CHAPTER 4

NETWORK MEDIA

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

Define the primary cables used in wired networking

Describe the characteristics of the major types of fiber-optic media

Explain the technologies used for wireless networking

Network media are the materials through which network signals travel between devices. They can be a physical material, such as copper wire or glass fiber, or simply the air. When a physical material is used as the medium, it's usually referred to as "wired networking," and when signals are transmitted through the air, the medium is aptly called "wireless networking."

In this chapter, you learn about common options for wired and wireless networking and where these options make sense. You learn about the characteristics of wired media and how to choose a media type to suit a situation and environment. You also learn how to install and terminate the most common types of LAN media. In addition, you learn about transmission technologies for making wireless network links for both short-range Wi-Fi networks and long-range wireless networks.

Table 4-1 summarizes what you need for the hands-on projects in this chapter.

Table 4-1 Hands-on project requirements

Hands-on project	Requirements	Time required	Notes
Hands-On Project 4-1: Making a Patch Cable	Wire cutter and cable stripper, RJ-45 crimping tool, 2 to 4 feet of Cat 5e or Cat 6 cable, two RJ-45 plugs, and a cable tester (optional)	20 minutes	
Hands-On Project 4-2: Terminating UTP Cable	Wire cutter and cable stripper, 2 to 4 feet of Cat 5e or Cat 6 cable, 110 punchdown tool, Cat 5e or Cat 6 patch panel, RJ-45 jack, and a cable tester (optional)	20 minutes	
Hands-On Project 4-3: Conducting End-to-End Testing	The patch cable you made, an additional patch cable, the patch panel and RJ-45 jack to which you terminated the cable, a lab computer, and a switch	10 minutes	

Wired Networking

Certification

98-366 Understanding network hardware:

Understand media types

Wired networking uses tangible physical media called "cables." Cables used in networking come in two broad categories: copper wire and fiber optic. Regardless of the material used, all networking cables must support the basic tasks of sending and receiving bit signals. The composition of these signals (electricity or light), the speed at which these signals can be sent (bandwidth), and the distance they can effectively travel make up the main differences between cabling types. The following sections discuss cable characteristics, the criteria for choosing a particular type of cabling, and a variety of cable types, including both copper and fiber optic.

Criteria for Choosing Network Media

All cables share certain fundamental characteristics you should know to understand their function and correct use. Even though copper cables differ radically from fiber-optic cables in composition and the types of signals they carry, the characteristics described in the following sections apply equally to both types of cabling.

Bandwidth Rating

Bandwidth, the number of bits per second that can be transmitted across a medium, is as much a function of the technology used to transmit bit signals as it is of the medium. For example, Category 5e UTP cabling was originally intended to support speeds only up to 100 Mbps but was later upgraded to support up to 1000 Mbps when the 1000BaseT standard was developed.

What really determines the bandwidth of a cabling type is how fast a transmitting device, such as a NIC, can generate bit signals on the medium and whether these signals can be received accurately at the other end of the cable. Bit signals lose strength as they travel along the medium, so when judging whether a cabling type is suitable for a particular transmission speed, the maximum cable length must also be considered.

Another factor determining bandwidth is how bit signals are represented on the medium, a process called **encoding**. Different networking standards use different patterns of electrical or light pulses to represent a series of bits on the medium.

Note

Encoding is beyond the scope of this book, but if you'd like to read more about it, take a look at this Web site: *http://units.folder101.com/cisco/sem1/Notes/ch7-technologies/encoding.htm*

Although different media types and cable grades can support higher bandwidths than others, what's most important is choosing the media type and cable grade specified by the networking standard you want to run. Keep in mind that today's 1000BaseT network might be tomorrow's 10GBaseT network. So, when possible, choose a cabling category that's compatible with the standard you want to implement now but will support the next level of speed your network is likely to need in the future.

Maximum Segment Length

A **cable segment** is a length of cable between two network devices, such as a NIC and a switch. Any intermediate passive (unpowered) devices, such as wall jacks, are considered part of the total segment length.

Each cable type can transport data at a particular speed only so far before its signals begin to weaken past the point that a receiving station can read them accurately; this phenomenon is called attenuation, as you learned in Chapter 3. In addition, electrical signals are affected by electromagnetic interference, or "noise." The longer a signal travels down a cable segment, the more likely it is that electrical noise impairs the signal to the point that data can be misinterpreted. (For example, a 0 bit is read as a 1 bit.) An internetwork can be constructed of many cable segments, as long as

the hardware connecting them (such as switches and routers) can accurately capture the signals, which are then regenerated on the next cable segment at full strength.

