocate the capacity of transmission media are with baseband and broadband transmissions. *Baseband* devotes the entire capacity of the medium to one communication channel. *Broadband* enables two or more communication channels to share the bandwidth of the communications medium.

Baseband is the most common mode of operation. Most LANs function in baseband mode, for example. Baseband signaling can be accomplished with both analog and digital signals.

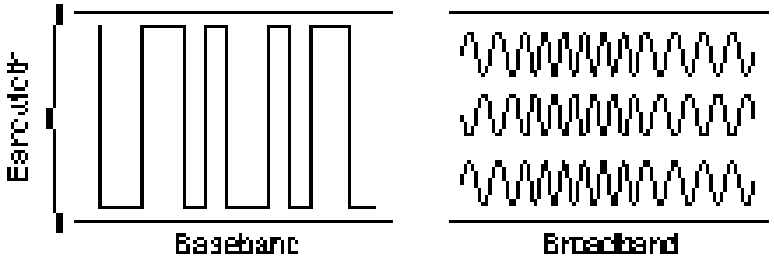
Although you might not realize it, you have a great deal of experience with broadband transmissions. Consider, for example, that the TV cable coming into your house from an antenna or a cable provider is a broadband medium. Many television signals can

share the bandwidth of the cable because each signal is modulated using a separately assigned frequency. You can use the television tuner to choose the channel you want to watch by selecting its frequency. This technique of dividing bandwidth into frequency bands is called *frequency-division multiplexing (FDM)* and works only with analog signals. Another technique, called *time-division multiplexing (TDM),* supports digital signals.

Figure 3.2 contrasts the difference between baseband and broadband modes of operation.

Figure 3.2

Baseband and broadband transmission modes.



Multiplexing

Multiplexing is a technique that enables broadband media to support multiple data channels. Multiplexing makes sense under a number of circumstances:

- **When media bandwidth is costly.** A high-speed leased line, such as a T1 or T3, is expensive to lease. If the leased line has sufficient bandwidth, multiplexing can enable the same line to carry mainframe, LAN, voice, video conferencing, and various other data types.
- **When bandwidth is idle.** Many organizations have installed fiber-optic cable that is used only to partial capacity. With the proper equipment, a single fiber can support hundreds of megabits—or even a gigabit or more—of data.
- **When large amounts of data must be transmitted through low-capacity channels.** Multiplexing techniques can divide the original data stream into several lower-bandwidth channels, each of which can be transmitted through a lower-capacity medium. The signals then can be recombined at the receiving end.

Multiplexing refers to combining multiple data channels for transmission on a common medium. *Demultiplexing* refers to recovering the original separate channels from a multiplexed signal.

Multiplexing and demultiplexing are performed by a multiplexor (also called a *mux*), which usually has both capabilities.

Frequency-Division Multiplexing

Figure 3.3 illustrates frequency-division multiplexing (FDM). This technique works by converting all data channels to analog form. Each analog signal can be modulated by a separate frequency (called a *carrier frequency*) that makes it possible to recover that signal during the demultiplexing process. At the receiving end, the demultiplexor can select the desired carrier signal and use it to extract the data signal for that channel.

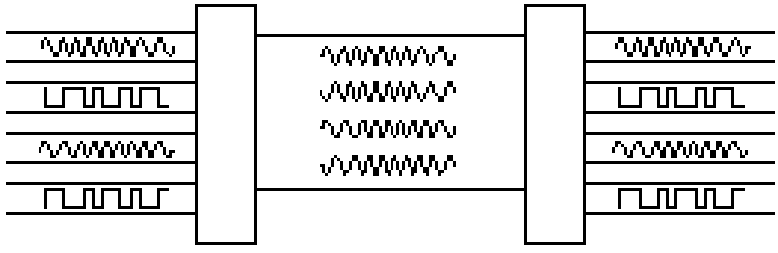


Figure 3.3

Frequency-division multiplexing.

FDM can be used in broadband LANs (a standard for Ethernet also exists). One advantage of FDM is that it supports bidirectional signaling on the same cable.

Time-Division Multiplexing

Time-division multiplexing (TDM) divides a channel into time slots that are allocated to the data streams to be transmitted, as illustrated in figure 3.4. If the sender and receiver agree on the time-slot assignments, the receiver can easily recover and reconstruct the original data streams.

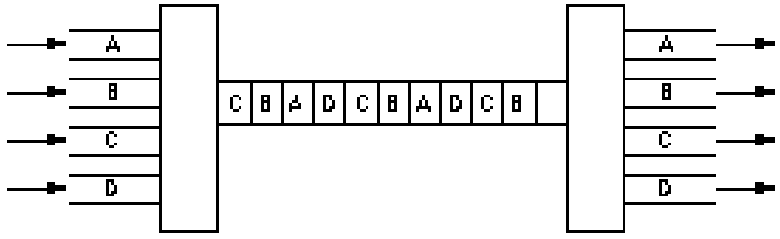


Figure 3.4

Time-division multiplexing creates time slots within the channel for the data streams.

TDM transmits the multiplexed signal in baseband mode. Interestingly, this process makes it possible to multiplex a TDM multiplexed signal as one of the data channels on an FDM system.

Conventional TDM equipment utilizes fixed-time divisions and allocates time to a channel, regardless of that channel's level of activity. If a channel isn't busy, its time slot isn't being fully utilized. Because the time divisions are programmed into the configurations of the multiplexors, this technique often is referred to as *synchronous TDM.*

If using the capacity of the data medium more efficiently is important, a more sophisticated technique, *statistical time-division multiplexing (StatTDM*), can be used. *A stat-mux* uses the time-slot technique but allocates time slots based on the traffic demand on the individual channels, as illustrated in figure 3.5. Notice that Channel B is allocated more time slots than Channel A, and that Channel C is allocated the fewest time slots. Channel D is idle, so no slots are allocated to it. To make this procedure work, the data transmitted for each time slot includes a control field that identifies the channel to which the data in the time slot should be assigned.

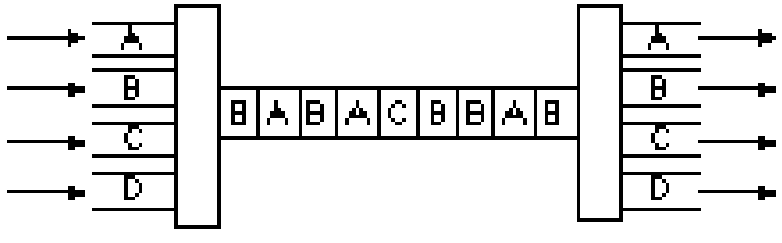


Figure 3.5

Statistical time-division multiplexing allocates time slots based on channels' traffic demand.

Attenuation

Attenuation is a measure of how much a signal weakens as it travels through a medium. This book doesn't discuss attenuation in formal terms, but it does address the impact of attenuation on performance.

Attenuation is a contributing factor to why cable designs must specify limits in the lengths of cable runs. When signal strength falls below certain limits, the electronic equipment that receives the signal can experience difficulty isolating the original signal from the noise present in all electronic transmissions. The effect is exactly like trying to tune in distant radio signals. Even if you can lock on to the signal on your radio, the sound generally still contains more noise than the sound for a local radio station.

Electromagnetic Interference

Electromagnetic interference (EMI) consists of outside electromagnetic noise that distorts the signal in a medium. When you listen to an AM radio, for example, you often hear EMI in the form of noise caused by nearby motors or lightning. Some network media are more susceptible to EMI than others.

Crosstalk is a special kind of interference caused by adjacent wires. Crosstalk is a particularly significant problem with computer networks because large numbers of cables often are located close together with minimal attention to exact placement.

Cable Media

For the Networking Essentials exam, you need to know how to make decisions about network transmission media based on some of the factors described in previous sections of this chapter. The following sections discuss three types of network cabling media, as follows:

- Coaxial cable
- Twisted-pair cable
- Fiber-optic cable

Later in this chapter, you learn about some of the wireless communication forms.

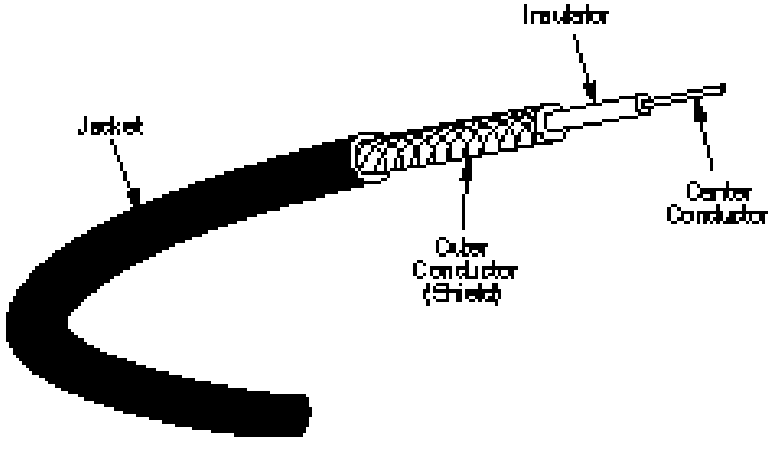
Some large networks use combinations of media. When you mix and match different types of media, difficulties can arise, largely because mixed media require a greater level of expertise and training on the part of the network support staff. As the number of media types increases, your own responsibilities increase—when a problem arises on the LAN, the number of areas you must investigate increases dramatically when mixed transmission media are involved.

