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

- Explain basic data transmission concepts, including full duplexing, attenuation, latency, and noise
- Describe the physical characteristics of coaxial cable, STP, UTP, and fiber-optic media
- Compare the benefits and limitations of different networking media
- Explain the principles behind and uses for serial connector cables
- Identify wiring standards and the best practices for cabling buildings and work areas
Just as highways and streets provide the foundation for automobile travel, networking media provide the physical foundation of data transmission. Media are the physical or atmospheric paths that signals follow. The first networks transmitted data over thick coaxial cables. Today, when not transmitted through the air, as in wireless networks, data is commonly transmitted over a type of cable that resembles telephone cords. It’s sheathed in flexible plastic and contains twisted copper wire inside. For long-distance network connections, fiber-optic cable is preferred. And more and more, organizations are sending signals through the atmosphere to form wireless networks, which are covered in Chapter 8. Because networks are always evolving and demanding greater speed, versatility, and reliability, networking media change rapidly.

I was working for a company whose building was being gutted for renovations. The IT people told the architect about a problem with one of the planned data connections. One cabling run was going to be 105 meters—a problem, since the Institute of Electrical and Electronics Engineers (IEEE) recommends that cabling runs be limited to 100 meters to prevent problems with a network. The architect was concerned about the IT department’s suggestion that he install an additional wiring closet to shorten the cabling run, given that it would cost another $2,000.

Our new network was going to be a switched Ethernet network, meaning that our connectivity devices would be switches rather than hubs. After some investigation and learning more details of the proposed network, a networking faculty member from a local college and I met with the architect and the Director of IT. We explained that the 100-meter cabling limitation is only a problem for older networks that rely on hubs. With a newer switched environment, we might see some slight loss of speed for the end user with a 105-meter cabling run, but it would be fairly small.

We offered two options: We could put a repeater between the switch and the end user to shorten the cabling run, or we could allow the cabling run to go over 100 meters. Using free software available over the Internet, we ran simulations for each scenario to see what sort of loss we had. We determined that, at worst, the user would see about a 5 percent drop in the speed of the network in each case.

The institution decided to go with the longer cabling run. We’ve done some tests on the user’s workstation subsequent to building the network and found that the reduction in throughput is even less than 5 percent. So with some free software and a little knowledge of modern network technology, we were able to save the institution the cost of a $2,000 dollar wiring closet.

Michael Qaissaunee
Brookdale Community College
Network problems often occur at or below the Physical layer. Therefore, understanding the characteristics of various networking media is critical to designing and troubleshooting networks. You also need to know how data is transmitted over the media. This chapter discusses physical networking media and the details of data transmission. You’ll learn what it takes to make data transmission dependable and how to correct some common transmission problems.

Transmission Basics

In data networking, the term transmit means to issue signals along a network medium such as a cable. Transmission refers to either the process of transmitting or the progress of signals after they have been transmitted. In other words, you could say, “My NIC transmitted a message, but because the network is slow, the transmission took 10 seconds to reach the server.” In fact, NICs both transmit and receive signals, which means they are a type of transceiver.

Long ago, people transmitted information across distances via smoke or fire signals. Needless to say, many different methods of data transmission have evolved since that time. The transmission techniques in use on today’s networks are complex and varied. In the following sections, you will learn about some fundamental characteristics that define today’s data transmission. In later chapters, you will learn about more subtle and specific differences between types of data transmission.

Analog and Digital Signaling

One important characteristic of data transmission is the type of signaling involved. On a data network, information can be transmitted via one of two signaling methods: analog or digital.

Computers generate and interpret digital signals as electrical current, the pressure of which is measured in volts. The strength of an electrical signal is directly proportional to its voltage. Thus, when network engineers talk about the strength of a signal, they often refer to the signal’s voltage. After being generated, signals travel over copper cabling as electrical current. Over fiber-optic cable, they travel as light pulses. And through the atmosphere, they travel as electromagnetic waves.

Analog data signals are also generated as voltage. However, in analog signals, voltage varies continuously and appears as a wavy line when graphed over time, as shown in Figure 3-1.

An analog signal, like other waveforms, is characterized by four fundamental properties: amplitude, frequency, wavelength, and phase. A wave’s amplitude is a measure of its strength at any given point in time. On a wave graph, the amplitude is the height of the wave at any point in time. In Figure 3-1, for example, the wave has an amplitude of 5 volts at .25 seconds, an amplitude of 0 volts at .5 seconds, and an amplitude of −5 volts at .75 seconds.

Whereas amplitude indicates an analog wave’s strength, frequency is the number of times that a wave’s amplitude cycles from its starting point, through its highest amplitude and its lowest amplitude, and back to its starting point over a fixed period of time. Frequency is expressed in cycles per second, or hertz (Hz), named after German physicist Heinrich Hertz, who experimented with electromagnetic waves in the late nineteenth century. For example, in Figure 3-1 the wave cycles to its highest then lowest amplitude and returns to its starting point once in 1 second. Thus, the frequency of that wave would be 1 cycle per second, or 1 Hz—which, as it turns out, is an extremely low frequency.
Frequencies used to convey speech over telephone wires fall in the 300 to 3300 Hz range. Humans can hear frequencies between 20 and 20,000 Hz. An FM radio station may use a frequency between 850,000 Hz (or 850 kHz) and 108,000,000 Hz (or 108 MHz) to transmit its signal through the air. You will learn more about radio frequencies used in networking later in this chapter.

The distance between corresponding points on a wave’s cycle—for example, between one peak and the next—is called its wavelength. Wavelengths can be expressed in meters or feet. A wave’s wavelength is inversely proportional to its frequency. In other words, the higher the frequency, the shorter the wavelength. For example, a radio wave with a frequency of 1,000,000 cycles per second (1 MHz) has a wavelength of 300 meters, while a wave with a frequency of 2,000,000 Hz (2 MHz) has a wavelength of 150 meters.

The term phase refers to the progress of a wave over time in relationship to a fixed point. Suppose two separate waves have identical amplitudes and frequencies. If one wave starts at its lowest amplitude at the same time the second wave starts at its highest amplitude, these waves will have different phases. More precisely, they will be 180 degrees out of phase (using the standard assignment of 360 degrees to one complete wave). Had the second wave also started at its lowest amplitude, the two waves would be in phase. Figure 3-2 illustrates waves with identical amplitudes and frequencies whose phases are 90 degrees apart.

One benefit to analog signals is that, because they are more variable than digital signals, they can convey greater subtleties with less energy. For example, think of the difference between your voice and a digital voice, such as the automated service that some libraries use to notify
you when a book you have requested is available. The digital voice has a poorer quality than your own voice—that is, it sounds like a machine. It can’t convey the subtle changes in inflection that you expect in a human voice. Only very high-quality digital signals—for example, those used to record music on compact discs—can achieve such accuracy.

One drawback to analog signals is that their voltage is varied and imprecise. Thus, analog transmission is more susceptible to transmission flaws such as noise, or any type of interference that may degrade a signal, than digital signals. If you have tried to listen to AM radio on a stormy night, you have probably heard the crackle and static of noise affecting the signal.

Now contrast the analog signals pictured in Figures 3-1 and 3-2 to a digital signal, as shown in Figure 3-3. Digital signals are composed of pulses of precise, positive voltages and zero voltages. A pulse of positive voltage represents a 1. A pulse of zero voltage (in other words, the lack of any voltage) represents a 0. The use of 1s and 0s to represent information is characteristic of a binary system. Every pulse in the digital signal is called a binary digit, or *bit*. 

![Figure 3-2](image1)  
*Figure 3-2* Waves with a 90-degree phase difference

![Figure 3-3](image2)  
*Figure 3-3* An example of a digital signal
A bit can have only one of two possible values: 1 or 0. Eight bits together form a byte. In broad terms, one byte carries one piece of information. For example, the byte 01111001 means 121 on a digital network.

Computers read and write information—for example, program instructions, routing information, and network addresses—in bits and bytes. When a number is represented in binary form (for example, 01111001), each bit position, or placeholder, in the number represents a specific multiple of 2. Because a byte contains eight bits, it has eight placeholders. When counting placeholders in a byte, you move from right to left. The placeholder farthest to the right is known as the zero position, the one to its left is in the first position, and so on. The placeholder farthest to the left is in the seventh position, as shown in Figure 3-4.

To find the decimal value of a bit, you multiply the 1 or 0 (whichever the bit is set to) by $2^x$, where $x$ equals the bit’s position. For example, the 1 or 0 in the zero position must be multiplied by 2 to the 0 power, or $2^0$, to determine its value. Any number (other than zero) raised to the power of 0 has a value of 1. Thus, if the zero-position bit is 1, it represents a value of $1 \times 2^0$, or $1 \times 1$, which equals 1. If a 0 is in the zero position, its value equals $0 \times 2^0$, or $0 \times 1$, which equals 0. In every position, if a bit is 0, that position represents a decimal number of 0.

To convert a byte to a decimal number, determine the value represented by each bit, then add those values together. If a bit in the byte is 1 (in other words, if it’s “on”), the bit’s numerical equivalent in the coding scheme is added to the total. If a bit is 0, that position has no value and nothing is added to the total. For example, the byte 11111111 equals $1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$, or $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$. Its decimal equivalent, then, is 255. In another example, the byte 00100100 equals $0 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$, or $0 + 0 + 32 + 0 + 0 + 4 + 0 + 0$. Its decimal equivalent, then, is 36.

Figure 3-4 illustrates placeholders in a byte, the exponential multiplier for each position, and the different decimal values that are represented by a 1 in each position.

To convert a decimal number to a byte, you reverse this process. For example, the decimal number 8 equals $2^3$, which means a single “on” bit would be indicated in the fourth bit position as follows: 00001000. In another example, the decimal number 9 equals $8 + 1$, or $2^3 + 2^0$, and would be represented by the binary number 00010001.

The binary numbering scheme may be used with more than eight positions. However, in the digital world, bytes form the building blocks for messages, and bytes always include eight positions. In a data signal, multiple bytes are combined to form a message. If you were to peek at the 1s and 0s used to transmit an entire e-mail message, for example, you might see millions of zeros and ones passing by. A computer can quickly translate these binary numbers into codes, such as ASCII or JPEG, that express letters, numbers, and pictures.

<table>
<thead>
<tr>
<th>Bit position:</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary exponential:</td>
<td>$2^7$</td>
<td>$2^6$</td>
<td>$2^5$</td>
<td>$2^4$</td>
<td>$2^3$</td>
<td>$2^2$</td>
<td>$2^1$</td>
<td>$2^0$</td>
</tr>
<tr>
<td>Value if bit = 1:</td>
<td>128</td>
<td>64</td>
<td>32</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 3-4 Components of a byte
Converting between decimal and binary numbers can be done by hand, as shown previously, or by using a scientific calculator, such as the one available with the Windows XP or Windows Vista operating systems. Take, for example, the number 131. To convert it to a binary number:

1. On a Windows XP or Windows Vista computer, click the **Start** button, select **All Programs**, select **Accessories**, and then select **Calculator**. The Calculator window opens.

2. Click **View**, and then click **Scientific**. Verify that the **Dec** option button is selected.

3. Type **131**, and then click the **Bin** option button. The binary equivalent of the number 131, 10000011, appears in the display window.

You can reverse this process to convert a binary number to a decimal number.


If you’re connected to the Internet and using a Web browser, you can quickly convert binary and decimal numbers by using Google calculator. Simply point your browser to [www.google.com](http://www.google.com), then type in the number you want to convert, plus the format, in the search text box. For example, to convert the decimal number 131 into binary form, type “131 in binary” (without the quotation marks), and then press Enter. You see the following result: 131 = 0b10000011. The prefix “0b” indicates that the number is in binary format. To convert a binary number into decimal form, type “0b” (without the quotation marks) before the binary number. For example, entering “0b10000011 in decimal” (without the quotation marks) would return the number 131.

Because digital transmission involves sending and receiving only a pattern of 1s and 0s, represented by precise pulses, it is more reliable than analog transmission, which relies on variable waves. In addition, noise affects digital transmission less severely. On the other hand, digital transmission requires many pulses to transmit the same amount of information that an analog signal can transmit with a single wave. Nevertheless, the high reliability of digital transmission makes this extra signaling worthwhile. In the end, digital transmission is more efficient than analog transmission because it results in fewer errors and, therefore, requires less overhead to compensate for errors.

**Overhead** is a term used by networking professionals to describe the nondata information that must accompany data for a signal to be properly routed and interpreted by the network. For example, the Data Link layer header and trailer, the Network layer addressing information, and the Transport layer flow control information added to a piece of data in order to send it over the network are all part of the transmission’s overhead.

It’s important to understand that in both the analog and digital worlds, a variety of signaling techniques are used. For each technique, standards dictate what type of transmitter, communications channel, and receiver should be used. For example, the type of transmitter (NIC) used for computers on a LAN and the way in which this transmitter manipulates electric current to produce signals is different from the transmitter and signaling techniques used with a
satellite link. While not all signaling methods are covered in this book, you will learn about the most common methods used for data networking.

**Data Modulation**

Data relies almost exclusively on digital transmission. However, in some cases the type of connection your network uses may be capable of handling only analog signals. For example, telephone lines are designed to carry analog signals. If you connect to your ISP’s network via a telephone line, the data signals issued by your computer must be converted into analog form before they get to the phone line. Later, they must be converted back into digital form when they arrive at the ISP’s access server. A modem accomplishes this translation. The word *modem* reflects this device’s function as a modulator/demodulator—that is, it modulates digital signals into analog signals at the transmitting end, then demodulates analog signals into digital signals at the receiving end.

Data modulation is a technology used to modify analog signals to make them suitable for carrying data over a communication path. In **modulation**, a simple wave, called a carrier wave, is combined with another analog signal to produce a unique signal that gets transmitted from one node to another. The carrier wave has preset properties (including frequency, amplitude, and phase). Its purpose is to help convey information; in other words, it’s only a messenger. Another signal, known as the information or data wave, is added to the carrier wave. When the information wave is added, it modifies one property of the carrier wave (for example, the frequency, amplitude, or phase). The result is a new, blended signal that contains properties of both the carrier wave and added data. When the signal reaches its destination, the receiver separates the data from the carrier wave.