Interference and Eavesdropping Susceptibility

How well a media type resists signal interference from outside sources depends on the medium's construction and the type of signals it's designed to carry. Interference to electrical signals on copper media comes in the form of **electromagnetic interference (EMI)** and **radio frequency interference (RFI)**. Motors, transformers, fluorescent lights, and other sources of intense electrical activity can emit both EMI and RFI, but RFI problems are also associated with the proximity of strong broadcast sources in an environment (such as a nearby radio or TV station). RFI can also affect wireless networks if the frequencies are in the same range in which the wireless network operates.

Another type of interference in copper wires is a form of EMI called **crosstalk**, which is interference one wire generates on another wire when both are in a bundle (as all cabling in LANs is). When electrical signals travel across the medium, they create their own electromagnetic field. Although this field is weak, it can leak onto other wires, especially when the insulation is in contact with another wire. Although it's not as common now, you might have experienced crosstalk while talking on a landline phone and hearing another conversation faintly. With phone wires, crosstalk is merely an annoyance because people can filter out this noise easily, but in networking, excessive crosstalk can render the network connection unusable.

Because electrical signals traveling down a copper wire create an electromagnetic field that can be detected outside the wires, copper wire is susceptible to electronic eavesdropping. It might sound like the stuff of spy movies, but with the right type of equipment, an eavesdropper simply needs to get close to a copper cable to extract data from it. In the absence of sensitive electronic equipment, if eavesdroppers have physical access to the connecting equipment and the copper wire is slightly exposed, they would have no problem installing a listening device directly on the wires.

Fiber-optic cabling carries light signals and is impervious to interference. In addition, because no magnetic field is present, eavesdropping is a difficult proposition with fiber-optic cable. To eavesdrop, someone needs access to the glass strands carrying the optical signals to install a device that captures data and prevents the connection from being broken. It's not impossible, but it's extremely difficult.

When choosing a cable type, the environment the medium operates in is one of the most crucial factors in the decision. The choice is usually between copper cabling and fiber-optic cabling for high-performance applications and between copper cabling and wireless for less bandwidth-heavy applications.

Cable Grade

Building and fire codes include specific cabling requirements, usually aimed at the combustibility and toxicity of the jacket and insulation covering most cables. Polyvinyl chloride (PVC) covers the cheapest and most common cables (for example, the

120-volt cord in lamps and other household appliances). Unfortunately, when this material burns, it gives off toxic fumes, which makes it unsuitable for cables strung in ceilings or inside walls.

The space between a false ceiling and the true ceiling in most office buildings, called the "plenum," is commonly used to aid air circulation for heating and cooling. Any cables in this space must be plenum-rated, which typically means they're coated with Teflon because of its low combustibility and the nontoxic fumes it produces when burned. These cables can be used in the plenum or inside walls without being enclosed in conduit. Although plenum-rated cable is nearly twice as expensive as non-plenum-rated cable, eliminating the need for conduit makes installing plenum-rated network cabling much cheaper. UTP cabling is usually marked as communications riser (CMR) or communications plenum (CMP). CMR is suitable only for building risers, such as elevator shafts or in cable trays, and can't be used in spaces that carry environmental air. CMP is suitable for use in plenum spaces. Before installing any type of cable, check all local fire and building codes because requirements vary widely.

Connection Hardware

Every type of cable has connectors that influence the kinds of hardware the cable can connect to and that affect the costs of the resulting network. Some connectors are fairly easy to attach, requiring only inexpensive tools, but others need specialized and often expensive equipment to make the correct termination, and should be left to professionals. In this chapter, you learn how to install the connectors used in UTP cabling, which are the least expensive and most often used connectors. Fiber-optic connectors tend to be expensive, as are the tools used to attach them.

Other Media Considerations

Additional media considerations include ease of installation, testability, and of course cost:

- *Ease of installation*—The difficulty of installing a cable plant has a bearing on your choice of media. **Cable plant** is the term for all the cables and connectors tying a network together. Sometimes you have to make a tradeoff between the highest quality available and the cost and time factors involved in installing the medium correctly. Some factors to consider are a medium's minimum bend radius, which limits the angle at which a cable can be bent to run around corners; the cost and time to terminate the medium, which involves installing connectors and attaching media to patch panels and jacks; and the physical environment. (Cinderblock or plaster walls, concrete floors, and high ceilings can make installing a cable plant cost prohibitive, for example.) You might decide to make parts of your network wireless because of some of these factors.
- *Testability*—How difficult and expensive is it to test the medium after it's installed? Declaring a cable installation successful just because computers can communicate doesn't really constitute a test. A network that "works" might be crippled by excessive transmission errors caused by poor cable termination.