Coaxial Cable

Coaxial cables were the first cable types used in LANs. As shown in figure 3.6, coaxial cable gets its name because two conductors share a common axis; the cable is most frequently referred to as a *coax*.

Figure 3.6

The structure of coaxial cable consists of four main components.



The components of a coaxial cable are as follows:

- A *center conductor*, although usually solid copper wire, sometimes is made of stranded wire.
- An *outer conductor* forms a tube surrounding the center conductor. This conductor can consist of braided wires, metallic

foil, or both. The outer conductor, frequently called the *shield*, serves as a ground and also protects the inner conductor from EMI.

- An *insulation layer* keeps the outer conductor spaced evenly from the inner conductor.
- A plastic encasement (*jacket*) protects the cable from damage.

Types of Coaxial Cable

The two basic classifications for coaxial cable are as follows:

- Thinnet
- Thicknet

The following sections discuss thinnet and thicknet coaxial cabling.

Thinnet

Thinnet is a light and flexible cabling medium that is inexpensive and easy to install. Table 3.1 illustrates some Thinnet classifications. Note that Thinnet falls under the RG-58 family, which has a 50-Ohm impedance. Thinnet is approximately .25 inches (6 mm) in thickness.

All coaxial cables have a characteristic measurement called impedance, which is measured in ohms. *Impedance* is a measure of the apparent resistance to an alternating current. You must use a cable that has the proper impedance in any given situation.

Table 3.1

Thinnet Cable Classifications

Cable	Description	Impedance
RG-58/U	Solid copper center	50-Ohm
RG-58 A/U	Wire strand center	50-Ohm
RG-58 C/U	Military version of RG-58 A/U	50-Ohm

Thinnet cable can reliably transmit a signal for 185 meters (about 610 feet).

Thicknet

Thicknet—big surprise—is thicker than Thinnet. Thicknet coaxial cable is approximately 0.5 inches (13 mm) in diameter. Because it is thicker and does not bend as readily as Thinnet, Thicknet cable is harder to work with. A thicker center core, however, means that Thicknet can carry more signals a longer distance than Thinnet. Thicknet can transmit a signal approximately 500 meters (1650 feet).

Thicknet cable is sometimes called *Standard Ethernet* (although other cabling types described in this chapter are used for Ethernet also). Thicknet can be used to connect two or more small Thinnet LANs into a larger network.

Because of its greater size, Thicknet is also more expensive than Thinnet. Thicknet can be installed safely outside, running from building to building.

Coaxial Characteristics

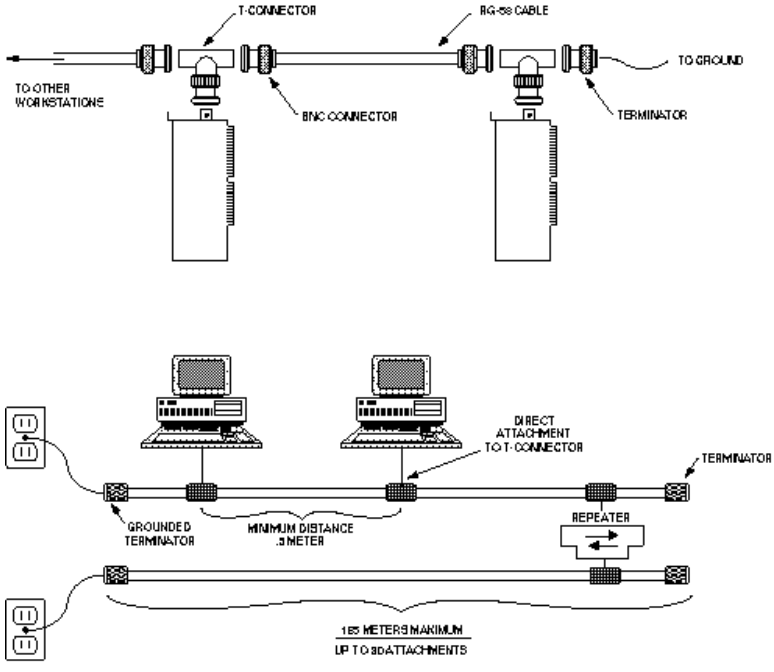
You should be familiar with the installation, cost, bandwidth, and EMI resistance characteristics of coaxial cable. The following sections discuss some of the characteristics of coaxial cable.

Installation

Coaxial cable typically is installed in two configurations: daisy-chain (from device to device—Ethernet) and star (ARCnet). Both are shown in figure 3.7.

Figure 3.7

Coaxial cable wiring configurations.



The Ethernet cabling shown in the figure is an example of Thinnet, which uses RG-58 type cable. Devices connect to the cable by means of *T-connectors*. Cables are used to provide connections between *T-connectors*. One characteristic of this type of cabling is that the ends of the cable run must be terminated by a special connector, called a *terminator*. The terminator contains a resistor that is matched to the characteristics of the cable. The resistor prevents signals that reach the end of the cable from bouncing back and causing interference.

Coaxial cable is reasonably easy to install because the cable is robust and difficult to damage. In addition, connectors can be installed with inexpensive tools and a bit of practice. The device-to-device cabling approach can be difficult to reconfigure, however, when new devices cannot be installed near an existing cabling path.

Cost

The coaxial cable used for Thinnet falls at the low end of the cost spectrum, whereas Thicknet is among the more costly options. Detailed cost comparisons are made later in this chapter in the section titled "Summary of Cable Characteristics."

Bandwidth

LANs that employ coaxial cable typically have a bandwidth between 2.5 Mbps (ARCnet) and 10 Mbps (Ethernet). Thicker coaxial cables offer higher bandwidth, and the potential bandwidth of coaxial is much higher than 10 Mbps. Current LAN technologies, however, don't take advantage of this potential.

EMI Characteristics

All copper media are sensitive to EMI, although the shield in coax makes the cable fairly resistant. Coaxial cables, however, do radiate a portion of their signal, and electronic eavesdropping equipment can detect this radiated signal.

Connectors for Coaxial Cable

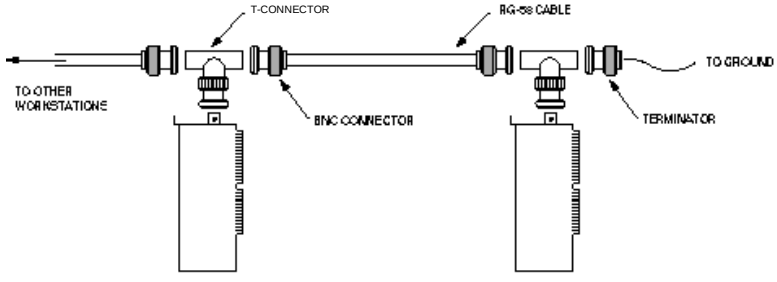
Two types of connectors are commonly used with coaxial cable. The most common is the *British Naval Connector (BNC)*. Figure 3.8 depicts the following characteristics of BNC connectors and Thinnet cabling:

- A BNC T-connector connects the network board in the PC to the network. The T-connector attaches directly to the network board.
- BNC cable connectors attach cable segments to the T-connectors.
- A BNC barrel connector connects to Thinnet cables.

- Both ends of the cable must be terminated. A BNC terminator is a special connector that includes a resistor that is carefully matched to the characteristics of the cable system.
- One of the terminators must be grounded. A wire from the connector is attached to a grounded point, such as the center screw of a grounded electrical outlet.

Figure 3.8

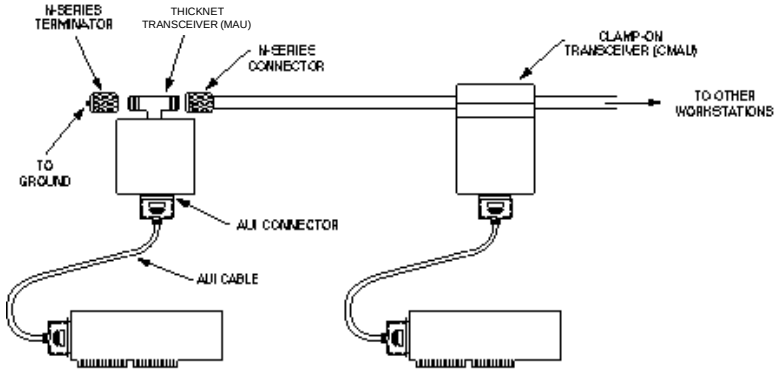
Thinnet uses BNC T-connectors .