Modulation can be used to make a signal conform to a specific pathway, as in the case of **FM (frequency modulation)** radio, in which the data must travel along a particular frequency. In frequency modulation, the frequency of the carrier signal is modified by the application of the data signal. In **AM (amplitude modulation)**, the amplitude of the carrier signal is modified by the application of the data signal. Modulation may also be used to issue multiple signals to the same communications channel and prevent the signals from interfering with one another. Figure 3-5 depicts an unaltered carrier wave, a data wave, and the combined wave as modified through frequency modulation. Later in this book, you will learn about networking technologies, such as DSL, that make use of modulation.

**Simplex, Half-Duplex, and Duplex**

Data transmission, whether analog or digital, may also be characterized by the direction in which the signals travel over the media. In cases in which signals may travel in only one direction, the transmission is considered **simplex**. An example of simplex communication is a football coach calling out orders to his team through a megaphone. In this example, the coach’s voice is the signal, and it travels in only one direction—away from the megaphone’s mouthpiece and toward the team. Simplex is sometimes called one-way, or unidirectional, communication.

In **half-duplex** transmission, signals may travel in both directions over a medium but in only one direction at a time. Half-duplex systems contain only one channel for communication, and that channel must be shared for multiple nodes to exchange information. For example, a walkie-talkie or an apartment’s intercom system that requires you to press a “talk” button to allow your voice to be transmitted uses half-duplex transmission. If you visit a friend’s apartment building, you press the “talk” button to send your voice signals to his apartment. When
your friend responds, he presses the “talk” button in his apartment to send his voice signal in the opposite direction over the wire to the speaker in the lobby where you wait. If you press the “talk” button while he’s talking, you will not be able to hear his voice transmission. In a similar manner, some networks operate with only half-duplex capability.

When signals are free to travel in both directions over a medium simultaneously, the transmission is considered full-duplex. Full-duplex may also be called bidirectional transmission or, sometimes, simply duplex. When you call a friend on the telephone, your connection is an example of a full-duplex transmission because your voice signals can be transmitted to your friend at the same time your friend’s voice signals are transmitted in the opposite direction to you. In other words, both of you can talk and hear each other simultaneously.

Figure 3-6 compares simplex, half-duplex, and full-duplex transmissions.

Full-duplex transmission is also used on data networks. For example, modern Ethernet networks are capable of full-duplex. In this situation, full-duplex transmission uses multiple channels on the same medium. A channel is a distinct communication path between nodes, much as a lane is a distinct transportation path on a freeway. Channels may be separated either logically or physically. You will learn about logically separate channels in the next section. An example of physically separate channels occurs when one wire within a network cable is used for transmission while another wire is used for reception. In this example, each separate wire in the medium allows half-duplex transmission. When combined in a cable,
they form a medium that provides full-duplex transmission. Full-duplex capability increases the speed with which data can travel over a network. In some cases—for example, when providing telephone service over the Internet—full-duplex data networks are a requirement.

Many network devices, such as modems and NICs, allow you to specify whether the device should use half- or full-duplex communication. It’s important to know what type of transmission a network supports before installing network devices on that network. If you configure a computer’s NIC to use full-duplex while the rest of the network is using half-duplex, for example, that computer will not be able to communicate on the network.

**Multiplexing**

A form of transmission that allows multiple signals to travel simultaneously over one medium is known as multiplexing. To carry multiple signals, the medium’s channel is logically separated into multiple smaller channels, or subchannels. Many different types of multiplexing are available, and the type used in any given situation depends on what the media, transmission, and reception equipment can handle. For each type of multiplexing, a device that can combine many signals on a channel, a multiplexer (mux), is required at the transmitting end of the channel. At the receiving end, a demultiplexer (demux) separates the combined signals and regenerates them in their original form. Networks rely on multiplexing to increase the amount of data that can be transmitted in a given time span over a given bandwidth.

One type of multiplexing, TDM (time division multiplexing), divides a channel into multiple intervals of time, or time slots. It then assigns a separate time slot to every node on the network and, in that time slot, carries data from that node. For example, if five stations are connected to a network over one wire, five different time slots are established in the communications channel. Workstation A may be assigned time slot 1, workstation B time slot 2, workstation C time slot 3, and so on. Time slots are reserved for their designated nodes regardless of whether the node has data to transmit. If a node does not have data to send, nothing is sent during its time slot. This arrangement can be inefficient if some nodes on the network rarely send data. Figure 3-7 shows a simple TDM model.

Statistical multiplexing is similar to time division multiplexing, but rather than assigning a separate slot to each node in succession, the transmitter assigns slots to nodes according to priority and need. This method is more efficient than TDM, because in statistical multiplexing time slots are unlikely to remain empty. To begin with, in statistical multiplexing, as in
TDM, each node is assigned one time slot. However, if a node doesn’t use its time slot, statistical multiplexing devices recognize that and assign its slot to another node that needs to send data. The contention for slots may be arbitrated according to use or priority or even more sophisticated factors, depending on the network. Most importantly, statistical multiplexing maximizes available bandwidth on a network. Figure 3-8 depicts a simple statistical multiplexing system.

FDM (frequency division multiplexing) is a type of multiplexing that assigns a unique frequency band to each communications subchannel. Signals are modulated with different carrier frequencies, then multiplexed to simultaneously travel over a single channel. The first use of FDM was in the early 20th century when telephone companies discovered they could send multiple voice signals over a single cable. That meant that rather than stringing separate lines for each residence (and adding to the urban tangle of wires), they could send as many as 24 multiplexed signals over a single neighborhood line. Each signal was then demultiplexed before being brought into the home.

Now, telephone companies also multiplex signals on the phone line that enters your residence. Voice communications use the frequency band of 300–3400 Hz (because this matches approximately the range of human hearing), for a total bandwidth of 3100 Hz. But the potential bandwidth of one phone line far exceeds this. Telephone companies implement FDM to subdivide and send signals in the bandwidth above 3400 Hz. Because the frequencies can’t be heard, you don’t notice the data transmission occurring while you talk on the telephone. Figure 3-9 provides a simplified view of FDM, in which waves representing three different frequencies are carried simultaneously by one channel.

Different forms of FDM exist. One type is used in cellular telephone transmission and another by DSL Internet access (you’ll learn more about DSL in Chapter 7).

WDM (wavelength division multiplexing) is a technology used with fiber-optic cable, which enables one fiber-optic connection to carry multiple light signals simultaneously.
WDM, a single fiber can transmit as many as 20 million telephone conversations at one time. WDM can work over any type of fiber-optic cable.

In the first step of WDM, a beam of light is divided into up to 40 different carrier waves, each with a different wavelength (and, therefore, a different color). Each wavelength represents a separate transmission channel capable of transmitting up to 10 Gbps. Before transmission, each carrier wave is modulated with a different data signal. Then, through a very narrow beam of light, lasers issue the separate, modulated waves to a multiplexer. The multiplexer combines all of the waves, in the same way that a prism can accept light beams of different wavelengths and concentrate them into a single beam of white light. Next, another laser issues this multiplexed beam to a strand of fiber within a fiber-optic cable. The fiber carries the multiplexed signals to a receiver, which is connected to a demultiplexer. The demultiplexer acts as a prism to separate the combined signals according to their different wavelengths (or colors). Then, the separate waves are sent to their destinations on the network. If the signal risks losing strength between the multiplexer and demultiplexer, an amplifier might be used to boost it. Figure 3-10 illustrates WDM transmission.

The form of WDM used on most modern fiber-optic networks is DWDM (dense wavelength division multiplexing). In DWDM, a single fiber in a fiber-optic cable can carry between 80 and 160 channels. It achieves this increased capacity because it uses more wavelengths for signaling. In other words, there is less separation between the usable carrier waves in DWDM than there is in the original form of WDM. Because of its extraordinary capacity,
DWDM is typically used on high-bandwidth or long-distance WAN links, such as the connection between a large ISP and its (even larger) network service provider.

**Relationships Between Nodes**

So far you have learned about two important characteristics of data transmission: the type of signaling (analog or digital) and the direction in which the signal travels (simplex, half-duplex, full-duplex, or multiplex). Another important characteristic is the number of senders and receivers, as well as the relationship between them. In general, data communications may involve a single transmitter with one or more receivers, or multiple transmitters with one or more receivers. The remainder of this section introduces the most common relationships between transmitters and receivers.

When a data transmission involves only one transmitter and one receiver, it is considered a point-to-point transmission. An office building in Dallas exchanging data with another office in St. Louis over a WAN connection is an example of point-to-point transmission. In this case, the sender only transmits data that is intended to be used by a specific receiver.

By contrast, point-to-multipoint transmission involves one transmitter and multiple receivers. Point-to-multipoint arrangements can be separated into two types: broadcast and nonbroadcast. Broadcast transmission involves one transmitter and multiple, undefined receivers. For example, a TV station indiscriminately transmitting a signal from its tower to thousands of homes with TV antennas uses broadcast transmission. A broadcast transmission sends data to any and all receivers, without regard for which receiver can use it. Broadcast transmissions are frequently used on both wired and wireless networks because they are simple and quick. They are used to identify certain nodes, to send data to certain nodes (even though every node is capable of picking up the transmitted data, only the destination node will actually do it), and to send announcements to all nodes.

When more tailored data transfer is desired, a network might use nonbroadcast point-to-multipoint transmission. In this scenario, a node issues signals to multiple, defined recipients. For example, a network administrator could schedule the LAN transmission of an instructional video which only she and all of her team’s workstations could receive.

Figure 3-11 contrasts point-to-point and point-to-multipoint transmissions.

**Throughput and Bandwidth**

The data transmission characteristic most frequently discussed and analyzed by networking professionals is throughput. Throughput is the measure of how much data is transmitted during a given period of time. It may also be called capacity or bandwidth (though as you will learn, bandwidth is technically different from throughput). Throughput is commonly expressed as a quantity of bits transmitted per second, with prefixes used to designate different throughput amounts. For example, the prefix kilo combined with the word bit (as in kilo-bit) indicates 1000 bits per second. Rather than talking about a throughput of 1000 bits per second, you typically say the throughput was 1 kilobit per second (1 Kbps). Table 3-1 summarizes the terminology and abbreviations used when discussing different throughput amounts. As an example, a residential broadband Internet connection might be rated for a maximum throughput of 1.544 Mbps. A fast LAN might transport up to 10 Gbps of data. Contemporary networks commonly achieve throughputs of 10 Mbps, 100 Mbps, 1 Gbps,
Applications that require significant throughput include videoconferencing and telephone signaling. By contrast, instant messaging and e-mail, for example, require much less throughput.

Be careful not to confuse bits and bytes when discussing throughput. Although data storage quantities are typically expressed in multiples of bytes, data transmission quantities (in other words, throughput) are more commonly expressed in multiples of bits per second. When representing different data quantities, a small \( b \) represents bits, while a capital \( B \) represents bytes. To put this into context, a modem may transmit data at 56.6 Kbps (kilobits per second); a data file may be 56 KB (kilobytes) in size. Another difference between data storage and data throughput measures is that in data storage the prefix \textit{kilo} means 2 to the 10\textsuperscript{th} power, or 1024, not 1000.

Often, the term \textit{bandwidth} is used interchangeably with throughput, and in fact, this may be the case on the Network+ certification exam. Bandwidth and throughput are similar...
concepts, but strictly speaking, **bandwidth** is a measure of the difference between the highest and lowest frequencies that a medium can transmit. This range of frequencies, which is expressed in Hz, is directly related to throughput. For example, if the FCC told you that you could transmit a radio signal between 870 and 880 MHz, your allotted bandwidth (literally, the width of your frequency band) would be 10 MHz.

**Baseband and Broadband**

**Baseband** is a transmission form in which (typically) digital signals are sent through direct current (DC) pulses applied to the wire. This direct current requires exclusive use of the wire’s capacity. As a result, baseband systems can transmit only one signal, or one channel, at a time. Every device on a baseband system shares the same channel. When one node is transmitting data on a baseband system, all other nodes on the network must wait for that transmission to end before they can send data. Baseband transmission supports half-duplexing, which means that computers can both send and receive information on the same length of wire. In some cases, baseband also supports full duplexing.

Ethernet is an example of a baseband system found on many LANs. In Ethernet, each device on a network can transmit over the wire—but only one device at a time. For example, if you want to save a file to the server, your NIC submits your request to use the wire; if no other device is using the wire to transmit data at that time, your workstation can go ahead. If the wire is in use, your workstation must wait and try again later. Of course, this retrying process happens so quickly that you don’t even notice the wait.

**Broadband** is a form of transmission in which signals are modulated as radiofrequency (RF) analog waves that use different frequency ranges. Unlike baseband, broadband technology does not encode information as digital pulses.

As you may know, broadband transmission is used to bring cable TV to your home. Your cable TV connection can carry at least 25 times as much data as a typical baseband system (like Ethernet) carries, including many different broadcast frequencies on different channels. In traditional broadband systems, signals travel in only one direction—toward the user. To allow users to send data as well, cable systems allot a separate channel space for the user’s transmission and use amplifiers that can separate data the user issues from data the network transmits. Broadband transmission is generally more expensive than baseband transmission because of the extra hardware involved. On the other hand, broadband systems can span longer distances than baseband.

In the field of networking, some terms have more than one meaning, depending on their context. **Broadband** is one of those terms. The **broadband** described in this chapter is the transmission system that carries RF signals across multiple channels on a coaxial cable, as used by cable TV. This definition was the original meaning of broadband. However, broadband has evolved to mean any of several different network types that use digital signaling to transmit data at very high transmission rates.