A true test of cabling, whether it's copper or fiber optic, is to install it, add the connectors and other termination points, and then test it with a device that can certify whether the cable meets the requirements for its category. Simple testers that check for basic electrical or optical connectivity are inexpensive (a few hundred dollars or less) but don't give you a true picture of your cable plant. Copper cable certifiers that do a full battery of Category 5e and above tests start at about $1000, and those capable of fiber-optic testing can cost more than $10,000.

- *Total cost*—When figuring the total cost for media, you must include the cabling, connectors, termination panels, wall jacks, termination tools, testing equipment, and, of course, time. The complexity of a large media installation (for a new building, for example) can be daunting, which is why there are companies specializing in media installation. In almost all cases, fiber-optic cabling costs considerably more than copper cabling for all components. When you need fiber-optic cabling, however, there's really no substitute. Some people opt for a wireless network because of the cost of wired components, but wireless networks are often not the solution when there are many users requiring high bandwidth. As a network administrator, you need to factor in all costs as well as users' needs before deciding which media types to use and in which situations. A combination of types tends to be the norm in today's networks.

Now that you know the general characteristics of cabling as well as which characteristics influence selecting cable types, you can understand the importance of the strengths and weaknesses of cabling types discussed in the following sections.

Coaxial Cable

For many years, coaxial cable—often called "coax" for short—was the predominant form of network cabling. Inexpensive and easy to install, coaxial cable was the networker's choice for many years, until the early 1990s. Now the main use for coaxial cable in networking is in connecting a cable modem to a wall outlet during installations by cable TV/Internet providers. For this reason, details on coax cable used in LANs are no longer covered.

Twisted-Pair Cable

Twisted-pair (TP) cable comes in two types: unshielded and shielded (UTP and STP). It consists of one or more pairs of insulated strands of copper wire twisted around one another and housed in an outer jacket or sheath (shown in Figure 4-1). These twists are important because they cause the electromagnetic fields that form around a wire carrying bit signals to wrap around one another and improve resistance to crosstalk and EMI from outside sources. In general, the more twists per unit length, the better the resistance the cable has to EMI and crosstalk. More expensive TP cable is usually more twisted than less expensive kinds and therefore provides a better pathway for higher bandwidth networks.

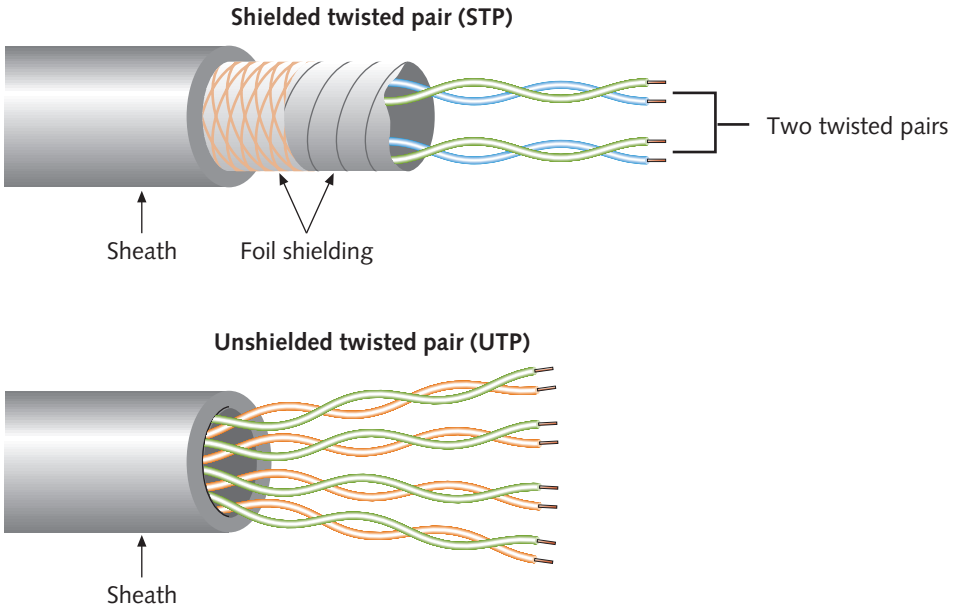


Figure 4-1 STP and UTP cable

Unshielded Twisted-Pair Cable

Most networks use UTP cabling, with STP used only where electrical noise is a major problem. The UTP cable used in LANs consists of four pairs of insulated wires; other UTP types contain fewer pairs. UTP is also used as phone wire, but because voice applications are much less demanding than networking in bandwidth and signal quality, the type of cable used for phone connections is usually unsuitable as network cabling.