In contrast, Thicknet uses *N-connectors*, which screw on instead of using a twist-lock (see fig. 3.9). As with Thinnet, both ends of the cable must be terminated, and one end must be grounded.

Figure 3.9

Connectors and cabling for Thicknet.



Workstations don't connect directly to the cable with Thicknet. Instead, a connecting device called a *transceiver* is attached to the Thicknet cable. This transceiver has a port for an *AUI connector*, and an *AUI cable* (also called a *transceiver cable* or a *drop cable*) connects the workstation to the Thicknet medium. Transceivers can connect to Thicknet cables in the following two ways:

- Transceivers can connect by cutting the cable and using N-connectors and a T-connector on the transceiver. As a result, the original method now is used rather infrequently.
- The more common approach is to use a clamp-on transceiver, which has pins that penetrate the cable without the need for cutting it. Because clamp-on transceivers force sharp teeth into the cable, they frequently are referred to as *vampire taps*.

You can use a transceiver to connect a Thinnet LAN to a Thicknet backbone.

AUI port connectors sometimes are called DIX connectors or DB-15 connectors.

Coax and Fire Code Classifications

The space above a drop ceiling (between the ceiling and the floor of a building's next level) is extremely significant to both network administrators and fire marshals. This space (called the *plenum*—see fig. 3.10) is a convenient place to run network cables around a building. The plenum, however, is typically an open space in which air circulates freely, and, consequently, fire marshals pay special attention to it.

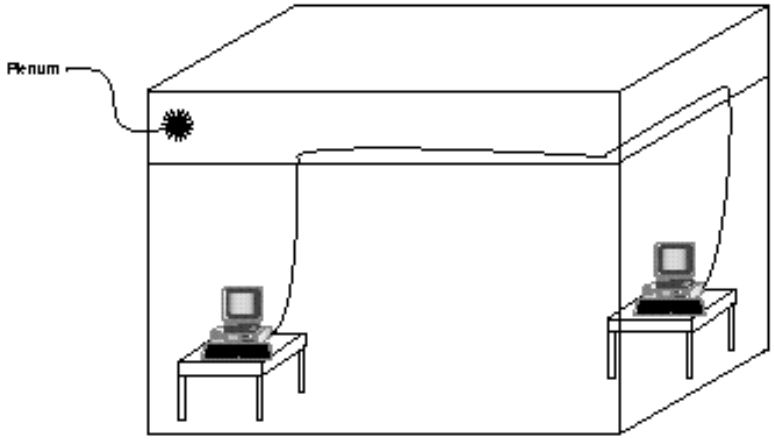


Figure 3.10

The plenum—the space between the ceiling of one room and the floor of the level above—is often a convenient spot for network cabling.

The most common outer covering for coaxial cabling is *polyvinyl chloride (PVC)*. PVC cabling gives off poisonous fumes when it burns. For that reason, fire codes prohibit PVC cabling in the plenum because poisonous fumes in the plenum can circulate freely throughout the building.

Plenum-grade coaxial cabling is specially designed to be used without conduit in plenums, walls, and other areas where fire codes prohibit PVC cabling. Plenum-grade cabling is less flexible and more expensive than PVC cabling, so it is used primarily where PVC cabling can't be used.

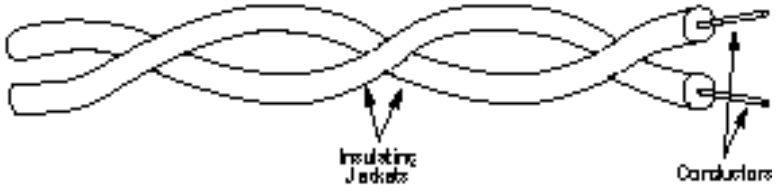
Twisted-Pair Cable

Twisted-pair cable has become the dominant cable type for all new network designs that employ copper cable. Among the several reasons for the popularity of twisted-pair cable, the most significant is its low cost. Twisted-pair cable is inexpensive to install and offers the lowest cost per foot of any cable type.

A basic twisted-pair cable consists of two strands of copper wire twisted together (see fig. 3.11). This twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components. This is because the radiated signals from the twisted wires tend to cancel each other out. (Antennas, which are purposely designed to radiate radio frequency signals, consist of parallel, not twisted, wires.)

Figure 3.11

Twisted-pair cable.



Twisting also controls the tendency of the wires in the pair to cause EMI in each other. Whenever two wires are in close proximity, the signals in each wire tend to produce noise, called crosstalk, in the other. Twisting the wires in the pair reduces crosstalk in much the same way that twisting reduces the tendency of the wires to radiate EMI.

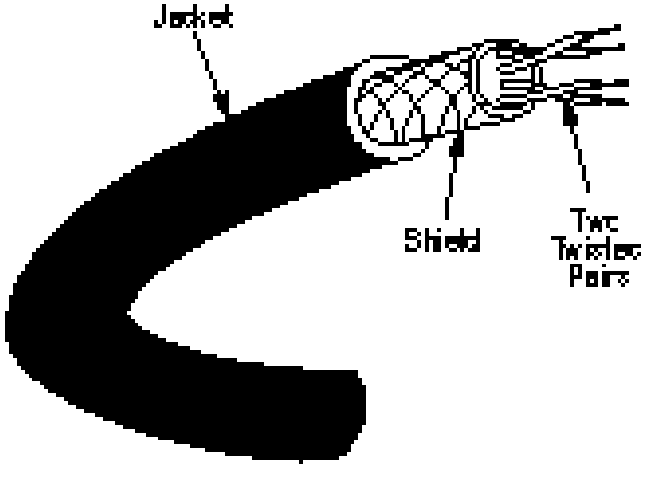
Two types of twisted-pair cable are used in LANs: *shielded* and *unshielded.*

Shielded Twisted-Pair (STP) Cable

Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding. Figure 3.12 shows IBM Type 1 cabling, the first cable type used with IBM Token Ring. Early LAN designers used shielded twisted-pair cable because the shield further reduces the tendency of the cable to radiate EMI and thus reduces the cable's sensitivity to outside interference.

Figure 3.12

A shielded twisted-pair cable.



Coaxial and STP cables use shields for the same purpose. The shield is connected to the ground portion of the electronic device to which the cable is connected. A *ground* is a portion of the device that serves as an electrical reference point, and usually, it literally is connected to a metal stake driven into the ground. A properly grounded shield prevents signals from getting into or out of the cable.

As shown in figure 3.12, IBM Type 1 cable includes two twisted pairs of wire within a single shield. Various types of STP cable exist, some that shield each pair individually and others that shield several pairs. The engineers who design a network's cabling system choose the exact configuration. IBM designates several twisted-pair cable types to use with their Token Ring network design, and each cable type is appropriate for a given kind of installation. A completely different type of STP is the standard cable for Apple's AppleTalk network.

Because so many different types of STP cable exist, stating precise characteristics is difficult. The following sections, however, offer some general guidelines.

Cost

STP cable costs more than thin coaxial or unshielded twisted-pair cable. STP is less costly, however, than thick coax or fiber-optic cable.

Installation

Naturally, different network types have different installation requirements. One major difference is the connector used. Apple LocalTalk connectors generally must be soldered during installation, a process that requires some practice and skill on the part of the installer. IBM Token Ring uses a so-called unisex data connector (the connectors are both male and female), which can be installed with such common tools as a knife, a wire stripper, and a large pair of pliers.

In many cases, installation can be greatly simplified by using prewired cables. You must learn to install the required connectors, however, when your installation requires the use of bulk cable.

Most connectors require two connector types to complete a connection. The traditional designation for connector types is male and female. The male connector is the connector with pins, and the female connector has receptacles into which the pins insert. In a standard AC wall outlet, for example, the outlet itself is female and the plug on the line cord is male.

These designations originated when electrical installation was a male province, so the terms male and female gradually are being replaced. A commonly used alternative is "pins and sockets."

The IBM data connector is called a unisex connector because the connector has both pins and sockets. Any IBM data connector can connect to any other IBM data connector.

STP cable tends to be rather bulky. IBM Type 1 cable is approximately $^1/_2$ inch (13 mm) in diameter. Therefore, it can take little time to fill up cable paths with STP cables.

Capacity

STP cable has a theoretical capacity of 500 Mbps, although few implementations exceed 155 Mbps with 100-meter cable runs. The most common data rate for STP cable is 16 Mbps, which is the top data rate for Token Ring networks.