**Transmission Flaws**

Both analog and digital signals are susceptible to degradation between the time they are issued by a transmitter and the time they are received. One of the most common transmission flaws affecting data signals is noise.
Noise As you learned earlier, noise is any undesirable influence that may degrade or distort a signal. Many different types of noise may affect transmission. A common source of noise is EMI (electromagnetic interference), or waves that emanate from electrical devices or cables carrying electricity. Motors, power lines, televisions, copiers, fluorescent lights, manufacturing machinery, and other sources of electrical activity (including a severe thunderstorm) can cause EMI. One type of EMI is RFI (radiofrequency interference), or electromagnetic interference caused by radio waves. (Often, you’ll see EMI referred to as EMI/RFI.) Strong broadcast signals from radio or TV towers can generate RFI. When EMI noise affects analog signals, this distortion can result in the incorrect transmission of data, just as if static prevented you from hearing a radio station broadcast. However, this type of noise affects digital signals much less. Because digital signals do not depend on subtle amplitude or frequency differences to communicate information, they are more apt to be readable despite distortions caused by EMI noise.

Another form of noise that hinders data transmission is cross talk. Cross talk occurs when a signal traveling on one wire or cable infringes on the signal traveling over an adjacent wire or cable. When cross talk occurs between two cables, it’s called alien cross talk. When it occurs between wire pairs near the source of a signal, it’s known as NEXT (near end cross talk). One potential cause of NEXT is an improper termination—for example, one in which wire insulation has been damaged or wire pairs have been untwisted too far.

If you’ve ever been on the phone and heard the conversation on your second line in the background, you have heard the effects of cross talk. In this example, the current carrying a signal on the second line’s wire imposes itself on the wire carrying your line’s signal, as shown in Figure 3-12. The resulting noise, or cross talk, is equal to a portion of the second line’s signal. Cross talk in the form of overlapping phone conversations is bothersome, but does not usually prevent you from hearing your own line’s conversation. In data networks, however, cross talk can be extreme enough to prevent the accurate delivery of data.

In addition to EMI and cross talk, less obvious environmental influences, including heat, can also cause noise. In every signal, a certain amount of noise is unavoidable. However, engineers have designed a number of ways to limit the potential for noise to degrade a signal. One way is simply to ensure that the strength of the signal exceeds the strength of the noise. Proper cable design and installation are also critical for protecting against noise’s effects. Note that all forms of noise are measured in decibels (dB).

Figure 3-12 Cross talk between wires in a cable
Another transmission flaw is attenuation, or the loss of a signal's strength as it travels away from its source. Just as your voice becomes fainter as it travels farther, so do signals fade with distance. To compensate for attenuation, both analog and digital signals are boosted en route. However, the technology used to boost an analog signal is different from that used to boost a digital signal. Analog signals pass through an amplifier, an electronic device that increases the voltage, or strength, of the signals. When an analog signal is amplified, the noise that it has accumulated is also amplified. This indiscriminate amplification causes the analog signal to worsen progressively. After multiple amplifications, an analog signal may become difficult to decipher. Figure 3-13 shows an analog signal distorted by noise and then amplified once.

When digital signals are repeated, they are actually retransmitted in their original form, without the noise they might have accumulated previously. This process is known as regeneration. A device that regenerates a digital signal is called a repeater. Figure 3-14 shows a digital signal distorted by noise and then regenerated by a repeater.

Amplifiers and repeaters belong to the Physical layer of the OSI model. Both are used to extend the length of a network. Because most networks are digital, however, they typically use repeaters.
Latency  In an ideal world, networks could transmit data instantaneously between sender and receiver, no matter how great the distance between the two. However, in the real world every network is subjected to a delay between the transmission of a signal and its eventual receipt. For example, when you press a key on your computer to save a file to a network server, the file’s data must travel through your NIC, the network wire, one or more connectivity devices, more cabling, and the server’s NIC before it lands on the server’s hard disk. Although electrons travel rapidly, they still have to travel, and a brief delay takes place between the moment you press the key and the moment the server accepts the data. This delay is called latency.

The length of the cable involved affects latency, as does the existence of any intervening connectivity device, such as a router. Different devices affect latency to different degrees. For example, modems, which must modulate both incoming and outgoing signals, increase a connection’s latency far more than hubs, which simply repeat a signal. The most common way to measure latency on data networks is by calculating a packet’s RTT (round trip time), or the length of time it takes for a packet to go from sender to receiver, then back from receiver to sender. RTT is usually measured in milliseconds.

Latency causes problems only when a receiving node is expecting some type of communication, such as the rest of a data stream it has begun to accept. If that node does not receive the rest of the data stream within a given time period, it assumes that no more data is coming. This assumption may cause transmission errors on a network. When you connect multiple network segments and thereby increase the distance between sender and receiver, you increase the network’s latency. To constrain the latency and avoid its associated errors, each type of cabling is rated for a maximum number of connected network segments, and each transmission method is assigned a maximum segment length.

Common Media Characteristics

Now that you are familiar with data-signaling characteristics, you are ready to learn more about the physical and atmospheric paths that these signals traverse. When deciding which kind of transmission media to use, you must match your networking needs with the characteristics of the media. This section describes the characteristics of several types of physical media, including throughput, cost, size and scalability, connectors, and noise immunity. The medium used for wireless transmission, the atmosphere, is discussed in detail in Chapter 8.

Throughput

Perhaps the most significant factor in choosing a transmission method is its throughput. All media are limited by the laws of physics that prevent signals from traveling faster than the speed of light. Beyond that, throughput is limited by the signaling and multiplexing techniques used in a given transmission method. Using fiber-optic cables allows faster throughput than copper or wireless connections. Noise and devices connected to the transmission medium can further limit throughput. A noisy circuit spends more time compensating for the noise and, therefore, has fewer resources available for transmitting data.
Cost

The precise costs of using a particular type of cable or wireless connection are often difficult to pinpoint. For example, although a vendor might quote you the cost-per-foot for new network cabling, you might also have to upgrade some hardware on your network to use that type of cabling. Thus, the cost of upgrading your media would actually include more than the cost of the cabling itself. Not only do media costs depend on the hardware that already exists in a network, but they also depend on the size of your network and the cost of labor in your area (unless you plan to install the cable yourself). The following variables can all influence the final cost of implementing a certain type of media:

- **Cost of installation**—Can you install the media yourself, or must you hire contractors to do it? Will you need to move walls or build new conduits or closets? Will you need to lease lines from a service provider?
- **Cost of new infrastructure versus reusing existing infrastructure**—Can you use existing wiring? In some cases, for example, installing all new Category 6 UTP wiring may not pay off if you can use existing Category 5 UTP wiring. If you replace only part of your infrastructure, will it be easily integrated with the existing media?
- **Cost of maintenance and support**—Reuse of an existing cabling infrastructure does not save any money if it is in constant need of repair or enhancement. Also, if you use an unfamiliar media type, it may cost more to hire a technician to service it. Will you be able to service the media yourself, or must you hire contractors to service it?
- **Cost of a lower transmission rate affecting productivity**—If you save money by reusing existing slower lines, are you incurring costs by reducing productivity? In other words, are you making staff wait longer to save and print reports or exchange e-mail?
- **Cost of obsolescence**—Are you choosing media that may become passing fads, requiring rapid replacement? Will you be able to find reasonably priced connectivity hardware that will be compatible with your chosen media for years to come?

Noise Immunity

As you learned earlier, noise can distort data signals. The extent to which noise affects a signal depends partly on the transmission media. Some types of media are more susceptible to noise than others. The type of media least susceptible to noise is fiber-optic cable, because it does not use electric current, but light waves, to conduct signals.

On most networks, noise is an ever-present threat, so you should take measures to limit its impact on your network. For example, install cabling well away from powerful electromagnetic forces. If your environment still leaves your network vulnerable, choose a type of transmission media that helps to protect the signal from noise. For example, wireless signals are more apt to be distorted by EMI/RFI than signals traveling over a cable. It is also possible to use antinoise algorithms to protect data from being corrupted by noise. If these measures don’t ward off interference, in the case of wired media, you may need to use a metal **conduit**, or pipeline, to contain and further protect the cabling.

Now that you understand data transmission and the factors to consider when choosing a transmission medium, you are ready to learn about different types of transmission media. To qualify for Network+ certification, you must know the characteristics and limitations of each type of media, how to install and design a network with each type, how to troubleshoot networking media problems, and how to provide for future network growth with each option.
Size and Scalability

Three specifications determine the size and scalability of networking media: maximum nodes per segment, maximum segment length, and maximum network length. In cabling, each of these specifications is based on the physical characteristics of the wire and the electrical characteristics of data transmission. The maximum number of nodes per segment depends on attenuation and latency. Each device added to a network segment causes a slight increase in the signal’s attenuation and latency. To ensure a clear, strong, and timely signal, you must limit the number of nodes on a segment.

The maximum segment length depends on attenuation and latency plus the segment type. A network can include two types of segments: populated and unpopulated. A populated segment is a part of a network that contains end nodes. For example, a switch connecting users in a classroom is part of a populated segment. An unpopulated segment, also known as a link segment, is a part of the network that does not contain end nodes, but simply connects two networking devices such as routers.

Segment lengths are limited because after a certain distance, a signal loses so much strength that it cannot be accurately interpreted. The maximum distance a signal can travel and still be interpreted accurately is equal to a segment’s maximum length. Beyond this length, data loss is apt to occur. As with the maximum number of nodes per segment, maximum segment length varies between different cabling types. The same principle of data loss applies to maximum network length, which is the sum of the network’s segment lengths.

Connectors and Media Converters

Connectors are the pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer. Every networking medium requires a specific kind of connector. The type of connectors you use will affect the cost of installing and maintaining the network, the ease of adding new segments or nodes to the network, and the technical expertise required to maintain the network. The connectors you are most likely to encounter on modern networks are illustrated throughout this chapter and shown together in Appendix C.

Connectors are specific to a particular media type, but that doesn’t prevent one network from using multiple media. Some connectivity devices are designed to accept more than one type of media. If you are working with a connectivity device that can’t, you can integrate the two media types by using media converters. A media converter is a piece of hardware that enables networks or segments running on different media to interconnect and exchange signals. For example, suppose a segment leading from your company’s data center to a group of workstations uses fiber-optic cable, but the workgroup hub can only accept twisted pair (copper) cable. In that case, you could use a media converter to interconnect the hub with the fiber-optic cable. The media converter completes the physical connection and also converts the electrical signals from the copper cable to light wave signals that can traverse the fiber-optic cable, and vice versa. Such a media converter is shown in Figure 3-15.

The terms wire and cable are used synonymously in some situations. Strictly speaking, however, wire is a subset of cabling, because the cabling category may also include fiber-optic cable, which is almost never called wire. The exact meaning of the term wire depends on context. For example, if you said, in a somewhat casual way, “We had 6 gigs of data go over the wire last night,” you would be referring to whatever transmission media helped carry the data—whether fiber, radio waves, coax, or UTP.
Coaxial cable, called “coax” for short, was the foundation for Ethernet networks in the 1970s and remained a popular transmission medium for many years. Over time, however, twisted pair and fiber-optic cabling have replaced coax in modern LANs. If you work on long-established networks or cable systems, however, you might have to work with coaxial cable.

Coaxial cable consists of a central metal core (often copper) surrounded by an insulator, a braided metal shielding, called braiding or shield, and an outer cover, called the sheath or jacket. Figure 3-16 depicts a typical coaxial cable. The core may be constructed of one solid metal wire or several thin strands of metal wire. The core carries the electromagnetic signal, and the braided metal shielding acts as both a shield against noise and a ground for the signal. The insulator layer usually consists of a plastic material such as PVC (polyvinyl chloride) or Teflon. It protects the core from the metal shielding, because if the two made contact, the wire would short-circuit. The sheath, which protects the cable from physical damage, may be PVC or a more expensive, fire-resistant plastic.
Because of its shielding, most coaxial cable has a high resistance to noise. It can also carry signals farther than twisted pair cabling before amplification of the signals becomes necessary (although not as far as fiber-optic cabling). On the other hand, coaxial cable is more expensive than twisted pair cable because it requires significantly more raw materials to manufacture.

Coaxial cabling comes in hundreds of specifications, although you are likely to see only two or three types of coax in use on data networks. All types have been assigned an RG specification number. (RG stands for radio guide, which is appropriate because coaxial cabling is used to guide radio frequencies in broadband transmission.) The significant differences between the cable types lie in the materials used for their shielding and conducting cores, which in turn influence their transmission characteristics, such as impedance (or the resistance that contributes to controlling the signal, as expressed in ohms), attenuation, and throughput. Each type of coax is suited to a different purpose. When discussing the size of the conducting core in a coaxial cable, we refer to its American Wire Gauge (AWG) size. The larger the AWG size, the smaller the diameter of a piece of wire. Following is a list of coaxial cable specifications used with data networks:

- **RG-6**—A type of coaxial cable that is characterized by an impedance of 75 ohms and contains an 18 AWG conducting core. The core is usually made of solid copper. RG-6 coaxial cables are used, for example, to deliver broadband cable Internet service and cable TV, particularly over long distances. If a service provider such as Comcast or Charter supplies you with Internet service, the cable entering your home is RG-6.

- **RG-8**—A type of coaxial cable characterized by a 50-ohm impedance and a 10 AWG core. RG-8 provided the medium for the first Ethernet networks, which followed the now-obsolete 10Base-5 standard. The 10 represents its maximum potential throughput of 10 Mbps, the Base stands for baseband transmission, and the 5 represents its maximum segment length of 500 meters. As you’ll learn, all Ethernet standards established by IEEE follow a similar naming convention. 10Base-5 is also known as Thicknet. You will never find Thicknet on new networks, but you might find it on older networks.

- **RG-58**—A type of coaxial cable characterized by a 50-ohm impedance and a 24 AWG core. RG-58 was a popular medium for Ethernet LANs in the 1980s. With a smaller diameter than RG-8, RG-58 is more flexible and easier to handle and install. Its core is typically made of several thin strands of copper. The Ethernet standard that relies on RG-58 coax is 10Base-2, with the 10 representing its data transmission rate of 10 Mbps, the Base representing the fact that it uses baseband transmission, and the 2 representing its maximum segment length of 185 meters (or roughly 200). Because it is thinner than Thicknet cables, it is also called Thinnet. Like Thicknet, Thinnet is almost never used on modern networks, although you might encounter it on networks installed in the 1980s.