UTP cabling is rated according to categories devised by the Telecommunications Industry Association (TIA) and the Electronic Industries Alliance (EIA); the American National Standards Institute (ANSI) has also endorsed these standards. The ANSI/TIA/EIA 568 Commercial Building Wiring Standard defines standards for the kinds of wiring used in commercial environments and helps ensure consistent performance from wiring products. Currently, the ANSI/TIA/EIA 568 standard includes nine categories for UTP wiring; these categories also govern the number of twists per foot or meter:

- *Category 1*—Applies to traditional UTP phone cabling, which is designed to carry voice but not data. This cabling is therefore labeled as **voicegrade**. Most UTP installed before 1982 falls into this category. This standard is no longer recognized by TIA/EIA.
- *Category 2*—Certifies UTP cabling for bandwidth up to 4 Mbps and consists of four pairs of wire. Because 4 Mbps is slower than most current networking technologies (except for older token ring installations), Category 2 is unlikely to be seen in networking environments and is no longer recognized by TIA/EIA.

- *Category 3*—Certifies UTP cabling for bandwidth up to 10 Mbps with signaling rates up to 16 MHz. This category supports 10BaseT Ethernet and 4 Mbps token ring networks with maximum segment lengths of 100 meters. Cat 3 consists of four pairs, with each pair having a minimum of three twists per foot (10 twists per meter). It remains in use in some older networks but should be replaced when networks are upgraded. Most networks have already migrated to 100 Mbps and 1000 Mbps speeds, and Cat 3 isn't suitable for these speeds.
- *Category 4*—Certifies UTP cabling for bandwidth up to 16 Mbps with signaling rates up to 20 MHz. This category supports mainly 10BaseT Ethernet and 16 Mbps token ring and is the first ANSI/TIA/EIA designation that labels cables as **datagrade** (capable of carrying data) rather than voicegrade. Cat 4 consists of four twisted pairs.
- *Category 5*—Certifies UTP cabling for bandwidth up to 100 Mbps with signaling rates up to 100 MHz. This category supports 100BaseTX, Asynchronous Transfer Mode (ATM) technologies at 25 and 155 Mbps, and Copper Distributed Data Interface (CDDI) at 100 Mbps. Category 5 also consists of four twisted pairs with an average of three to four twists per inch. This cabling has been superseded by Category 5e. It can be used in Gigabit Ethernet (1000BaseT), but Cat 5e is the minimum recommendation because of the additional tests required for it. Cat 5 cable is no longer widely available.
- *Category 5e*—The "e" means enhanced, so this category is an enhancement to Category 5 UTP. It differs mainly in the tests it must undergo and was designed to correct some shortcomings in Cat 5 cabling, particularly in Gigabit Ethernet and full-duplex operation. Cat 5e is an acceptable cable type for 1000BaseT Ethernet, but Category 6 should be considered for new installations. Cat 5e consists of four pairs and is rated for 100 MHz signaling rates; it comes in both shielded and unshielded versions.
- *Category 6*—This standard, published in June 2002 by the TIA/EIA, is the recommended UTP cabling standard for Ethernet applications over copper media at speeds up to 1 Gbps. Category 6 cabling uses the same type of modular jack as lower categories and is backward-compatible with Category 5 and Category 5e cable plants. It's specified to operate at signaling rates of 250 MHz. Some Cat 6 cabling includes a spline, or separator, in the jacket for additional separation between pairs of wires. However, this separator isn't a requirement. Cat 6 is the preferred cabling for 1000BaseT (Gigabit Ethernet) networks, but it can also support 10GBaseT for distances under 55 meters. It's a four-pair cable and comes in both shielded and unshielded versions.
- *Category 6a*—Published in February 2008, Category 6a (Category 6 augmented) is suitable for signaling rates up to 500 MHz and is the category specified for 10GBaseT networks with segments up to 100 meters. It comes in both shielded and unshielded versions.
- *Category 8*—Published in November 2016, Category 8 is suitable for signaling rates up to 2000 MHz and is the category specified for 25GBaseT and 40GBaseT

networks with segments up to 30 meters when supporting speeds faster than 10 Gbps. It comes in only shielded versions. A standard RJ-45 modular connector (discussed below) can be used to terminate Cat 8 cables.

Two additional categories aren't TIA/EIA standards. However, Europe has accepted the Category 7 and Category 7a standards, which specify a fully shielded twisted-pair cable (each wire pair is shielded, as is the outer sheath) with performance characteristics well above earlier cabling standards. Signaling rates are specified at up to 600 MHz for Cat 7 and 1000 MHz for Cat 7a. Because of a different connecting hardware design, these cables and connectors aren't likely to be backward-compatible. Cat 7 and 7a are ISO/IEC 11801 Class F cabling standards.