Attenuation

All varieties of twisted-pair cable have attenuation characteristics that limit the length of cable runs to a few hundred meters, although a 100-meter limit is most common.

EMI Characteristics

The shield in STP cable results in good EMI characteristics for copper cable, comparable to the EMI characteristics of coaxial cable. This is one reason STP might be preferred to unshielded twisted-pair cable in some situations. As with all copper cables, STP is sensitive to interference and vulnerable to electronic eavesdropping.

Connectors for STP

AppleTalk and Token Ring networks can be cabled using UTP cable and RJ-45 connectors (described later in this chapter), but both networks originated as STP cabling systems. For STP cable, AppleTalk employs a DIN-type connector, shown in figure 3.13. IBM, on the other hand, uses the IBM Data Connector, as shown in figure 3.14.

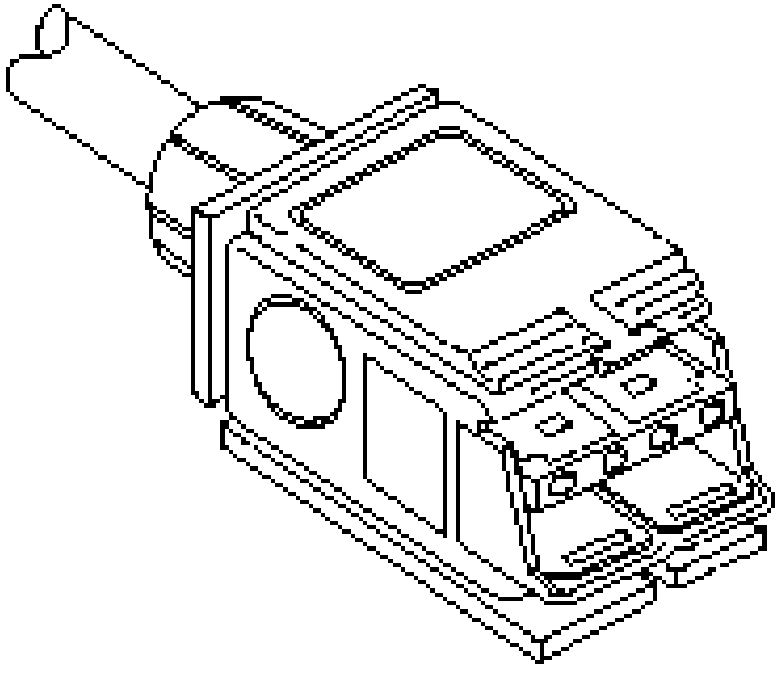
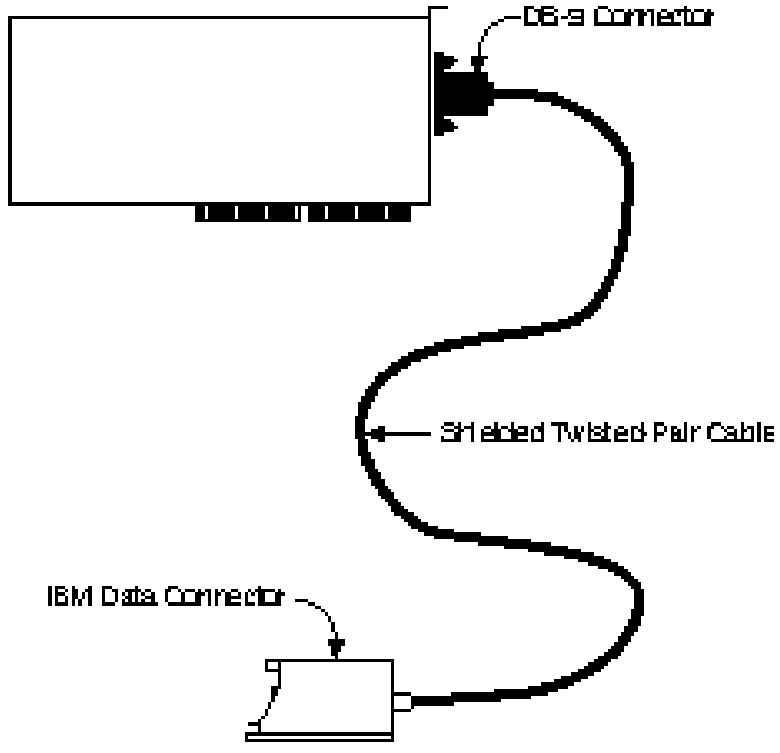


Figure 3.13

Connectors used with STP cable.

Figure 3.14

A PC ready to connect to a Token Ring network.



The IBM Data Connector is unusual because it doesn't come in two gender configurations. Instead, any IBM Data Connector can be snapped to any other IBM Data Connector. The IBM cabling system is discussed later in this chapter.

Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair cable doesn't incorporate a braided shield into its structure. However, the characteristics of UTP are similar in many ways to STP, differing primarily in attenuation and EMI. As shown in figure 3.15, several twisted-pairs can be bundled together in a single cable. These pairs typically are color coded to distinguish them.

Telephone systems commonly use UTP cabling. Network engineers can sometimes use existing UTP telephone cabling (if it is new enough and of a high enough quality to support network communications) for network cabling.

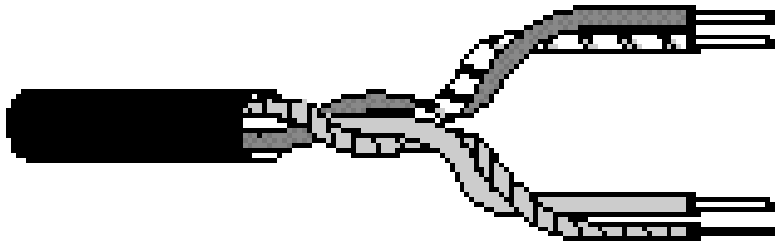


Figure 3.15
A multipair UTP cable.

UTP cable is a latecomer to high-performance LANs because engineers only recently solved the problems of managing radiated noise and susceptibility to EMI. Now, however, a clear trend toward UTP is in operation, and all new copper-based cabling schemes are based on UTP.

UTP cable is available in the following five grades, or categories:

- **Categories 1 and 2.** These voice-grade cables are suitable only for voice and for low data rates (below 4 Mbps). Category 1 was once the standard voice-grade cable for telephone systems. The growing need for data-ready cabling systems, however, has caused Categories 1 and 2 cable to be supplanted by Category 3 for new installations.
- **Category 3.** As the lowest data-grade cable, this type of cable generally is suited for data rates up to 10 Mbps. Some innovative schemes, however, enable the cable to support data rates up to 100 Mbps. Category 3, which uses four twisted-pairs with three twists per foot, is now the standard cable used for most telephone installations.
- **Category 4.** This data-grade cable, which consists of four twisted-pairs, is suitable for data rates up to 16 Mbps.
- **Category 5.** This data-grade cable, which also consists of four twisted-pairs, is suitable for data rates up to 100 Mbps. Most new cabling systems for 100 Mbps data rates are designed around Category 5 cable.

In a UTP cabling system, the cable is only one component of the system. All connecting devices also are graded, and the overall cabling system supports only the data rates permitted by the lowest-grade component in the system. In other words, if you require a Category 5 cabling system, all connectors and connecting devices must be designed for Category 5 operation.

Category 5 cable also requires more stringent installation procedures than the lower cable categories. Installers of Category 5 cable require special training and skills to understand these more rigorous requirements.

UTP cable offers an excellent balance of cost and performance characteristics, as discussed in the following sections.

Cost

UTP cable is the least costly of any cable type, although properly installed Category 5 tends to be fairly expensive. In some cases, existing cable in buildings can be used for LANs, although you should verify the category of the cable and know the length of the cable in the walls. Distance limits for voice cabling are much less stringent than for data-grade cabling.

Installation

UTP cable is easy to install. Some specialized equipment might be required, but the equipment is low in cost and can be mastered with a bit of practice. Properly designed UTP cabling systems easily can be reconfigured to meet changing requirements.

As noted earlier, however, Category 5 cable has stricter installation requirements than lower categories of UTP. Special training is recommended for dealing with Category 5 UTP.

Capacity

The data rates possible with UTP have pushed up from 1 Mbps, past 4 and 16 Mbps, to the point where 100 Mbps data rates are now common.

Attenuation

UTP cable shares similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters as the most frequent limit.

EMI Characteristics

Because UTP cable lacks a shield, it is more sensitive to EMI than coaxial or STP cables. The latest technologies make it possible to use UTP in the vast majority of situations, provided that reasonable care is taken to avoid electrically noisy devices such as motors and fluorescent lights. Nevertheless, UTP might not be suitable for noisy environments such as factories. Crosstalk between nearby unshielded pairs limits the maximum length of cable runs.