- **RG-59**—A type of coaxial cable characterized by a 75-ohm impedance and a 20 or 22 AWG core, usually made of braided copper. Less expensive but suffering from greater attenuation than the more common RG-6 coax, RG-59 is still used for relatively short connections, for example, when distributing video signals from a central receiver to multiple monitors within a building.

The two coaxial cable types commonly used in networks today, RG-6 and RG-59, can terminate with one of two connector types: an F-type connector or a BNC connector. F-type
connectors attach to coaxial cable so that the pin in the center of the connector is the conducting core of the cable. Therefore, F-type connectors require that the cable contain a solid metal core. After being attached to the cable by crimping or compression, connectors are threaded and screw together like a nut and bolt assembly. A male F-type connector, or plug, attached to coax is shown in Figure 3-17. A corresponding female F-type connector, or jack, would be coupled with the male connector. F-type connectors are most often used with RG-6 cables.

BNC stands for Bayonet Neill-Concelman, a term that refers to both a style of connection and its two inventors. (Sometimes the term British Naval Connector is also used.) A BNC connector is crimped, compressed, or twisted onto a coaxial cable. It connects to another BNC connector via a turning and locking mechanism—this is the bayonet coupling referenced in its name. Unlike an F-type connector, male BNC connectors do not use the central conducting core of the coax as part of the connection, but provide their own conducting pin. BNC was once the standard for connecting coaxial-based Ethernet segments. Today, though, you’re more likely to find BNC connectors used with RG-59 coaxial cable. Less commonly, they’re also used with RG-6. Figure 3-18 shows a BNC connector that is not attached to a cable.

When sourcing connectors for coaxial cable, you need to specify the type of cable you are using. For instance, when working with RG-6 coax, choose an F-type connector made specifically for RG-6 cables. That way, you’ll be certain that the connectors and cable share the same impedance rating. If impedance ratings don’t match, data errors will result and network performance will suffer.

Next, you will learn about a medium you are more likely to find on modern LANs, twisted pair cable.
Twisted Pair Cable

Twisted pair cable consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm (approximately the diameter of a straight pin). Every two wires are twisted around each other to form pairs, and all the pairs are encased in a plastic sheath, as shown in Figure 3-19. The number of pairs in a cable varies, depending on the cable type.

The more twists per foot in a pair of wires, the more resistant the pair will be to cross talk. Higher-quality, more expensive twisted pair cable contains more twists per foot. The number of twists per meter or foot is known as the twist ratio. Because twisting the wire pairs more tightly requires more cable, however, a high twist ratio can result in greater attenuation. For
optimal performance, cable manufacturers must strike a balance between minimizing cross talk and reducing attenuation.

Because twisted pair is used in such a wide variety of environments and for a variety of purposes, it comes in hundreds of different designs. These designs vary in their twist ratio, the number of wire pairs that they contain, the grade of copper used, the type of shielding (if any), and the materials used for shielding, among other things. A twisted pair cable may contain from 1 to 4200 wire pairs. Modern networks typically use cables that contain four wire pairs, in which one pair is dedicated to sending data and another pair is dedicated to receiving data.

In 1991, two standards organizations, the TIA/EIA, finalized their specifications for twisted pair wiring in a standard called “TIA/EIA 568.” Since then, this body has continually revised the international standards for new and modified transmission media. Its standards now cover cabling media, design, and installation specifications. The TIA/EIA 568 standard divides twisted pair wiring into several categories. The types of twisted pair wiring you will hear about most often are Cat (category) 3, 4, 5, 5e, 6, and 6e, and Cat 7. All of the category cables fall under the TIA/EIA 568 standard. Modern LANs use Cat 5 or higher wiring.

Twisted pair cable is relatively inexpensive, flexible, and easy to install, and it can span a significant distance before requiring a repeater (though not as far as coax). Twisted pair cable easily accommodates several different topologies, although it is most often implemented in star or star-hybrid topologies. Furthermore, twisted pair can handle the faster networking transmission rates currently being employed. Due to its wide acceptance, it will probably continue to be updated to handle the even faster rates that will emerge in the future. All twisted pair cable falls into one of two categories: STP (shielded twisted pair) or UTP (unshielded twisted pair).

**STP (Shielded Twisted Pair)**

STP (shielded twisted pair) cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. Some STP use a braided copper shielding. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. It also contains the electrical energy of the signals inside. The shielding may be grounded to enhance its protective effects. The effectiveness of STP’s shield depends on the level and type of environmental noise, the thickness and material used for the shield, the grounding mechanism, and the symmetry and consistency of the shielding. Figure 3-20 depicts an STP cable.

**UTP (Unshielded Twisted Pair)**

UTP (unshielded twisted pair) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP. Figure 3-21 depicts a typical UTP cable.

Earlier, you learned that the TIA/EIA consortium designated standards for twisted pair wiring. To manage network cabling, you need to be familiar with the standards for use on modern networks, particularly Cat 3 and Cat 5 or higher:

- **Cat 3 (Category 3)**—A form of UTP that contains four wire pairs and can carry up to 10 Mbps of data with a possible bandwidth of 16 MHz. Cat 3 has typically been used
for 10-Mbps Ethernet or 4-Mbps token ring networks. Where it remains, network administrators are replacing their existing Cat 3 cabling with Cat 5 or better cabling to accommodate higher throughput.

- **Cat 4 (Category 4)**—A form of UTP that contains four wire pairs and can support up to 16 Mbps throughput. Uncommon on new networks, Cat 4 may be found on older 16 Mbps token ring or 10 Mbps Ethernet networks. It is guaranteed for signals as high as 20 MHz and provides more protection against cross talk and attenuation than Cat 3.

- **Cat 5 (Category 5)**—A form of UTP that contains four wire pairs and supports up to 1000 Mbps throughput and a 100-MHz signal rate. Figure 3-22 depicts a typical Cat 5 UTP cable with its twisted pairs untwisted, allowing you to see their matched color coding. For example, the wire that is colored solid orange is twisted around the wire that is part orange and part white to form the pair responsible for transmitting data.
It can be difficult to tell the difference between four-pair Cat 3 cables and four-pair Cat 5 or Cat 5e cables. However, some visual clues can help. On Cat 5 cable, the jacket is usually stamped with the manufacturer’s name and cable type, including the Cat 5 specification. A cable whose jacket has no markings is more likely to be Cat 3. Also, pairs in Cat 5 cables have a significantly higher twist ratio than pairs in Cat 3 cables. Although Cat 3 pairs might be twisted as few as three times per foot, Cat 5 pairs are twisted at least 12 times per foot. Other clues, such as the date of installation (old cable is more likely to be Cat 3), looseness of the jacket (Cat 3’s jacket is typically looser than Cat 5’s), and the extent to which pairs are untwisted before a termination (Cat 5 can tolerate only a small amount of untwisting) are also helpful, though less definitive.

- **Cat 5e (Enhanced Category 5)**—A higher-grade version of Cat 5 wiring that contains high-quality copper, offers a high twist ratio, and uses advanced methods for reducing cross talk. Cat 5e can support a signaling rate as high as 350 MHz, more than triple the capability of regular Cat 5.

- **Cat 6 (Category 6)**—A twisted pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheath covers the second foil layer. The foil insulation provides excellent resistance to cross talk and enables Cat 6 to support a 250-MHz signaling rate and at least six times the throughput supported by regular Cat 5.

- **Cat 6e (Enhanced Category 6)**—A higher-grade version of Cat 6 wiring that reduces attenuation and cross talk, and allows for potentially exceeding traditional network segment length limits. Cat 6e is capable of a 550 MHz signaling rate and can reliably transmit data at multi-Gigabit per second rates.

- **Cat 7 (Category 7)**—A twisted pair cable that contains multiple wire pairs, each surrounded by its own shielding, then packaged in additional shielding beneath the sheath. Although standards have not yet been finalized for Cat 7, cable supply companies are selling it, and some organizations are installing it. One advantage to Cat 7 cabling is that it can support signal rates up to 1 GHz. However, it requires different
connectors than other versions of UTP because its twisted pairs must be more isolated from each other to ward off cross talk. Because of its added shielding, Cat 7 cabling is also larger and less flexible than other versions of UTP cable. Cat 7 is uncommon on modern networks, but it will likely become popular as the final standard is released and network equipment is upgraded.

Technically, because Cat 6 and Cat 7 contain wires that are individually shielded, they are not unshielded twisted pair. Instead, they are more similar to shielded twisted pair.

UTP cabling may be used with any one of several IEEE Physical layer networking standards that specify throughput maximums of 10, 100, 1000, and even 10,000 Mbps. These standards are described in detail in Chapter 5.

Comparing STP and UTP

STP and UTP share several characteristics. The following list highlights their similarities and differences:

- **Throughput**—STP and UTP can both transmit data at 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps, depending on the grade of cabling and the transmission method in use.
- **Cost**—STP and UTP vary in cost, depending on the grade of copper used, the category rating, and any enhancements. Typically, STP is more expensive than UTP because it contains more materials and it has a lower demand. It also requires grounding, which can lead to more expensive installation. High-grade UTP, can be expensive too, however. For example, Cat 6e costs more per foot than Cat 5 cabling.
- **Connector**—STP and UTP use RJ-45 (Registered Jack 45) modular connectors and data jacks, which look similar to analog telephone connectors and jacks. However, telephone connections follow the RJ-11 (Registered Jack 11) standard. Figure 3-23 shows a close-up of an RJ-45 connector for a cable containing four wire pairs. For comparison, this figure also shows a traditional RJ-11 phone line connector. All types of Ethernet that rely on twisted pair cabling use RJ-45 connectors.
Noise immunity—Because of its shielding, STP is more noise resistant than UTP. On the other hand, signals transmitted over UTP may be subject to filtering and balancing techniques to offset the effects of noise.

Size and scalability—The maximum segment length for both STP and UTP is 100 m, or 328 feet, on Ethernet networks that support data rates from 1 Mbps to 10 Gbps. These accommodate a maximum of 1024 nodes. (However, attaching so many nodes to a segment is very impractical, as it would slow traffic and make management nearly impossible.)

Terminating Twisted Pair Cable

Imagine you have been sent to one of your employer’s remote offices and charged with upgrading all the old Cat 3 patch cables in a data closet with new, Cat 6 patch cables. A patch cable is a relatively short (usually between 3 and 25 feet) length of cabling with connectors at both ends. Based on the company’s network documentation, you brought 50 premade cables with RJ-45 plugs on both ends, which you purchased from an online cable vendor. At the remote location, however, you discover that its data closet actually contains 60 patch cables that need replacing. No additional premade cables are available at that office, and you don’t have time to order more. Luckily, you have brought your networking tool kit with spare RJ-45 plugs and a spool of Cat 6 cable. Knowing how to properly terminate Cat 6 cables allows you to make all the new patch cables you need and complete your work. Even if you are never faced with this situation, it’s likely that at some point you will have to replace an RJ-45 connector on an existing cable. This section describes how to terminate twisted pair cable.

Proper cable termination is a basic requirement for two nodes on a network to communicate. Beyond that, however, poor terminations can lead to loss or noise—and consequently, errors—in a signal. Closely following termination standards, then, is critical. TIA/EIA has specified two different methods of inserting twisted pair wires into RJ-45 plugs: TIA/EIA 568A and TIA/EIA 568B. Functionally, there is no difference between the standards. You only have to be certain that you use the same standard on every RJ-45 plug and jack on your network, so that data is transmitted and received correctly. Figure 3-24 depicts pin numbers and assignments (or pinouts) for the TIA/EIA 568A standard when used on an Ethernet network. Figure 3-25 depicts pin numbers and assignments for the TIA/EIA 568B standard. (Although networking professionals commonly refer to wires in Figures 3-24 and 3-25 as transmit and receive, their original T and R designations stand for Tip and Ring, terms that come from early telephone technology but are irrelevant today.)

If you terminate the RJ-45 plugs at both ends of a patch cable identically, following one of the TIA/EIA 568 standards, you will create a straight-through cable. A straight-through cable is so named because it allows signals to pass “straight through” from one end to the other. This is the type used to connect a workstation to a hub or router, for example. However, in some cases you may want to reverse the pin locations of some wires—for example, when you want to connect two workstations without using a connectivity device or when you want to connect two hubs through their data ports. This can be accomplished through the use of a crossover cable, a patch cable in which the termination locations of the transmit and receive wires on one end of the cable are reversed, as shown in Figure 3-26. In this example, the TIA/EIA 568B standard is used on the left side, whereas the TIA/EIA 568A standard is used on the right side. Notice that only pairs 2 and 3 are switched, because those are the pairs sending and receiving data.
## 2.4 TIA/EIA 568A Standard Terminations

### Figure 3-24

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Color</th>
<th>Pair #</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White with green stripe</td>
<td>3</td>
<td>Transmit +</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>3</td>
<td>Transmit -</td>
</tr>
<tr>
<td>3</td>
<td>White with orange stripe</td>
<td>2</td>
<td>Receive +</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>1</td>
<td>Unused</td>
</tr>
<tr>
<td>5</td>
<td>White with blue stripe</td>
<td>1</td>
<td>Unused</td>
</tr>
<tr>
<td>6</td>
<td>Orange</td>
<td>2</td>
<td>Receive -</td>
</tr>
<tr>
<td>7</td>
<td>White with brown stripe</td>
<td>4</td>
<td>Unused</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>4</td>
<td>Unused</td>
</tr>
</tbody>
</table>

**Figure 3-24** TIA/EIA 568A standard terminations

## 2.4 TIA/EIA 568B Standard Terminations

### Figure 3-25

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Color</th>
<th>Pair #</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White with orange stripe</td>
<td>2</td>
<td>Transmit +</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>2</td>
<td>Transmit -</td>
</tr>
<tr>
<td>3</td>
<td>White with green stripe</td>
<td>3</td>
<td>Receive +</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>1</td>
<td>Unused</td>
</tr>
<tr>
<td>5</td>
<td>White with blue stripe</td>
<td>1</td>
<td>Unused</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>3</td>
<td>Receive -</td>
</tr>
<tr>
<td>7</td>
<td>White with brown stripe</td>
<td>4</td>
<td>Unused</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>4</td>
<td>Unused</td>
</tr>
</tbody>
</table>

**Figure 3-25** TIA/EIA 568B standard terminations
The tools you’ll need to terminate a twisted-pair cable with an RJ-45 plug are a wire cutter, wire stripper, and crimping tool, which are pictured in Figures 3-27, 3-28, and 3-29, respectively. (In fact, you can find a single device that contains all three of these tools.)