Connectors for UTP

The most common connector used with UTP cables is the *RJ-45 connector*, shown in figure 3.16. These connectors are easy to install on cables and are also extremely easy to connect and disconnect. An RJ-45 connector has eight pins and looks like a common RJ-11 telephone jack. They are slightly different sizes and won't fit together: an RJ-11 has only four pins.

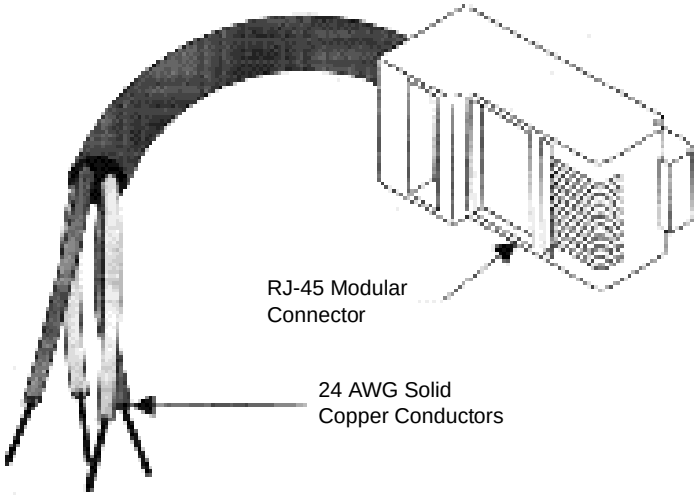


Figure 3.16
An RJ-45 connector.

Distribution racks, shelves, and patch panels are available for large UTP installations. These accessories enable you to organize network cabling and also provide a central spot for expansion and reconfiguration. One necessary accessory, a *jack coupler*, is a small device that attaches to a wall plate or a patch panel and receives an RJ-45 connection. Jack couplers can support transmission speeds of up to 100 Mbps.

Fiber-Optic Cable

In almost every way, fiber-optic cable is the ideal cable for data transmission. Not only does this type of cable accommodate extremely high bandwidths, but it also presents no problems with EMI and supports durable cables and cable runs as long as several kilometers. The two disadvantages of fiber-optic, however, are cost and installation difficulty.

The center conductor of a fiber-optic cable is a fiber that consists of highly refined glass or plastic designed to transmit light signals with little loss. A glass core supports a longer cabling distance, but a plastic core is typically easier to work with. The fiber is coated with a cladding that reflects signals back into the fiber to reduce signal loss. A plastic sheath protects the fiber. See figure 3.17.

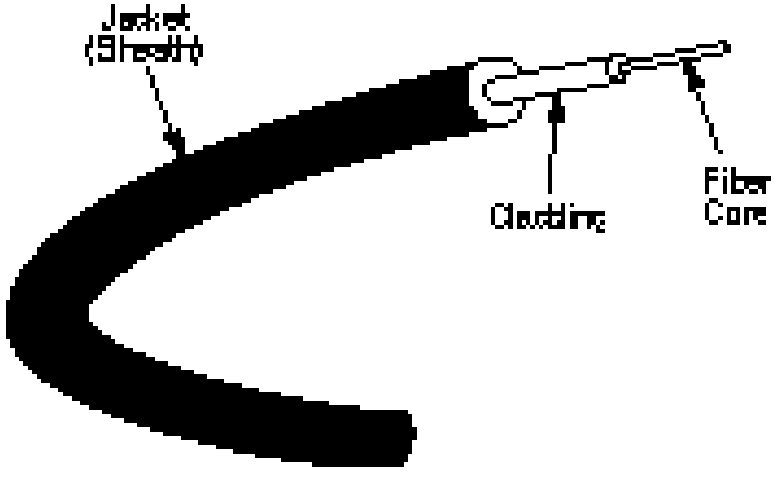


Figure 3.17
A fiber-optic cable.

A fiber-optic network cable consists of two strands separately enclosed in plastic sheaths—one strand sends and the other receives. Two types of cable configurations are available: loose and tight configurations. Loose configurations incorporate a space between the fiber sheath and the outer plastic encasement; this space is filled with a gel or other material. Tight configurations contain strength wires between the conductor and the outer plastic encasement. In both cases, the plastic encasement must supply the strength of the cable, while the gel layer or strength wires protect the delicate fiber from mechanical damage.

Optical fiber cables don't transmit electrical signals. Instead, the data signals must be converted into light signals. Light sources include lasers and light-emitting diodes (LEDs). LEDs are inexpensive but produce a fairly poor quality of light suitable for less-stringent applications.

A *laser* is a light source that produces an especially pure light that is monochromatic (one color) and coherent (all waves are parallel). The most commonly used source of laser light in LAN devices is called an *injection laser diode (ILD).* The purity of laser light makes lasers ideally suited to data transmissions because they can work with long distances and high bandwidths. Lasers, however, are expensive light sources used only when their special characteristics are required.

The end of the cable that receives the light signal must convert the signal back to an electrical form. Several types of solid-state components can perform this service.

One of the significant difficulties of installing fiber-optic cable arises when two cables must be joined. The small cores of the two cables (some are as small as 8.3 microns) must be lined up with extreme precision to prevent excessive signal loss.

Fiber-Optic Characteristics

As with all cable types, fiber-optic cables have their share of advantages and disadvantages.

Cost

The cost of the cable and connectors has fallen significantly in recent years. However, the electronic devices required are significantly more expensive than comparable devices for copper cable. Fiber-optic cable is also the most expensive cable type to install.

Installation

Greater skill is required to install fiber-optic cable than to install most copper cables. Improved tools and techniques, however, have reduced the training required. Still, fiber-optic cable requires greater care because the cables must be treated fairly gently during installation. Every cable has a minimum bend radius, for example, and fibers are damaged if the cables are bent too sharply. It also is important not to stretch the cable during installation.

Capacity

Fiber-optic cable can support high data rates (as high as 200,000 Mbps) even with long cable runs. Although UTP cable runs are limited to less than 100 meters with 100 Mbps data rates, fiber-optic cables can transmit 100 Mbps signals for several kilometers.

Attenuation

Attenuation in fiber-optic cables is much lower than in copper cables. Fiber-optic cables are capable of carrying signals for several kilometers.

EMI Characteristics

Because fiber-optic cables don't use electrical signals to transmit data, they are totally immune to electromagnetic interference. The cables also are immune to a variety of electrical effects that must be taken into account when designing copper cabling systems.

When electrical cables are connected between two buildings, the ground potentials (voltages) between the two buildings can differ. When a difference exists (as it frequently does), the current flows through the grounding conductor of the cable, even though the ground is supposed to be electrically neutral and no current should flow. When current flows through the ground conductor of a cable, the condition is called a *ground loop*. Ground loops can result in electrical instability and various other types of anomalies.

Because fiber-optic cable is immune to electrical effects, the best way to connect networks in different buildings is by putting in a fiber-optic link segment.

Because the signals in fiber-optic cable are not electrical in nature, they cannot be detected by the electronic eavesdropping equipment that detects electromagnetic radiation. Therefore, fiber-optic cable is the perfect choice for high-security networks.

Summary of Cable Characteristics

Table 3.2 summarizes the characteristics of the four cable types discussed in this section.

Table 3.2

Comparison of Cable Media

Cable Type	Cost	Installation	Capacity	Range	EMI
Coaxial Thinnet	<STP	Inexpensive/ easy	10 Mbps typical	185 m	<sensitive than UTP
Coaxial Thicknet	>STP <Fiber	Easy	10 Mbps typical	500 m	<sensitive than UTP
Shielded Twisted-Pair (STP)	>UTP <Thicknet	Fairly easy	16 Mbps typical up to 500 Mbps	100 m typical	<sensitive than UTP

Cable Type	Cost	Installation	Capacity	Range	EMI
Unshielded Twisted-Pair (UTP)	Lowest	Inexpensive/ easy	10 Mbps typical up to 100 Mbps	100 m typical	Most sensitive
Fiber-Optic	Highest	Expensive/ difficult	100 Mbps typical	10s of kilometers	Insensitive

When comparing cabling types, remember that the characteristics you observe depend highly on the implementations. Engineers once thought that UTP cable would never reliably support data rates above 4 Mbps, but 100 Mbps data rates now are common.

Some comparisons between cable types are fairly involved. For example, although fiber-optic cable is costly on a per-foot basis, you can construct a fiber-optic cable that is many kilometers in length. To build a copper cable many kilometers in length, you need to install repeaters at several points along the cable to amplify the signal. These repeaters could easily exceed the cost of a fiber-optic cable run.

IBM Cabling

IBM assigns separate names, standards, and specifications for network cabling and cabling components. These IBM cabling types roughly parallel standard forms used elsewhere in the industry, as table 3.3 illustrates. The AWG designation in this table stands for the American Wire Gauge standard, a specification for wire gauges. The higher the gauge, the thinner the wire.

IBM provides a unique connector (mentioned earlier in this chapter) that is of both genders—any two of the same type can be connected together.

Table 3.3

IBM Cabling Types

Cable Type	Description	Comment
Type 1	Shielded twisted-pair (STP)	Two twisted-pairs of 22 AWG wire in braided shield
Type 2	Voice and data	Two twisted-pairs of 22 AWG wire for data and braided shield, and two twisted-pairs of 26 AWG for voice
Type 3	Voice	Four solid UTP pairs; 22 or 24 AWG wire
Type 4	Not defined	
Type 5	Fiber-optic	Two 62.5/125-micron multi-mode fibers
Type 6	Data patch cable	Two twisted-pairs of 26 AWG wire, dual foil, and braided shield
Type 7	Not defined	
Type 8	Carpet grade	Two twisted-pairs of 26 AWG wire with shield for use under carpets
Type 9	Plenum grade	Two twisted-pairs, shielded (See previous discussion of plenum-grade cabling.)

Wireless Media

The extraordinary convenience of wireless communications has placed an increased emphasis on wireless networks in recent years. Technology is expanding rapidly and will continue to expand into the near future, offering more and better options for wireless networks.

Presently, you can subdivide wireless networking technology into three basic types corresponding to three basic networking scenarios:

- **Local area networks (LANs).** Occasionally, you will see a fully wireless LAN, but more typically, one or more wireless machines will function as members of a cable-based LAN. A LAN with both wireless and cable-based components is called a *hybrid*.
- **Extended local networks.** A wireless connection serves as a backbone between two LANs. For instance, a company with office networks in two nearby but separate buildings could connect those networks using a wireless bridge.
- **Mobile computing.** A mobile machine connects to the home network using cellular or satellite technology.

The following sections describe these technologies and some of the networking options available with each.

Wireless point-to-point communications are another facet of wireless LAN technology. Point-to-point wireless technology specifically facilitates communications between a pair of devices (rather than attempting to achieve an integrated networking capability). For instance, a point-to-point connection might transfer data between a laptop and a home-based computer or between a computer and a printer. Point-to-point signals can pass through walls, ceilings, and other obstructions. Point-to-point provides data transfer rates of 1.2 to 38.4 Kbps for a range of up to 200 feet indoors (or one third of a mile for line-of-sight broadcasts).

Reasons for Wireless Networks

Wireless networks are especially useful for the following situations:

- **Spaces where cabling would be impossible or inconvenient.** These include open lobbies, inaccessible parts of buildings, older buildings, historical buildings where renovation is prohibited, and outdoor installations.

- **People who move around a lot within their work environment.** Network administrators, for instance, must troubleshoot a large office network. Nurses and doctors need to make rounds at a hospital.
- **Temporary installations.** These situations include any temporary department set up for a specific purpose that soon will be torn down or relocated.
- **People who travel outside of the work environment and need instantaneous access to network resources.**

Wireless Communications with LANs

For some of the reasons described earlier in this chapter, it is often advantageous for a network to include some wireless nodes. Typically, though, the wireless nodes will be part of what is otherwise a traditional, cable-based network.

An *access point* is a stationary transceiver connected to the cable-based LAN that enables the cordless PC to communicate with the network. The access point acts as a conduit for the wireless PC. The process is initiated when the wireless PC sends a signal to the access point; from there, the signal reaches the network. The truly *wireless* communication, therefore, is the communication from the wireless PC to the access point. An access point transceiver is one of several ways to achieve wireless networking. Some of the others are described in later sections.

You can classify wireless LAN communications according to transmission method. The four most common LAN wireless transmission methods are as follows:

- Infrared
- Laser
- Narrow-band radio
- Spread-spectrum radio

Characteristics of Radio Transmission

Designing a radio system to have the ideal characteristics for an application requires plenty of design tradeoffs. This is because the characteristics of radio transmissions change dramatically with frequency. Low-frequency radio, for example, supports limited data rates but has the significant advantage that it frequently can communicate past the horizon. Shortwave operators are familiar with this phenomenon, and they commonly can monitor transmissions from the other side of the earth.

As frequency increases, transmissions become increasingly line-of-site. AM radio broadcast frequencies, for example, range from kilohertz to low-megahertz. Perhaps you have picked up an AM radio station from several states away late at night, which can occur because AM radio transmissions can bounce off the atmosphere's ozone layer. Some of the lowest-frequency AM radio transmissions can actually travel along the ground in a phenomenon called *ground waves*. Some transmissions can bounce a considerable distance. Conversely, FM transmissions seldom can be received past the horizon—in fact, you can seldom clearly receive an FM broadcast beyond a range of 100 miles. This is partly a function of power, but the primary cause of the range limitation is the inability of FM frequencies to go beyond the horizon. On a line-of-sight basis, however, high-frequency transmissions attenuate less rapidly than low-frequency transmissions.

Lower-frequency radio waves can penetrate solid materials to a greater degree than higher frequencies. Very low radio frequencies, for example, can be used to communicate with submerged submarines, although the data rates are extremely slow. Penetration capability also is a function of power—higher-power transmissions penetrate building walls more effectively than lower-power transmissions.

The following sections look briefly at these important wireless transmission methods.

Infrared Transmission

You use an infrared communication system every time you control your television with a remote control. The remote control transmits pulses of infrared light that carry coded instructions to a receiver on the TV. This technology also can be adapted to network communication.

Four varieties of infrared communications are as follows:

- **Broadband optical telepoint.** This method uses broadband technology. Data transfer rates in this high-end option are competitive with those for a cable-based network.
- **Line-of-sight infrared.** Transmissions must occur over a clear, line-of-sight path between transmitter and receiver.
- **Reflective infrared.** Wireless PCs transmit toward a common, central unit, which then directs communication to each of the nodes.
- **Scatter infrared.** Transmissions reflect off floors, walls, and ceilings until (theoretically) they finally reach the receiver. Because of the imprecise trajectory, data transfer rates are slow. The maximum reliable distance is around 100 feet.

Infrared transmissions typically are limited to within 100 feet. Within this range, however, infrared is relatively fast. Infrared's high bandwidth supports transmission speeds of up to 10 Mbps.

Infrared devices are insensitive to radio-frequency interference, but reception can be degraded by bright light. Because transmissions are tightly focused, they are fairly immune to electronic eavesdropping.

Laser Transmission

High-powered laser transmitters can transmit data for several thousand yards when line-of-sight communication is possible. Lasers can be used in many of the same situations as microwave links (described later in this chapter), without requiring an FCC license. On a LAN scale, laser light technology is similar to infrared technology.

Narrow-Band Radio Transmission

In narrow-band radio communications (also called single-frequency radio), transmissions occur at a single radio frequency. The range of narrow-band radio is higher than infrared, effectively enabling mobile computing over a limited area. Neither the receiver nor the transmitter must be placed along a direct line of sight; the signal can bounce off walls, buildings, and even the atmosphere, but heavy walls, such as steel or concrete enclosures, can block the signal.

Spread-Spectrum Radio Transmission

Spread-spectrum radio transmission is a technique originally developed by the military to solve several communication problems. Spread-spectrum improves reliability, reduces sensitivity to interference and jamming, and is less vulnerable to eavesdropping than single-frequency radio.

As its name suggests, spread-spectrum transmission uses multiple frequencies to transmit messages. Two techniques employed are *frequency hopping* and *direct sequence modulation*.

Frequency hopping switches (*hops*) among several available frequencies (see fig. 3.18), staying on each frequency for a specified interval of time. The transmitter and receiver must remain synchronized during a process called a *hopping sequence* in order for this technique to work. Range for this type of transmission is up to two miles outdoors and 400 feet indoors. Frequency hopping typically transmits at up to 250 Kbps, although some versions can reach as high as 2 Mbps.