Following are the steps to create a straight-through patch cable. To create a crossover cable, you would simply reorder the wires in Step 4 to match Figure 3-26. The process of fixing wires inside the connector is called crimping, and it is a skill that requires practice—so don’t be discouraged if the first cable you create doesn’t reliably transmit and receive data. You’ll get to practice making cables in the end-of-chapter Hands-on Projects:

1. Using the wire cutter, make a clean cut at both ends of the twisted-pair cable.
2. Using the wire stripper, remove the sheath off of one end of the twisted-pair cable, beginning at approximately one inch from the end. Be careful to neither damage nor remove the insulation that’s on the twisted pairs inside.
3. Separate the four wire pairs slightly. Carefully unwind each pair no more than ½ inch.
4. To make a straight-through cable, align all eight wires on a flat surface, one next to the other, ordered according to their colors and positions listed in Figure 3-25. (It might be
helpful first to “groom”—or pull steadily across the length of—the unwound section of each wire to straighten it out and help it stay in place.

5. Keeping the wires in order and in line, gently slide them all the way into their positions in the RJ-45 plug.

6. After the wires are fully inserted, place the RJ-45 plug in the crimping tool and press firmly to crimp the wires into place. (Be careful not to rotate your hand or the wire as you do this, otherwise only some of the wires will be properly terminated.) Crimping causes the internal RJ-45 pins to pierce the insulation of the wire, thus creating contact between the two conductors.

7. Now remove the RJ-45 connector from the crimping tool. Examine the end and see whether each wire appears to be in contact with the pin. It may be difficult to tell simply by looking at the connector. The real test is whether your cable will successfully transmit and receive signals.

8. Repeat Steps 2 through 7 for the other end of the cable. After completing Step 7 for the other end, you will have created a straight-through patch cable.

Even after you feel confident making your own cables, it’s a good idea to verify that they can transmit and receive data at the necessary rates using a cable tester. Cable testing is discussed in Chapter 13, Troubleshooting Network Problems.

In this section you’ve learned about twisted pair wiring, the most common network transmission medium in use today. The next section describes a transmission medium that, due to its many advantages, is enjoying ever-growing popularity.
Fiber-optic cable, or simply fiber, contains one or several glass or plastic fibers at its center, or core. Data is transmitted via pulsing light sent from a laser (in the case of 1- and 10-Gigabit technologies) or an LED (light-emitting diode) through the central fibers. Surrounding the fibers is a layer of glass or plastic called cladding. The cladding has a different density from the glass or plastic in the strands. It reflects light back to the core in patterns that vary depending on the transmission mode. This reflection allows the fiber to bend around corners without diminishing the integrity of the light-based signal. Outside the cladding, a plastic buffer protects the cladding and core. Because the buffer is opaque, it also absorbs any light that might escape. To prevent the cable from stretching, and to protect the inner core further, strands of Kevlar (a polymeric fiber) surround the plastic buffer. Finally, a plastic sheath covers the strands of Kevlar. Figure 3-30 shows a fiber-optic cable with multiple, insulated fibers.

Like twisted pair and coaxial cabling, fiber-optic cabling comes in a number of different varieties, depending on its intended use and the manufacturer. For example, fiber-optic cables used to connect the facilities of large telephone and data carriers may contain as many as 1000 fibers and be heavily sheathed to prevent damage from extreme environmental conditions. At the other end of the spectrum, fiber-optic patch cables for use on LANs may contain only two strands of fiber and be pliable enough to wrap around your hand.

However, all fiber cable variations fall into two categories: single-mode and multimode.

**SMF (Single-Mode Fiber)**

SMF (single-mode fiber) uses a narrow core (less than 10 microns in diameter) through which light generated by a laser travels over one path, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows single-mode fiber to accommodate the highest bandwidths and longest distances (without requiring repeaters) of all network transmission media. Single-mode fiber may be used to connect a carrier’s two facilities. However, it costs too much to be considered for use on

![Figure 3-30 A fiber-optic cable](image)
typical LANs and WANs. Figure 3-31 depicts a simplified version of how signals travel over single-mode fiber.

**MMF (Multimode Fiber)**

MMF (multimode fiber) contains a core with a larger diameter than single-mode fiber (between 50 and 115 microns in diameter; the most common size is 62.5 microns) over which many pulses of light generated by a laser or LED travel at different angles. It is commonly found on cables that connect a router to a switch or a server on the backbone of a network. Figure 3-32 depicts a simplified view of how signals travel over multimode fiber.

Because of its reliability, fiber is currently used primarily as a cable that connects the many segments of a network. Fiber-optic cable provides the following benefits over copper cabling:

- Extremely high throughput
- Very high resistance to noise
- Excellent security
- Ability to carry signals for much longer distances before requiring repeaters than copper cable
- Industry standard for high-speed networking

The most significant drawback to the use of fiber is that covering a certain distance with fiber-optic cable is much more expensive than using twisted pair cable. Also, fiber-optic cable requires special equipment to splice, which means that quickly repairing a fiber-optic
cable in the field (given little time or resources) can be difficult. Fiber’s characteristics are summarized in the following list:

- **Throughput**—Fiber has proved reliable in transmitting data at rates that can reach 100 gigabits (or 100,000 megabits) per second per channel. (Rates demanded by most networks are lower, however.) Fiber’s amazing throughput is partly due to the physics of light traveling through glass. Unlike electrical pulses traveling over copper, the light experiences virtually no resistance. Therefore, light-based signals can be transmitted at faster rates and with fewer errors than electrical pulses. In fact, a pure glass strand can accept up to 1 billion laser light pulses per second. Its high throughput capability makes it suitable for network backbones and for serving applications that generate a great deal of traffic, such as video or audio conferencing.

- **Cost**—Fiber-optic cable is the most expensive transmission medium. Because of its cost, most organizations find it impractical to run fiber to every desktop. Not only is the cable itself more expensive than copper cabling, but fiber-optic NICs and hubs can cost as much as five times more than NICs and hubs designed for UTP networks. In addition, hiring skilled fiber cable installers costs more than hiring twisted pair cable installers.

- **Connector**—With fiber cabling, you can use any of 10 different types of connectors. Figures 3-33, 3-34, 3-35, and 3-36 show four of the most common connector types: the ST (straight tip), SC (subscriber connector or standard connector), LC (local connector), and MT-RJ (mechanical transfer registered jack). Each of these connectors can be obtained for single-mode or multimode fiber-optic cable. Existing fiber networks typically use ST or SC connectors. However, LC and MT-RJ connectors are used on the very latest fiber-optic technology. LC and MT-RJ connectors are preferable to ST and SC connectors because of their smaller size, which allows for a higher density of connections at each termination point. The MT-RJ connector is unique because it contains two strands of multimode fiber in a single ferrule, which is a short tube within a connector that encircles the fiber and keeps it properly aligned. With two strands in each ferrule, a single MT-RJ connector provides for a duplex signaling.
Noise immunity—Because fiber does not conduct electrical current to transmit signals, it is unaffected by EMI. Its impressive noise resistance is one reason why fiber can span such long distances before it requires repeaters to regenerate its signal.

Size and scalability—Depending on the type of fiber-optic cable used, segment lengths vary from 150 to 40,000 meters. This limit is due primarily to optical loss, or the degradation of the light signal after it travels a certain distance away from its source (just as the light of a flashlight dims after a certain number of feet). Optical loss accrues over long distances and grows with every connection point in the fiber network. Dust or oil in a connection (for example, from people handling the fiber while splicing it) can further exacerbate optical loss.
DTE (Data Terminal Equipment) and DCE (Data Circuit-Terminating Equipment) Connector Cables

So far you have learned about the kinds of physical media used between connectivity devices and with nodes on a LAN or WAN. This section describes some common cable types used to connect DTE (data terminal equipment) and DCE (data circuit-terminating equipment) found on a network. DTE refers to any end-user device, such as a workstation, terminal (essentially a monitor with little or no independent data-processing capability), or a console (for example, the user interface for a router). DCE refers to a device, such as a multiplexer or modem, that processes signals. Importantly, DCE also supplies a clock signal to synchronize transmission between DTE and DCE. Most connectivity devices, such as routers and switches, can be configured to act as DTE or DCE, depending on the context in which they’re used.

DTE and DCE are connected through special, typically short, cables, that attach to the equipment’s serial interface. Serial refers to a style of data transmission in which the pulses that represent bits follow one another along a single transmission line. In other words, they are issued sequentially, not simultaneously. A serial cable is one that carries serial transmissions. Several types of serial cables exist.

EIA/TIA has codified a popular serial data transmission method known as RS-232 (Recommended Standard 232). This Physical layer standard specifies, among other things, signal voltage and timing, plus the characteristics of compatible interfaces. Different connector types comply with this standard, including RJ-45 connectors, DB-9 connectors, and DB-25 connectors. You are already familiar with RJ-45 plugs. Figures 3-37 and 3-38 illustrate male DB-9 and DB-25 connectors, respectively. Notice that the arrangement of the pins on both connectors resembles a sideways letter D. Also notice that a DB-9 connector contains 9 contact points and a DB-25 connector contains 25.

You might connect a workstation (DTE) and an external modem (DCE) using RS-232. This was its primary use for many years. However, as an administrator on today’s networks, you’re more likely to use an RS-232 connection between a PC and a router to make your PC act as a console for configuring and managing that router. In fact, a higher-end router designed for use in your data center (not the kind of router you’d use at home) usually...
comes with an RS-232-compatible cable. The serial interface on the back of the connectivity device is often labeled “Console.” (This is not to say that a serial cable is the only way of connecting to a router for configuring and managing it. However, if the router is brand new or for some other reason lacks an IP address, you need to access it directly, and not via a network connection.)

You can find RS-232 cables with different types of connectors at either end. For example, many Cisco routers come with a console port that’s RJ-45 compliant. If you wanted to connect such a router to your laptop’s DB-9 serial port, you could find an RS-232 cable with an RJ-45 plug on one end and a DB-9 plug on the other.

The fact that a serial cable terminates in an RJ-45 connector does not mean it will work if plugged into a device’s RJ-45 Ethernet port! When using a serial cable with an RJ-45 connector, be certain to plug it into the appropriate serial interface.

In addition to using different connector types, the termination points on RS-232 cables can be arranged in various ways, depending on the cable’s purpose. Earlier you learned about the difference between straight-through and crossover cables in the context of terminating twisted pair cables. An RS-232 cable, whether it uses DB-9, DB-25 or RJ-45 connectors, can also be straight-through. You also have the option of reversing the transmit and receive pins on one end, thereby making it into a crossover cable. Among other things, you could use such a crossover cable to directly connect two routers via their serial interfaces.

Yet another type of cable is a rollover cable (or rolled over cable). In a rollover cable, the usual wire positions are exactly reversed in one of the two RJ-45 terminations. (Imagine you were making a cable according to the steps described earlier in this chapter and flipped one end upside-down before inserting it into the RJ-45 jack.) Rollover cables are mainly used to connect a console to a connectivity device, such as a router. Do not confuse them with crossover cables, which reverse the transmit and receive pairs (pinouts 1, 2, 3 and 6) from one end of a cable to the other.

You’ll learn more about the connectivity devices, such as routers and switches, that use DTE and DCE connector cables in Chapter 6. The following section describes how to arrange physical networking media between end users and connectivity devices on a LAN or WAN.
Structured Cabling

Organizations that pay attention to their cable plant—the hardware that makes up the enterprise-wide cabling system—are apt to experience fewer Physical layer network problems, smoother network expansions, and simpler network troubleshooting. Following the cabling standards and best practices described in this chapter can help.

If you were to tour hundreds of data centers and equipment rooms at established enterprises you would see similar cabling arrangements. That’s because most organizations follow a cabling standard. One popular standard is TIA/EIA’s joint 568 Commercial Building Wiring Standard, also known as structured cabling, for uniform, enterprise-wide, multivendor cabling systems. The standard suggests how networking media can best be installed to maximize performance and minimize upkeep. Structured cabling applies no matter what type of media or transmission technology a network uses. (It does, however, assume a network based on the star topology.) In other words, it’s designed to work just as well for 10 Mbps networks as it does for 10 Gbps networks. Structured cabling is based on a hierarchical design that begins where a telecommunications company’s service enters a building and ends at a user’s workstation. Figure 3-39 illustrates the different components of structured cabling in an enterprise from a bird’s eye view. Figure 3-40 gives a glimpse of how structured cabling appears within a building (in this case, one that is not part of a larger, enterprise-wide network). Detailed descriptions of the components referenced in these figures follow:

- **Entrance facilities**—The facilities necessary for a service provider (whether it is a local phone company, Internet service provider, or long-distance carrier) to connect with another organization’s LAN or WAN. Entrance facilities may include fiber-optic cable and multiplexers, coaxial cable, UTP, satellite or wireless transceivers, and other devices or cabling. If the entrance facilities are supplied by a telecommunications carrier and rely on UTP, they may come in the form of 25-pair wire. As the name suggests, 25-pair wire is a bundle of 25 wire pairs. As you might expect, 100-pair wire contains 100 twisted wire pairs. More commonly, however, entrance facilities depend...

---

**Figure 3-39** TIA/EIA structured cabling in an enterprise
on fiber-optic cable. The entrance facility designates where the telecommunications service provider accepts responsibility for the (external) connection. The point of division between the service provider’s network and the internal network is also known as the demarcation point (or demarc).

- **MDF (main distribution frame)**—Also known as the main cross-connect, the first point of interconnection between an organization’s LAN or WAN and a service provider’s facility. An MDF typically includes connectivity devices, such as switches and routers, and media, such as fiber-optic cable, capable of the greatest throughput. Often, it also houses an organization’s main servers. In an enterprise-wide network, equipment in an MDF connects to equipment housed in another building’s IDF. Sometimes the MDF is simply known as the computer room or equipment room.