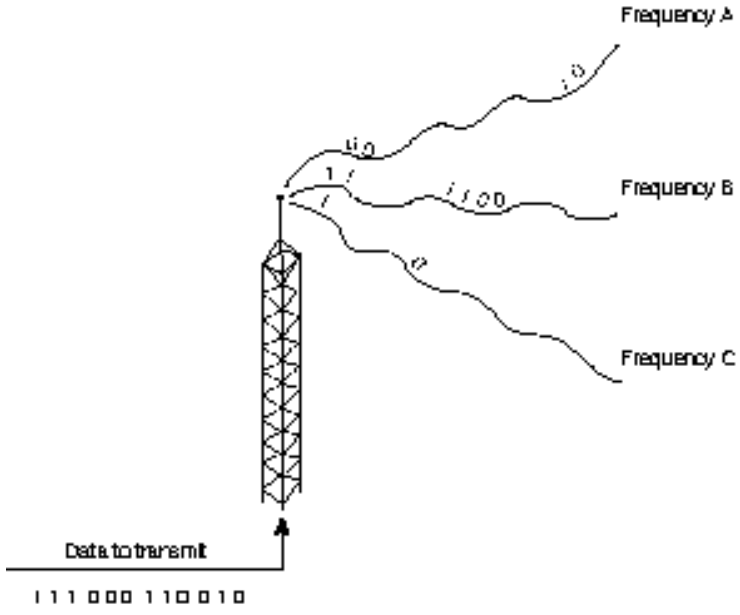


Figure 3.18

Frequency hopping employs various frequencies for a specific time period.

Direct sequence modulation breaks original messages into parts called *chips* (see fig. 3.19), which are transmitted on separate frequencies. To confuse eavesdroppers, decoy data also can be transmitted on other frequencies. The intended receiver knows which frequencies are valid and can isolate the chips and reassemble the message. Eavesdropping is difficult because the correct frequencies are not known, and the eavesdropper cannot isolate the frequencies carrying true data. Because different sets of frequencies can be selected, this technique can operate in environments that support other transmission activity. Direct sequence modulation systems operating at 900 MHz support bandwidths of 2–6 Mbps.

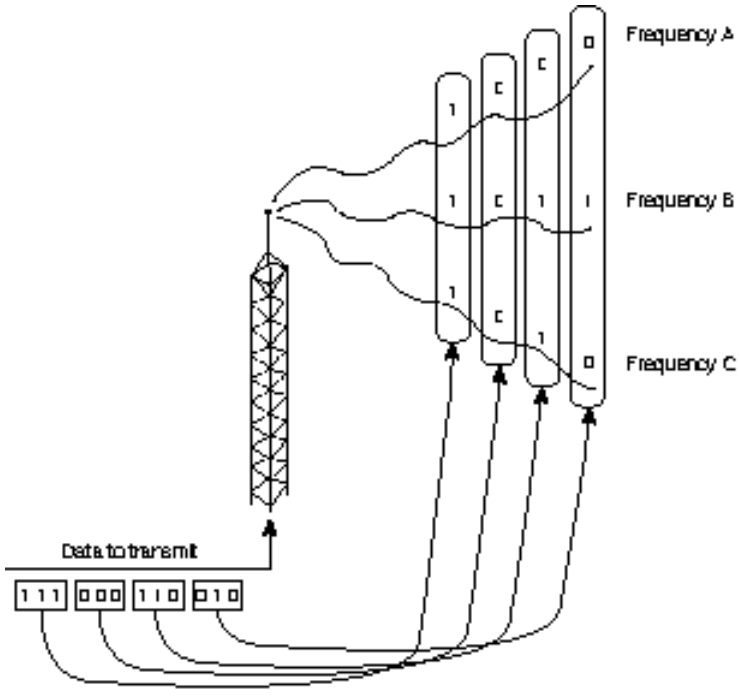


Figure 3.19

Direct sequence modulation.

Extended LANs (Wireless Bridging)

Wireless technology can connect LANs in two different buildings into an extended LAN. This capability is, of course, also available through other technologies (such as a T1 line or a leased line from a telephone provider), but depending on the conditions, a wireless solution is sometimes more cost-effective. A wireless connection between two buildings also provides a solution to the ground-potential problem described in a note earlier in this chapter.

A *wireless bridge* acts as a network bridge, merging two local LANs over a wireless connection (see Chapter 2, "Networking Standards," and Chapter 6, "Connectivity Devices," for more information on bridges). Wireless bridges typically use spread-spectrum radio technology to transmit data for up to three miles. (Antennae at each end of the bridge should be placed in an appropriate location, such as a rooftop.) A device called a *long-range wireless bridge* has a range of up to 25 miles.

The Radio Frequency Spectrum

The radio portion of the electromagnetic spectrum extends from 10 KHz to 1 GHz. Within this range are numerous bands, or ranges, of frequencies that are designated for specific purposes. You are probably familiar with the following frequency bands:

- Shortwave frequency
- Very High Frequency (VHF) (used in television and FM radio)
- Ultra High Frequency (UHF) (used in television)

Within the United States, the Federal Communications Commission (FCC) controls the use of radio frequencies. The majority of frequency allocations are licensed; an organization is granted an exclusive license to use a particular range of frequencies within a certain limited geographic area. Thus, you can have only one television Channel 5 within a given area, and Channel 5 allocations are spread out so that they don't interfere with each other. A licensed frequency allocation guarantees the license owner a clear, low-interference communication channel.

A few frequency ranges are unlicensed, which means that they can be used freely for the purpose specified for those frequencies. The FCC has designated three unlicensed frequency bands: 902–928 MHz, 2.4 GHz, and 5.72–5.85 GHz. The 902 MHz range has been available the longest and has been used for everything from cordless telephones to model airplane remote control. Because the 902 MHz range is quite crowded, many vendors are pushing development of devices for the less crowded 2.4 GHz band. Equipment for the 5.72 GHz remains expensive and is used infrequently.

Use of an unlicensed frequency occurs at the user's risk, and a clear communication channel is not guaranteed. Equipment used in these frequency bands, however, must operate at a regulated power level to limit range and reduce the potential for interference.

Mobile Computing

Mobile computing is a growing technology that provides almost unlimited range for traveling computers by using satellite and cellular phone networks to relay the signal to a home network. Mobile computing typically is used with portable PCs or personal digital assistant (PDA) devices.

Three forms of mobile computing are as follows:

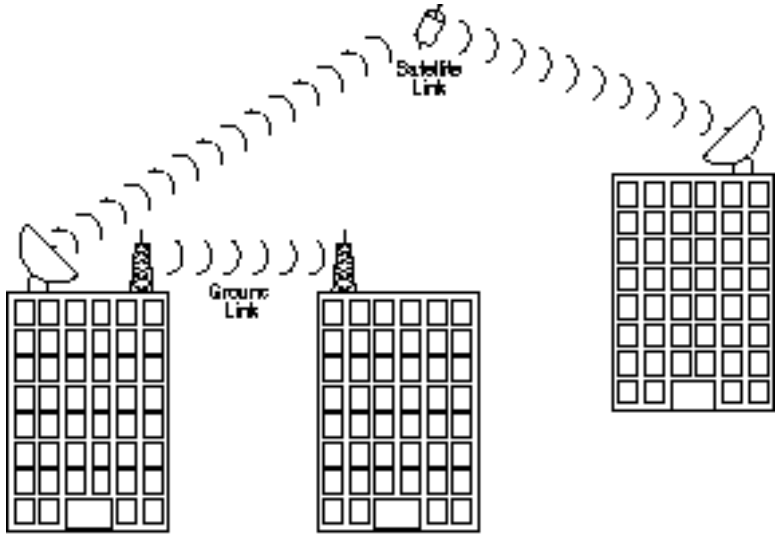
- **Packet-radio networking.** The mobile device sends and receives network-style packets via satellite. Packets contain a source and destination address, and only the destination device can receive and read the packet.
- **Cellular networking.** The mobile device sends and receives cellular digital packet data (CDPD) using cellular phone technology and the cellular phone network. Cellular networking provides very fast communications.
- **Satellite station networking.** Satellite mobile networking stations use satellite microwave technology, which is described later in this chapter.

Microwave

Microwave technology has applications in all three of the wireless networking scenarios: LAN, extended LAN, and mobile networking. As shown in figure 3.20, microwave communication can take two forms: terrestrial (ground) links and satellite links. The frequencies and technologies employed by these two forms are similar, but as you'll see, distinct differences exist between them.

Figure 3.20

Terrestrial and satellite microwave links.



Terrestrial Microwave

Terrestrial microwave communication employs Earth-based transmitters and receivers. The frequencies used are in the low-gigahertz range, which limits all communications to line-of-sight. You probably have seen terrestrial microwave equipment in the form of telephone relay towers, which are placed every few miles to relay telephone signals crosscountry.

Microwave transmissions typically use a parabolic antenna that produces a narrow, highly directional signal. A similar antenna at the receiving site is sensitive to signals only within a narrow focus. Because the transmitter and receiver are highly focused, they must be adjusted carefully so that the transmitted signal is aligned with the receiver.

A microwave link frequently is used to transmit signals in instances in which it would be impractical to run cables. If you need to connect two networks separated by a public road, for example, you might find that regulations restrict you from running cables above or below the road. In such a case, a microwave link is an ideal solution.

Some LANs operate at microwave frequencies at low power and use nondirectional transmitters and receivers. Network hubs can be placed strategically throughout an organization, and workstations can be mobile or fixed. This approach is one way to enable mobile workstations in an office setting.

In many cases, terrestrial microwave uses licensed frequencies. A license must be obtained from the FCC, and equipment must be installed and maintained by licensed technicians.

Terrestrial microwave systems operate in the low-gigahertz range, typically at 4–6 GHz and 21–23 GHz, and costs are highly variable depending on requirements. Long-distance microwave systems can be quite expensive but might be less costly than alternatives. (A leased telephone circuit, for example, represents a costly monthly expense.) When line-of-sight transmission is possible, a microwave link is a one-time expense that can offer greater bandwidth than a leased circuit.

Costs are on the way down for low-power microwave systems for the office. Although these systems don't compete directly in cost with cabled networks, when equipment frequently must be moved, microwave can be a cost-effective technology. Capacity can be extremely high, but most data communication systems operate at data rates between 1 and 10 Mbps. Attenuation characteristics are determined by transmitter power, frequency, and antenna size. Properly designed systems are not affected by attenuation under normal operational conditions—rain and fog, however, can cause attenuation of higher frequencies.

Microwave systems are highly susceptible to atmospheric interference and also can be vulnerable to electronic eavesdropping. For this reason, signals transmitted through microwave are frequently encrypted.

Satellite Microwave

Satellite microwave systems relay transmissions through communication satellites that operate in geosynchronous orbits 22,300 miles above the earth. Satellites orbiting at this distance remain located above a fixed point on earth.

Earth stations use parabolic antennas (satellite dishes) to communicate with satellites. These satellites then can retransmit signals in broad or narrow beams, depending on the locations set to receive the signals. When the destination is on the opposite side of the earth, for example, the first satellite cannot transmit directly to the receiver and thus must relay the signal through another satellite.

Because no cables are required, satellite microwave communication is possible with most remote sites and with mobile devices, which enables transmission with ships at sea and motor vehicles.

The distances involved in satellite communication result in an interesting phenomenon: Because all signals must travel 22,300 miles to the satellite and 22,300 miles when returning to a receiver, the time required to transmit a signal is independent of distance. It takes as long to transmit a signal to a receiver in the

same state as it does to a receiver a third of the way around the world. The time required for a signal to arrive at its destination is called *propagation delay*. The delays encountered with satellite transmissions range from 0.5 to 5 seconds.

Unfortunately, satellite communication is extremely expensive. Building and launching a satellite can cost easily in excess of a billion dollars. In most cases, organizations share these costs or purchase services from a commercial provider. AT&T, Hughes Network Services, and Scientific-Atlanta are among the firms that sell satellite-based communication services.

Satellite links operate in the low-gigahertz range, typically at 11–14 GHz. Costs are extremely high and usually are distributed across many users by selling communication services. Bandwidth is related to cost, and firms can purchase almost any required bandwidth. Typical data rates are 1–10 Mbps. Attenuation characteristics depend on frequency, power, and atmospheric conditions. Properly designed systems also take attenuation into account—rain and atmospheric conditions might attenuate higher frequencies. Microwave signals also are sensitive to EMI and electronic eavesdropping, so signals transmitted through microwave frequently are encrypted.

Earth stations can be installed by numerous commercial providers. Transmitters operate on licensed frequencies and require an FCC license.

Summary

This chapter examined the characteristics of some common network transmission media. You learned about some of the advantages and disadvantages of popular transmission media. This chapter looked at characteristics such as cost, distance limitation, ease of installation, EMI characteristics, and common uses for coaxial, UTP, STP, and fiber-optic cable, and wireless communication methods.

Exercises

Exercise 3.1: Shopping for Network Cabling

Objective: Explore the prices and availability of network cabling media in your area. Obtain a real-world view of cabling options.

Estimated time: 15 minutes

This chapter discussed the advantages and disadvantages of common network transmission media. In this exercise, you'll explore how network installation professionals perceive the differences between the cabling types. Remember that the cabling types discussed in this chapter are all tied to particular network topologies and architectures. You may want to read through Chapter 4, "Network Topologies and Architectures," before attempting this exercise.

1. Call a local computer store (preferably a store that provides network installations) and ask for some basic information on network cabling. Ask about coaxial Thinnet and Thicknet, UTP, and STP. Find out which type the store prefers to work with and in what situations they would recommend each of the types. Ask for pricing on Thinnet PVC and Plenum-grade cable. Try to get a feeling for how the real world perceives the cabling types described in this chapter.

Computer vendors generally are busy people, so try to be precise. Don't imply that you're getting ready to buy a whole network (unless you are). Just tell them you're trying to learn more about network cabling—vendors are often happy to share their knowledge. If they're helpful, remember them the next time you need a bid.

Review Questions

The following questions test your knowledge of the information presented in this chapter. For additional exam help, visit Microsoft's site at www.microsoft.com/train_cert/cert/Mcpsteps.htm.

1. Which two of the following are true about coaxial Thinnet:

   A. Thinnet cable is approximately 0.5 in. thick.

   B. Thinnet has 50-ohm impedance.

   C. Thinnet is sometimes called Standard Ethernet.

   D. Thinnet cable includes an insulation layer.

2. Transceivers for Thicknet cables are often connected using _____.

   A. ghost taps

   B. vampire taps

   C. witch widgets

   D. skeleton clamps

3. Which two of the following are true about UTP?

   A. You can use an RJ-11 connector with an RJ-45 socket.

   B. UTP has the lowest cost of any cabling system except Thinnet.

   C. Telephone systems use UTP.

   D. UTP is more sensitive to EMI than Thinnet.

4. Which of the following is not a permissible location for coaxial PVC cabling?

   A. A bathroom

   B. Above a drop ceiling

   C. Outside

   D. Along an exterior wall

5. UTP Category 3 uses _____ twisted-pair(s) of cables.

   A. 1
   B. 2
   C. 3
   D. 8

6. Transmission rates of _____ are typical for fiber-optic cables.

   A. 10 Mbps
   B. 25 Mbps
   C. 100 Mbps
   D. 500 Mbps

7. _____ is a transceiver that connects a wireless node with the LAN.

   A. An access provider
   B. An access point
   C. A Central Access Device (CAD)
   D. A Wireless Access Device (WAD)

8. _____ transmissions are designed to reflect the light beam off walls, floors, and ceilings until it finally reaches the receiver.

   A. Reflective infrared
   B. Scatter infrared
   C. Spread-spectrum infrared
   D. None of the above

9. Which three of the following are forms of mobile network technology?

   A. Cellular
   B. Packet-radio
   C. Wireless bridge
   D. Satellite station

10. Which of the following cable types supports the greatest cable lengths?

   A. Unshielded twisted-pair
   B. Shielded twisted-pair
   C. Thicknet coaxial cable
   D. Thinnet coaxial cable

11. What are two advantages of UTP cable?

   A. Low cost
   B. Easy installation
   C. High resistance to EMI due to twists in cable
   D. Cabling of up to 500 meters

12. What are two benefits of shielding in a cable?

   A. Reduction in signal attenuation
   B. Reduction in EMI radiation
   C. Reduction in sensitivity to outside interference
   D. None of the above

13. What are two disadvantages of fiber-optic cable?

   A. Sensitive to EMI
   B. Expensive hardware
   C. Expensive to install
   D. Limited in bandwidth

14. Which cable type is ideal for connecting between two buildings?

    A. UTP
    B. STP
    C. Coaxial
    D. Fiber-optic

15. As frequency increases, radio transmission becomes increasingly _____.

    A. attenuated
    B. rapid
    C. line-of-sight
    D. sensitive to electromagnetic interference

16. Which two statements are true of microwave systems?

    A. Microwave transmissions do not attenuate under any conditions.
    B. All microwave systems operate in the low-gigahertz range.
    C. Microwave signals are sensitive to EMI and electronic eavesdropping.
    D. Unlike most other types of radio transmitters, microwave transmitters don't need to be licensed.

17. DIN Connectors are primarily used for _____.

    A. connecting UTP cables
    B. cabling Macintosh computers to AppleTalk networks
    C. connecting devices with Thick-wire Ethernet
    D. none of the above

18. Which two connectors are frequently used with STP cable?

    A. T-connectors
    B. RJ-45 connectors
    C. IBM unisex connectors
    D. AppleTalk DIN connectors

19. Which two connectors are commonly used with coaxial cable?

    A. DB-25 connectors
    B. N-connectors
    C. ST-connectors
    D. BNC connectors

20. Which two statements are true of Thinnet cabling?

    A. A T-connector must be used to connect the PC's network board to the network.
    B. Either end of the cable can be terminated, but not both ends.
    C. BNC connectors cannot be used.
    D. One terminator must be grounded.