- **Cross-connect facilities**—The points where circuits interconnect with other circuits. For example, when an MDF accepts UTP from a service provider, the wire pairs terminate at a punch-down block. A **punch-down block** is a panel of data receptors into which twisted pair wire is inserted, or punched down, to complete a circuit. Punch-down blocks were for many years the standard method of terminating telephone circuits,
the best known type being a 66 block. Another, known as the 100 block, meets standards for Cat 5 or better UTP terminations, and therefore, is used on data networks. Note that both 66 block and 100 block versions are available in several different capacities. That is, their numerical designation does not represent the number of wire pairs each can terminate. From a punch-down block, wires are distributed to a patch panel, a wall-mounted panel of data receptors. Figure 3-41 shows a patch panel and Figure 3-42 shows a punch-down block. A patch panel allows the insertion of patch cables. Note that cross-connect facilities are not limited to the MDF and may be used in other equipment rooms that are part of a building’s cable infrastructure.

- **IDF (intermediate distribution frame)**—A junction point between the MDF and concentrations of fewer connections—for example, those that terminate in a telecommunications closet

- ** Backbone wiring**—The cables or wireless links that provide interconnection between entrance facilities and MDFs, MDFs and IDF, and IDF and telecommunications closets. One component of the backbone is given a special term: *vertical cross-connect*. A vertical cross-connect runs between a building’s floors. For example, it might connect an MDF and IDF or IDF and telecommunications closets (described next) within a
building. The TIA/EIA standard designates distance limitations for backbones of varying cable types, as specified in Table 3-2. On modern networks, backbones are usually composed of fiber-optic or UTP cable.

- **Telecommunications closet**—Also known as a “telco room,” it contains connectivity for groups of workstations in its area, plus cross-connections to IDF’s or, in smaller organizations, an MDF. Large organizations may have several telco rooms per floor, but the TIA/EIA standard specifies at least one per floor. Telecommunications closets typically house patch panels, punch-down blocks, and connectivity devices for a work area. Because telecommunications closets are usually small, enclosed spaces, good cooling and ventilation systems are important to maintaining a constant temperature.

- **Horizontal wiring**—This is the wiring that connects workstations to the closest telecommunications closet. TIA/EIA recognizes three possible cabling types for horizontal wiring: STP, UTP, or fiber-optic cable. The maximum allowable distance for horizontal wiring is 100 m. This span includes 90 m to connect a data jack on the wall to the telecommunications closet plus a maximum of 10 m to connect a workstation to the data jack on the wall. Figure 3-43 depicts a horizontal wiring configuration.

- **Work area**—An area that encompasses all patch cables and horizontal wiring necessary to connect workstations, printers, and other network devices from their NICs to the telecommunications closet. The TIA/EIA standard calls for each wall jack to contain at least one voice and one data outlet, as pictured in Figure 3-44. Realistically,

### Table 3-2 TIA/EIA specifications for backbone cabling

<table>
<thead>
<tr>
<th>Cable type</th>
<th>Cross-connects to telecommunications closet</th>
<th>MDF or IDF to telecommunications closet</th>
<th>Cross-connects to IDF or MDF</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTP</td>
<td>800 m (voice specification)</td>
<td>500 m</td>
<td>300 m</td>
</tr>
<tr>
<td>Single-mode fiber</td>
<td>3000 m</td>
<td>500 m</td>
<td>1500 m</td>
</tr>
<tr>
<td>Multimode fiber</td>
<td>2000 m</td>
<td>500 m</td>
<td>1500 m</td>
</tr>
</tbody>
</table>

![Figure 3-43](Figure 3-43 Horizontal wiring)
you will encounter a variety of wall jacks. For example, in a student computer lab lacking phones, a wall jack with a combination of voice and data outlets is unnecessary.

Figure 3-45 illustrates a cable installation using UTP from the telecommunications closet to the work area.

Knowing the standards for cabling a building or enterprise is key, but until you have practiced terminating, running, and testing cables, this knowledge is only theoretical. The following section provides some practical information that you can apply when working with physical networking media.
Best Practices for Cable Installation and Management

So far, you have read about the variety of cables used in networking and the limitations inherent in each. You may worry that with hundreds of varieties of cable, choosing the correct one and making it work with your network is next to impossible. The good news is that if you follow both the manufacturers’ installation guidelines and the TIA/EIA standards, you are almost guaranteed success. Many network problems can be traced to poor cable installation techniques. For example, if you don’t crimp twisted pair wires in the correct position in an RJ-45 connector, the cable will fail to transmit or receive data (or both—in which case, the cable will not function at all). Installing the wrong grade of cable can either cause your network to fail or render it more susceptible to damage.

The art of proper cabling could fill an entire book. If you plan to specialize in cable installation, design, or maintenance, you should invest in a reference dedicated to this topic. As a network professional, you will likely occasionally add new cables to a room or telecommunications closet, repair defective cable ends, or install a data outlet. Following are some cable installation tips that will help prevent Physical layer failures:

- Do not untwist twisted pair cables more than one-half inch before inserting them into the punch-down block.
- Do not leave more than 1 inch of exposed (stripped) cable before a twisted pair termination. Doing so will increase the possibility for cross talk and data errors.
- Pay attention to the bend radius limitations for the type of cable you are installing. **Bend radius** is the radius of the maximum arc into which you can loop a cable before you will impair data transmission. Generally, a twisted pair cable’s bend radius is equal to or greater than four times the diameter of the cable. Be careful not to exceed it.
- Use a cable tester to verify that each segment of cabling you install transmits data reliably. This practice will prevent you from later having to track down errors in multiple, long stretches of cable. Chapter 13, which covers troubleshooting network problems, explains the tools and methods needed to test cable continuity.
- Avoid cinching cables so tightly that you squeeze their outer covering, a practice that leads to difficult-to-diagnose data errors.
- Avoid laying cable across the floor where it might sustain damage from rolling chairs or foot traffic. If you must take this tack, cover the cable with a cable protector.
- Install cable at least 3 feet away from fluorescent lights or other sources of EMI. This will reduce the possibility for noise to affect your network’s signals.
- Always leave some slack in cable runs. Stringing cable too tightly risks connectivity and data transmission problems.
- If you run cable in the **plenum**, the area above the ceiling tile or below the subflooring, make sure the cable sheath is plenum-rated, and consult with local electric installation codes to be certain you are installing it correctly. A plenum-rated cable is more fire resistant, and if burned, produces less smoke than other cables.
- Pay attention to grounding requirements and follow them religiously.
- Adhering to structured cabling hierarchies is only part of a smart cable management strategy. You or your network manager should also specify standards for the types of
cable used by your organization and maintain a list of approved cabling vendors. Keep a supply room stocked with spare parts so that you can easily and quickly replace defective parts.

- Create documentation for your cabling plant, including the locations, installation dates, lengths, and grades of installed cable. Label every data jack, punch-down block, and connector. Use color-coded cables for different purposes (cables can be purchased in a variety of sheath colors). For example, you might want to use pink for patch cables, green for horizontal wiring, and gray for vertical (backbone) wiring. Be certain to document your color schemes.

- Keep your cable plant documentation in a centrally accessible location and be certain to update it as you change the network. The more you document, the easier it will be to move or add cable segments.

- Finally, create a plan for expanding your cabling plant. For example, if your organization is rapidly enlarging, consider replacing your backbone with fiber and leave plenty of space in your telecommunications closets for more racks.

Chapter Summary

- Information can be transmitted via two methods: analog or digital. Analog signals are continuous waves that result in variable and inexact transmission. Digital signals are based on electrical or light pulses that represent information encoded in binary form.

- In half-duplex transmission, signals can travel in both directions over a medium but in only one direction at a time. When signals can travel in both directions over a medium simultaneously, the transmission is considered full-duplex.

- A form of transmission that allows multiple signals to travel simultaneously over one medium is known as multiplexing. In multiplexing, the single medium is logically separated into multiple channels, or subchannels.

- Throughput is the amount of data that the medium can transmit during a given period of time. Throughput is usually measured in bits per second and depends on the physical nature of the medium.

- Baseband is a form of transmission in which digital signals are sent through direct current pulses applied to the wire. Baseband systems can transmit only one signal, or one channel, at a time. Broadband, on the other hand, uses modulated analog frequencies to transmit multiple signals over the same wire.

- Noise is interference that distorts an analog or digital signal. It may be caused by electrical sources, such as power lines, fluorescent lights, copiers, and microwave ovens, or by broadcast signals.

- Analog and digital signals both suffer attenuation, or loss of signal, as they travel farther from their sources. To compensate, analog signals are amplified, and digital signals are regenerated through repeaters.

- Every network is susceptible to a delay between the transmission of a signal and its receipt. This delay is called latency. The length of the cable contributes to latency, as does the presence of any intervening connectivity device.
Coaxial cable consists of a central metal conducting core (often copper) surrounded by a plastic insulator, a braided metal shielding, and an outer plastic cover called the sheath. The conducting core carries the electromagnetic signal, and the shielding acts as both a protection against noise and a ground for the signal. The insulator layer protects the copper core from the metal shielding. The sheath protects the cable from physical damage.

Most networks no longer rely on coaxial cable; however, if you obtain Internet service from a cable company, the cable that enters your home will be a type of coax known as RG-6. Twisted pair cable consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, twisted around each other and encased in plastic coating.

STP (shielded twisted pair) cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil, to reduce the effects of noise on the signal. UTP (unshielded twisted pair) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name suggests, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.

Fiber-optic cable contains one or several glass or plastic fibers in its core. Data is transmitted via pulsing light sent from a laser or light-emitting diode through the central fiber(s). Outside the fiber(s), cladding reflects light back to the core in different patterns that vary depending on the transmission mode. Fiber-optic cable provides the benefits of very high throughput, very high resistance to noise, and excellent security.

Fiber cable variations fall into two categories: single-mode and multimode. Single-mode fiber uses a small-diameter core, over which light travels mostly down its center, reflecting very few times. This allows single-mode fiber to accommodate high bandwidths and long distances (without requiring repeaters).

MMF (multimode fiber) uses a core with a larger diameter, over which many pulses of light travel at different angles. Multimode fiber is less expensive than SMF (single-mode fiber).

Serial communication is often used on short links between DTE (data terminal equipment) and DCE (data circuit-terminating equipment). For example, you might use an RS-232 serial cable to connect your laptop to a router so that you can configure the router from your laptop.

TIA/EIA’s 568 Commercial Building Wiring Standard, also known as structured cabling, provides guidelines for uniform, enterprise-wide, multivendor cabling systems. Structured cabling is based on a hierarchical design that begins with a service provider’s facilities and end at users’ workstations.

The best practice for installing cable is to follow the TIA/EIA 568 specifications and the manufacturer’s recommendations. Be careful not to exceed a cable’s bend radius, untwist wire pairs more than one-half inch, or remove more than one inch of insulation from copper wire. Install plenum-rated cable in ceilings and floors, and run cabling away from where it might suffer physical damage. Maintain clear, comprehensive documentation on your cable plant.
## Key Terms

1. **Gigabit per second (Gbps)**: 1,000,000,000 bits per second.
2. **Kilobit per second (Kbps)**: 1,000 bits per second.
3. **Megabit per second (Mbps)**: 1,000,000 bits per second.
4. **Terabit per second (Tbps)**: 1,000,000,000,000 bits per second.

100 block: Part of an organization’s cross-connect facilities, a type of punch-down block designed to terminate Cat 5 or better twisted pair wires.

100 pair wire: UTP supplied by a telecommunications carrier that contains 100 wire pairs.

10Base-2: See Thinnet.

10Base-5: See Thicknet.

25 pair wire: UTP supplied by a telecommunications carrier that contains 25 wire pairs.

66 block: Part of an organization’s cross-connect facilities, a type of punch-down block used for many years to terminate telephone circuits. It does not meet Cat 5 or better standards, and so it is infrequently used on data networks.

Alien cross talk: EMI interference induced on one cable by signals traveling over a nearby cable.

AM (amplitude modulation): A modulation technique in which the amplitude of the carrier signal is modified by the application of a data signal.

American Wire Gauge: See AWG.

Amplifier: A device that boosts, or strengthens, an analog signal.

Amplitude: A measure of a signal’s strength.

Amplitude modulation: See AM.

Analog: A signal that uses variable voltage to create continuous waves, resulting in an inexact transmission.

Attenuation: The extent to which a signal has weakened after traveling a given distance.

AWG (American Wire Gauge): A standard rating that indicates the diameter of a wire, such as the conducting core of a coaxial cable.

Bandwidth: A measure of the difference between the highest and lowest frequencies that a medium can transmit.

Baseband: A form of transmission in which digital signals are sent through direct current pulses applied to a wire. This direct current requires exclusive use of the wire’s capacity, so baseband systems can transmit only one signal, or one channel, at a time. Every device on a baseband system shares a single channel.

Bend radius: The radius of the maximum arc into which you can loop a cable before you will cause data transmission errors. Generally, a twisted pair cable’s bend radius is equal to or greater than four times the diameter of the cable.

Binary: A system founded on using 1s and 0s to encode information.

Bit (binary digit): A bit equals a single pulse in the digital encoding system. It may have only one of two values: 0 or 1.
BNC (Bayonet Neill-Concelman, or British Naval Connector) A standard for coaxial cable connectors named after its coupling method and its inventors.

BNC connector A coaxial cable connector type that uses a twist-and-lock (or bayonet) style of coupling. It may be used with several coaxial cable types, including RG-6 and RG-59.

braiding A braided metal shielding used to insulate some types of coaxial cable.

broadband A form of transmission in which signals are modulated as radiofrequency analog pulses with different frequency ranges. Unlike baseband, broadband technology does not involve binary encoding. The use of multiple frequencies enables a broadband system to operate over several channels and, therefore, carry much more data than a baseband system.

broadcast A transmission that involves one transmitter and multiple, undefined receivers.

byte Eight bits of information. In a digital signaling system, broadly speaking, one byte carries one piece of information.

cable plant The hardware that constitutes the enterprise-wide cabling system.

capacity See throughput.

Cat Abbreviation for the word category when describing a type of twisted pair cable. For example, Category 3 unshielded twisted pair cable may also be called Cat 3.

Cat 3 (Category 3) A form of UTP that contains four wire pairs and can carry up to 10 Mbps, with a possible bandwidth of 16 MHz. Cat 3 has typically been used for 10-Mbps Ethernet or 4-Mbps token ring networks. Network administrators are gradually replacing Cat 3 cabling with Cat 5 to accommodate higher throughput. Cat 3 is less expensive than Cat 5.

Cat 4 (Category 4) A form of UTP that contains four wire pairs and can support up to 16-Mbps throughput. Cat 4 may be used for 16-Mbps token ring or 10-Mbps Ethernet networks. It is guaranteed for data transmission up to 20 MHz and provides more protection against cross talk and attenuation than Cat 1, Cat 2, or Cat 3.

Cat 5 (Category 5) A form of UTP that contains four wire pairs and supports up to 100-Mbps throughput and a 100-MHz signal rate.

Cat 5e (Enhanced Category 5) A higher-grade version of Cat 5 wiring that contains high-quality copper, offers a high twist ratio, and uses advanced methods for reducing cross talk. Enhanced Cat 5 can support a signaling rate of up to 350 MHz, more than triple the capability of regular Cat 5.

Cat 6 (Category 6) A twisted pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheath covers the second foil layer. The foil insulation provides excellent resistance to cross talk and enables Cat 6 to support a signaling rate of 250 MHz and at least six times the throughput supported by regular Cat 5.

Cat 6e (Enhanced Category 6) A higher-grade version of Cat 6 wiring that further reduces attenuation and cross talk and allows for potentially exceeding traditional network segment length limits. Cat 6e is capable of a 550-MHz signaling rate and can reliably transmit data at multi-gigabit per second rates.

Cat 7 (Category 7) A twisted pair cable that contains multiple wire pairs, each separately shielded then surrounded by another layer of shielding within the jacket. Cat 7 can support up to a 1-GHz signal rate. But because of its extra layers, it is less flexible than other forms of twisted pair wiring.
Category 3  See Cat 3.
Category 4  See Cat 4.
Category 5  See Cat 5.
Category 6  See Cat 6.
Category 7  See Cat 7.

**channel**  A distinct communication path between two or more nodes, much like a lane is a distinct transportation path on a freeway. Channels may be separated either logically (as in multiplexing) or physically (as when they are carried by separate wires).

**cladding**  The glass or plastic shield around the core of a fiber-optic cable. Cladding reflects light back to the core in patterns that vary depending on the transmission mode. This reflection allows fiber to bend around corners without impairing the light-based signal.

**coaxial cable**  A type of cable that consists of a central metal conducting core, which might be solid or stranded and is often made of copper, surrounded by an insulator, a braided metal shielding, called braiding, and an outer cover, called the sheath or jacket. Coaxial cable, called “coax” for short, was the foundation for Ethernet networks in the 1980s. Today it’s used to connect cable Internet and cable TV systems.

**conduit**  The pipeline used to contain and protect cabling. Conduit is usually made from metal.

**connectors**  The pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer.

**core**  The central component of a cable designed to carry a signal. The core of a fiber-optic cable, for example, consists of one or several glass or plastic fibers. The core of a coaxial copper cable consists of one large or several small strands of copper.

**crossover cable**  A twisted pair patch cable in which the termination locations of the transmit and receive wires on one end of the cable are reversed.

**cross talk**  A type of interference caused by signals traveling on nearby wire pairs infringing on another pair’s signal.

**data circuit-terminating equipment**  See DCE.

**data terminal equipment**  See DTE.

**DB-9 connector**  A type of connector with nine pins that’s commonly used in serial communication that conforms to the RS-232 standard.

**DB-25 connector**  A type of connector with 25 pins that’s commonly used in serial communication that conforms to the RS-232 standard.

**DCE (data circuit-terminating equipment)**  A device, such as a multiplexer or modem, that processes signals. DCE supplies a clock signal to synchronize transmission between DTE and DCE.

**demarcation point (demarc)**  The point of division between a telecommunications service carrier’s network and a building’s internal network.

**demultiplexer (demux)**  A device that separates multiplexed signals once they are received and regenerates them in their original form.

**dense wavelength division multiplexing**  See DWDM.
digital  As opposed to analog signals, digital signals are composed of pulses that can have a value of only 1 or 0.

DTE (data terminal equipment)  Any end-user device, such as a workstation, terminal (essentially a monitor with little or no independent data-processing capability), or a console (for example, the user interface for a router).

duplex  See full-duplex.

DWDM (dense wavelength division multiplexing)  A multiplexing technique used over single-mode or multimode fiber-optic cable in which each signal is assigned a different wavelength for its carrier wave. In DWDM, little space exists between carrier waves in order to achieve extraordinary high capacity.

electromagnetic interference  See EMI.

EMI (electromagnetic interference)  A type of interference that may be caused by motors, power lines, televisions, copiers, fluorescent lights, or other sources of electrical activity.

enhanced Category 5  See Cat 5e.

enhanced Category 6  See Cat 6e.

entrance facilities  The facilities necessary for a service provider (whether it is a local phone company, Internet service provider, or long-distance carrier) to connect with another organization’s LAN or WAN.

F-type connector  A connector used to terminate coaxial cable used for transmitting television and broadband cable signals.

FDM (frequency division multiplexing)  A type of multiplexing that assigns a unique frequency band to each communications subchannel. Signals are modulated with different carrier frequencies, then multiplexed to simultaneously travel over a single channel.

ferrule  A short tube within a fiber-optic cable connector that encircles the fiber strand and keeps it properly aligned.

fiber-optic cable  A form of cable that contains one or several glass or plastic fibers in its core. Data is transmitted via pulsing light sent from a laser or light-emitting diode (LED) through the central fiber (or fibers). Fiber-optic cables offer significantly higher throughput than copper-based cables. They may be single-mode or multimode and typically use wave-division multiplexing to carry multiple signals.

FM (frequency modulation)  A method of data modulation in which the frequency of the carrier signal is modified by the application of the data signal.

frequency  The number of times that a signal’s amplitude changes over a fixed period of time, expressed in cycles per second, or hertz (Hz).

frequency division multiplexing  See FDM.

frequency modulation  See FM.

full-duplex  A type of transmission in which signals may travel in both directions over a medium simultaneously. May also be called, simply, “duplex.”

half-duplex  A type of transmission in which signals may travel in both directions over a medium, but in only one direction at a time.

hertz (Hz)  A measure of frequency equivalent to the number of amplitude cycles per second.
**IFD (intermediate distribution frame)** A junction point between the MDF and concentrations of fewer connections—for example, those that terminate in a telecommunications closet.

**Impedance** The resistance that contributes to controlling an electrical signal. Impedance is measured in ohms.

**Intermediate distribution frame** See IDF.

**Latency** The delay between the transmission of a signal and its receipt.

**LC (local connector)** A connector used with single-mode or multimode fiber-optic cable.

**Link segment** See unpopulated segment.

**Local connector** See LC.

**Main cross-connect** See MDF.

**Main distribution frame** See MDF.

**MDF (main distribution frame)** Also known as the main cross-connect, the first point of interconnection between an organization’s LAN or WAN and a service provider’s facility.

**Mechanical transfer-registered jack** See MT-RJ.

**Media converter** A device that enables networks or segments using different media to interconnect and exchange signals.

**MMF (multimode fiber)** A type of fiber-optic cable that contains a core with a diameter between 50 and 100 microns, through which many pulses of light generated by a light-emitting diode (LED) travel at different angles.

**Modem** A device that modulates analog signals into digital signals at the transmitting end for transmission over telephone lines, and demodulates digital signals into analog signals at the receiving end.

**Modulation** A technique for formatting signals in which one property of a simple carrier wave is modified by the addition of a data signal during transmission.

**MT-RJ (mechanical transfer-registered jack)** A connector used with single-mode or multimode fiber-optic cable.

**Multimode fiber** See MMF.

**Multiplexer (mux)** A device that separates a medium into multiple channels and issues signals to each of those subchannels.

**Multiplexing** A form of transmission that allows multiple signals to travel simultaneously over one medium.

**Near end cross talk** See NEXT.

**NEXT (near end cross talk)** Cross talk, or the impingement of the signal carried by one wire onto a nearby wire, that occurs between wire pairs near the source of a signal.

**Noise** The unwanted signals, or interference, from sources near network cabling, such as electrical motors, power lines, and radar.

**Nonbroadcast point-to-multipoint transmission** A communications arrangement in which a single transmitter issues signals to multiple, defined recipients.
optical loss  The degradation of a light signal on a fiber-optic network.

overhead  The nondata information that must accompany data in order for a signal to be properly routed and interpreted by the network.

patch cable  A relatively short section (usually between 3 and 25 feet) of cabling with connectors on both ends.

patch panel  A wall-mounted panel of data receptors into which cross-connect patch cables from the punch-down block are inserted.

phase  A point or stage in a wave’s progress over time.

plenum  The area above the ceiling tile or below the subfloor in a building.

point-to-point  A data transmission that involves one transmitter and one receiver.

point-to-multipoint  A communications arrangement in which one transmitter issues signals to multiple receivers. The receivers may be undefined, as in a broadcast transmission, or defined, as in a nonbroadcast transmission.

populated segment  A network segment that contains end nodes, such as workstations.

punch-down block  A panel of data receptors into which twisted pair wire is inserted, or punched down, to complete a circuit.

radiofrequency interference  See RFI.

Recommended Standard 232  See RS-232.

regeneration  The process of retransmitting a digital signal. Regeneration, unlike amplification, repeats the pure signal, with none of the noise it has accumulated.

registered jack 11  See RJ-11.

registered jack 45  See RJ-45.

repeater  A device used to regenerate a signal.

RFI (radiofrequency interference)  A kind of interference that may be generated by broadcast signals from radio or TV towers.

RG-6  A type of coaxial cable with an impedance of 75 ohms and that contains an 18 AWG core conductor. RG-6 is used for television, satellite, and broadband cable connections.

RG-8  A type of coaxial cable characterized by a 50-ohm impedance and a 10 AWG core. RG-8 provided the medium for the first Ethernet networks, which followed the now-obsolete 10Base-5 standard.

RG-58  A type of coaxial cable characterized by a 50-ohm impedance and a 24 AWG core. RG-58 was a popular medium for Ethernet LANs in the 1980s, used for the now-obsolete 10Base-2 standard.

RG-59  A type of coaxial cable characterized by a 75-ohm impedance and a 20 or 22 AWG core, usually made of braided copper. Less expensive but suffering greater attenuation than the more common RG-6 coax, RG-59 is used for relatively short connections.

RJ-11 (registered jack 11)  The standard connector used with unshielded twisted pair cabling (usually Cat 3 or Level 1) to connect analog telephones.

RJ-45 (registered jack 45)  The standard connector used with shielded twisted pair and unshielded twisted pair cabling.
rollover cable  A type of cable in which the terminations on one end are exactly the reverse of the terminations on the other end. It is used for serial connections between routers and consoles or other interfaces.

round trip time  See RTT.

RS-232 (Recommended Standard 232)  A Physical layer standard for serial communications, as defined by EIA/TIA.

RTT (round trip time)  The length of time it takes for a packet to go from sender to receiver, then back from receiver to sender. RTT is usually measured in milliseconds.

SC (subscriber connector or standard connector)  A connector used with single-mode or multimode fiber-optic cable.

serial  A style of data transmission in which the pulses that represent bits follow one another along a single transmission line. In other words, they are issued sequentially, not simultaneously.

serial cable  A cable, such as an RS-232 type, that permits serial data transmission.

sheath  The outer cover, or jacket, of a cable.

shield  See braiding.

shielded twisted pair  See STP.

simplex  A type of transmission in which signals may travel in only one direction over a medium.

single-mode fiber  See SMF.

SMF (single-mode fiber)  A type of fiber-optic cable with a narrow core that carries light pulses along a single path data from one end of the cable to the other end. Data can be transmitted faster and for longer distances on single-mode fiber than on multimode fiber. However, single-mode fiber is more expensive.

ST (straight tip)  A connector used with single-mode or multimode fiber-optic cable.

standard connector  See SC.

statistical multiplexing  A method of multiplexing in which each node on a network is assigned a separate time slot for transmission, based on the node’s priority and need.

STP (shielded twisted pair)  A type of cable containing twisted-wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil.

straight-through cable  A twisted pair patch cable in which the wire terminations in both connectors follow the same scheme.

straight tip  See ST.

structured cabling  A method for uniform, enterprise-wide, multivendor cabling systems specified by the TIA/EIA 568 Commercial Building Wiring Standard. Structured cabling is based on a hierarchical design using a high-speed backbone.

subchannel  One of many distinct communication paths established when a channel is multiplexed or modulated.

subscriber connector  See SC.
TDM (time division multiplexing) A method of multiplexing that assigns a time slot in the flow of communications to every node on the network and, in that time slot, carries data from that node.

telecommunications closet Also known as a “telco room,” the space that contains connectivity for groups of workstations in a defined area, plus cross-connections to IDFs or, in smaller organizations, an MDF. Large organizations may have several telecommunications closets per floor, but the TIA/EIA standard specifies at least one per floor.

Thicknet An IEEE Physical layer standard for achieving a maximum of 10-Mbps throughput over coaxial copper cable. Thicknet is also known as 10Base-5. Its maximum segment length is 500 meters, and it relies on a bus topology.

thickwire Ethernet See Thicknet.

thin Ethernet See Thinnet.

Thinnet An IEEE Physical layer standard for achieving 10-Mbps throughput over coaxial copper cable. Thinnet is also known as 10Base-2. Its maximum segment length is 185 meters, and it relies on a bus topology.

throughput The amount of data that a medium can transmit during a given period of time. Throughput is usually measured in megabits (1,000,000 bits) per second, or Mbps. The physical nature of every transmission media determines its potential throughput.

time division multiplexing See TDM.

transceiver A device that transmits and receives signals.

transmission In networking, the application of data signals to a medium or the progress of data signals over a medium from one point to another.

transmit To issue signals to the network medium.

twist ratio The number of twists per meter or foot in a twisted pair cable.

twisted pair A type of cable similar to telephone wiring that consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, twisted around each other and encased in plastic coating.

unpopulated segment A network segment that does not contain end nodes, such as workstations. Unpopulated segments are also called link segments.

unshielded twisted pair See UTP.

UTP (unshielded twisted pair) A type of cabling that consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.

vertical cross-connect Part of a network’s backbone that supplies connectivity between a building’s floors. For example, vertical cross-connects might connect an MDF and an IDF or IDFs and telecommunications closets within a building.

volt The measurement used to describe the degree of pressure an electrical current exerts on a conductor.

voltage The pressure (sometimes informally referred to as the strength) of an electrical current.
wavelength  The distance between corresponding points on a wave’s cycle. Wavelength is inversely proportional to frequency.

wavelength division multiplexing  See WDM.

WDM (wavelength division multiplexing)  A multiplexing technique in which each signal on a fiber-optic cable is assigned a different wavelength, which equates to its own subchannel. Each wavelength is modulated with a data signal. In this manner, multiple signals can be simultaneously transmitted in the same direction over a length of fiber.

Review Questions

1. What is different about the method used to boost a digital signal’s strength, compared with the method of boosting an analog signal’s strength?
   a. A digital signal requires an amplifier, which introduces noise into the signal, and an analog signal requires a repeater, which retransmits the signal in its original form.
   b. A digital signal requires a repeater, which increases the strength of both the signal and the noise it has accumulated, and an analog signal requires an amplifier, which retransmits the signal in its original form.
   c. A digital signal requires an amplifier, which increases the strength of both the noise and the signal, and an analog signal requires a repeater, which retransmits the signal in its original form.
   d. A digital signal requires a repeater, which retransmits the signal in its original form, and an analog signal requires an amplifier, which increases the strength of both the signal and the noise it has accumulated.

2. Which of the following decimal numbers corresponds to the binary number 00000111?
   a. 3
   b. 5
   c. 7
   d. 9

3. A wave with which of the following frequencies would have the shortest wavelength?
   a. 10 MHz
   b. 100 MHz
   c. 1 GHz
   d. 100 GHz

4. What is the origin of the word *modem*?
   a. Modifier/demodifier
   b. Modulator/demodulator
   c. Modulator/decoder
   d. Multiplexer/demultiplexer
5. With everything else being equal, which of the following transmission techniques is capable of the greatest throughput?
   a. Simplex
   b. Half-duplex
   c. Full-duplex
   d. All techniques transmit data at equally high throughputs.

6. In addition to some types of data networks, which of the following use half-duplex communication?
   a. Telephones
   b. Walkie-talkies
   c. Television broadcast towers
   d. Satellite Internet connections

7. In wavelength division multiplexing, two modulated signals are guaranteed to differ in what characteristic?
   a. Throughput
   b. Phase
   c. Amplitude
   d. Color

8. Which of the following can increase latency on a network?
   a. An EMI source, such as fluorescent lighting
   b. The use of full-duplex transmission
   c. Adding 50 meters to the length of the network
   d. The use of multiple protocols

9. You are helping to install a cable broadband system in your friend’s home. She wants to bring the signal from where the service provider’s cable enters the house to a room on another floor, which means you have to attach a new cable to the existing one. What type of cable should this be?
   a. RG-6
   b. RG-8
   c. RG-58
   d. RG-59

10. What part of a cable protects it against environmental damage?
    a. Sheath
    b. Braiding
    c. Plenum
    d. Cladding
11. With everything else being equal, a network using which of the following UTP types will suffer the most cross talk?
   a. Cat 3
   b. Cat 5
   c. Cat 5e
   d. Cat 7

12. What are two advantages of using twisted pair cabling over coaxial cabling on a network?
   a. Twisted pair cable is more reliable.
   b. Twisted pair cable is less expensive.
   c. Twisted pair cable is more resistant to noise.
   d. Twisted pair cable is more resistant to physical damage.
   e. Twisted pair cable is required for modern transmission standards.

13. Which of the following problems could be solved by using a crossover cable?
   a. You’re missing a patch cable, but need to connect a workstation to a switch.
   b. You’re missing a connectivity device, but need to exchange data between two laptops.
   c. You’re missing a serial cable, but need to configure a new router using your laptop.
   d. You’re missing a repeater, but need to extend a network segment.

14. Which of the following network transmission media offers the highest potential throughput over the longest distances?
   a. UTP
   b. STP
   c. MMF
   d. SMF

15. In which of the following network links might you use SC connectors?
   a. A coaxial connection between a cable modem and a server
   b. A UTP connection between a workstation and a hub
   c. A wireless connection between a handheld computer and a desktop computer
   d. A fiber-optic connection between a server and router.

16. What type of fiber-optic cable is used most frequently on LANs?
   a. Multithreaded fiber
   b. Twisted fiber
   c. Single-mode fiber
   d. Multimode fiber
17. What is the purpose of cladding in a fiber-optic cable?
   a. It protects the inner core from damage.
   b. It reflects the signal back to the core.
   c. It shields the signal from EMI.
   d. It concentrates the signal and helps keep it from fading.

18. Which of the following is a potential drawback to using fiber-optic cable for LANs?
   a. It is expensive.
   b. It cannot handle high-bandwidth transmissions.
   c. It can carry transmissions using only TCP/IP.
   d. It is not yet an accepted standard for high-speed networking.

19. In what part of a structured cabling system would you find users’ desktop computers?
   a. Telco room
   b. MDF
   c. IDF
   d. Work area

20. You’ve just received a new Cisco router for your data center, and it came with a rollover cable. What can you do with this cable?
   a. Make a connection from the router’s console port to your laptop’s serial port and configure the router from your laptop.
   b. Make a connection from the router’s Ethernet port to a port on the patch panel in the telecommunications closet to establish connectivity for workstations in a work area.
   c. Make a connection from the router’s Ethernet port to the Ethernet port on your laptop to configure the router.
   d. Make a connection from the router’s console port to another router’s console port to daisy-chain the routers.

21. What is the maximum distance specified in the structured cabling standard for a horizontal wiring subsystem?
   a. 10 m
   b. 90 m
   c. 100 m
   d. 200 m

22. Which of the following can occur as a result of improper cable termination?
   a. Cross talk
   b. Noise
   c. Data errors
   d. All of the above
23. If your MDF contains a 66 block, the type of cable terminating at that punch-down block is probably what?
   a. UTP designed for telephone signaling
   b. UTP designed for 100 Mbps Ethernet
   c. UTP designed for 1 Gbps Ethernet
   d. Fiber-optic cable

24. Your campuswide WAN is experiencing slow Internet response times. When you call your Internet service provider to ask if they can troubleshoot the problem from their end, they warn you that their responsibilities end at the demarc. What do they mean?
   a. They will not diagnose problems beyond your organization’s MDF.
   b. They will not diagnose problems beyond your organization’s entrance facilities.
   c. They will not diagnose problems beyond your organization’s IDF.
   d. They will not diagnose problems beyond your organization’s telco rooms.

25. What is the maximum amount you should untwist twisted pair wires before inserting them into connectors?
   a. ¼ inch
   b. ½ inch
   c. 1 inch
   d. 2 inches

Hands-On Projects

Project 3-1
Previously in this chapter you learned about how to terminate UTP in RJ-45 plugs. In this project, you will practice putting an RJ-45 connector on a twisted pair cable, and then use the cable to connect a workstation to the network.

For this project, you will need a wire cutter, a wire stripper, and a crimping tool, which are pictured in Figures 3-26, 3-27, and 3-28, respectively. You’ll also need a 5-foot length of Cat 5 (or better) UTP, at least two RJ-45 connectors, and a simple client/server network (for example, a Windows XP client connecting to a wall jack or hub as part of a Windows Server 2003 network, or a Linux workstation similarly connecting to a UNIX server) that you have verified works with a reliable twisted pair cable.

1. Follow the steps for adding an RJ-45 connector to UTP as described in this chapter’s “Terminating Twisted Pair Cable” section to make a straight-through cable. Follow the pinouts shown in Figure 3-24 for the TIA/EIA 586B standard.

2. Use your newly created patch cable to connect your workstation to the network. Can you log on? Can you open a file?
3. If you cannot communicate reliably with the network, try the process again, beginning at Step 1. (You have to recut the wires; otherwise, they will not properly connect with the RJ-45 connector.) Continue until you can reliably log on to the network using the patch cable you have made.

**Project 3-2**

As you learned in this chapter, it is sometimes useful to connect two computers directly, rather than go through a traditional network, as you did in the previous project. In this project you will make a crossover cable and use it to connect two workstations. For this project, you will need one workstation running the Windows XP or Windows Vista operating system and one server running the Windows Server 2003 or Windows Server 2008 operating system. Both must contain functioning NICs. You will also need a crimping tool, a wire stripper, a wire cutter, a 5-foot length of Cat 5 (or better) UTP, and two RJ-45 connectors. To rule out unrelated network connectivity issues when testing your homemade cable, also have a known good Cat 5 or better patch cable handy.

1. On one end of your Cat 5 UTP cable, install an RJ-45 connector by following the steps described in this chapter’s “Terminating Twisted Pair Cable” section.

2. On the opposite end of the same cable, install an RJ-45 connector in a similar manner, but reverse the locations of the transmit and receive wires. Refer to Figure 3-25 for a visual representation of the crossover cable’s RJ-45 terminations.

3. Now that your crossover cable is complete, insert one of the cable’s RJ-45 connectors into the workstation’s NIC and the other RJ-45 connector into the server’s NIC.

4. To test whether your cable works, from the workstation, attempt to view your network connections. To do this from a Windows XP or Windows Vista workstation, for example, click the Start button, then select **My Network Places**. You should see the icon for your server. If the server isn’t evident, your cable might be faulty—or your network connection might not work for other reasons. Replace your homemade cable with a known good Cat 5 or better patch cable to see if you get the same result. If you can see an icon for your server using the known good patch cable, it is probably safe to assume your homemade cable is flawed. In that case, start over.

5. Double-click the server icon and log on to the server.

6. Once you have logged on, copy a file from your workstation to the server to verify that the connection is sound.

**Project 3-3**

Early in this chapter, you learned that the majority of network problems can be traced to its Physical layer components. One potential hazard is a damaged UTP cable. This can happen from misuse (for example, tugging too hard on the cable to make it reach between devices) or by accident (for example, while installing new equipment racks and pinching a cable between the rack’s metal sides). In this project, you will experiment with damaged cables. For this project, you will need a crossover cable, such as the one you created in Project 3-2. You will also need a workstation running the Windows XP or Windows Vista operating system capable of connecting to a server running the Windows Server 2003 or Server
2008 operating system. On the server, a large, shareable program, such as Adobe Photoshop, should be installed for access by workstation users. Finally, you will also need a utility knife and a stopwatch.

1. Connect the workstation and server using the crossover cable. Verify that you can log on to the server from the Windows XP or Windows Vista workstation.

2. Try to run a large application, such as Adobe Photoshop, from the server, starting the stopwatch timer as you do so. When the application is completely loaded into your workstation’s memory, stop the timer. Note how long it took for the application to be served to your workstation.

3. Close the application on your workstation.

4. With your hands approximately 2 feet apart, grab a section of the UTP cable and pull as hard as you can—if possible, until the sheath begins to stretch.

5. From the workstation, attempt once more to open the large application on the server, restarting your stopwatch as you do so. When the application is completely loaded into your workstation’s memory, stop the timer. Did this process take longer than it did in Step 2?

6. In another attempt to damage the cable, take the utility knife and scrape it along the side of the UTP cable until it has perforated the sheath, entered the wire’s insulation, and at least nicked some of the twisted pairs inside.

7. Repeat Step 5. Did the time required to load the application change? Did the application even load? If not, what type of error message did your workstation receive?

---

**Case Projects**

**Case Project 3-1**

You have been asked to design the entire cabling system for a medical instrument manufacturer’s new central warehouse. The company already has three buildings within two city blocks, and the warehouse will be its fourth building. Currently, the buildings run on separate networks, but the company would like to be able to exchange data among them. For example, the Quality Control Department in building 1 would like to be able to access servers in the Research Department in building 2. In addition, the Sales Department in building 3 wants to conduct video training sessions for its representatives in the field via the Internet. Next door, in the warehouse, 50 shipping and packing personnel in the Fulfillment Department will be riding up and down the aisles on forklifts pulling inventory off the shelves on a daily basis. What kind of transmission media would you recommend for each different building and department of the medical instrument company and why? What type of media would you recommend using to connect the buildings and why? Finally, what kind of media should the company request from its ISP for connecting the corporate WAN to the Internet?
Case Project 3-2

While you were gathering information to recommend transmission media for the medical instrument manufacturer, you noticed that some of the telco rooms were in disarray. For one thing you notice sloppy cable terminations. Further, cables are pulled tightly around the corners of racks and intertwined. You also suspect that the horizontal wiring spans exceed TIA/EIA 568 recommendations. And to top it off, cables, ports on connectivity devices, and data jacks aren’t labeled. However, the company’s network manager tells you she and her staff don’t have time to attend to these oversights. What can you say to convince her that the minor oversights could have a significant impact? What do you consider the single most important reason to pay attention to faulty terminations and excessive horizontal wiring spans? Why is it critical to label patch cables, ports, and data jacks?

Case Project 3-3

Thanks to your persuasive skills, the medical instrument company took a few days to improve its cable management practices. That’s fortunate, because now, several months later, it has just won a huge contract and its network will expand. The brand-new warehouse is busy with activity. The inventory shelves are being stocked to the ceiling. Nearby, machines that carry merchandise along a conveyor belt are working nonstop. However, the company has a new problem: since production has stepped up, several inventory specialists in the warehouse are complaining that occasionally their handheld computers will not connect to the network or that they suddenly lose their connection. It’s especially frustrating because more personnel than ever are trying to use the network. What could be causing the handheld computers to experience intermittent connectivity problems? What can you do to rule out the possibility that the handheld computers are simply faulty?