Categories 5e and 6 are by far the most installed categories of UTP cabling. Their huge installed base guarantees that developers of new high-speed networking technologies will strive to make their technologies compatible with these categories; for example, Category 5 cable, originally designed for 10 Mbps Ethernet, is capable (although not recommended) of running at speeds up to 1 Gbps. Table 4-2 summarizes the characteristics of the two most common UTP cabling types.

Table 4-2 Category 5e and 6 UTP cabling characteristics

Characteristic	Value
Maximum cable length	100 m (328 ft)
Bandwidth	Up to 1000 Mbps
Bend radius	Minimum four times the cable diameter or 1 inch
Installation and maintenance	Easy to install, no need to reroute; the most flexible
Cost	Least expensive of all cabling options
Connector type	RJ-45 plug, RJ-45 jack, and patch panels
Security	Moderately susceptible to eavesdropping
Signaling rates	100 MHz for Cat 5e; 250 MHz for Cat 6
Interference rating	Susceptible to EMI and crosstalk

Shielded Twisted-Pair Cable

As its name indicates, STP includes shielding to reduce crosstalk and limit the effects of external interference. For most STP cables, this means the wiring includes a wire braid inside the cladding or sheath material as well as a foil wrap around each wire pair. This shielding improves the cable's transmission speed and resistance to interference, which allows using STP in electrically noisy environments or very high-bandwidth applications. You can readily find STP versions of Cat 5e (shown in Figure 4-2), Cat 6, and Cat 6a. These STP versions are sometimes referred to as "foiled twisted pair (FTP)," and the shielding surrounds all four wire pairs rather than each wire pair.

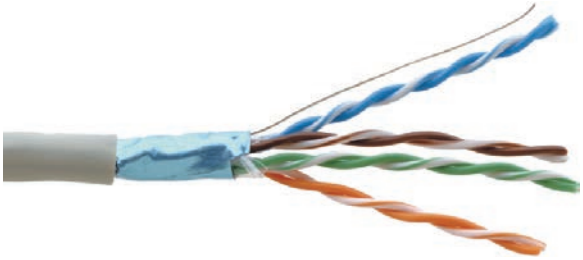


Figure 4-2 Cat 5e shielded twisted pair

Twisted-Pair Cable Plant Components

A twisted-pair cable plant requires more than just the cabling, which is usually sold in spools of 1000 feet. In addition, you find most of the following components:

- *RJ-45 connectors*—Whether STP or UTP, most twisted-pair cabling uses registered jack 45 (RJ-45) connectors to plug into network interfaces or other networked devices. This connector looks much like the RJ-11 connector on modular phone jacks, but it's larger and contains eight wire traces rather than the four or six in an RJ-11. An RJ-45 connector (see Figure 4-3), often called an **RJ-45 plug**, is most commonly used in patch cables, which are used to connect computers to switches and computers to RJ-45 wall jacks.

Figure 4-3 An RJ-45 plug

Courtesy of Hyperline Systems

- *Patch cable*—A **patch cable** (see Figure 4-4) is a short cable for connecting a computer to an RJ-45 jack or connecting a patch-panel port to a switch or hub. Patch cables can be made with inexpensive tools, two RJ-45 plugs, and a length of TP cable, which you do later in Hands-On Project 4-1. Although making a patch cable is easy, most network administrators prefer buying ready-made cables to save time.

Figure 4-4 A patch cable
spilman/Shutterstock.com

- *RJ-45 jacks*—An **RJ-45 jack** (shown in Figure 4-5) is what you plug an RJ-45 connector into when the computer is in a work area away from hubs and switches. It has a receptacle for an RJ-45 plug on one side and a place to terminate, or "punch down," the TP cabling on the other side. RJ-45 jacks are usually placed behind wall plates when cables are run inside walls but can also be recessed into the floor or placed in surface-mounted boxes if the cabling runs on the outside of walls.

Figure 4-5 An RJ-45 jack
Courtesy of Hyperline Systems

- *Patch panels*—Patch panels are used to terminate long runs of cable from the work area (where computers are) to the wiring closet (where switches are). Patch panels are like RJ-45 jacks, in that they have a receptacle on one end and punchdown terminals on the other, but a patch panel can usually accommodate 12, 24, or 48 cables. Figure 4-6 shows the front side of a patch panel, where a patch cable plugs in, and the back side, where long runs of cable are terminated.

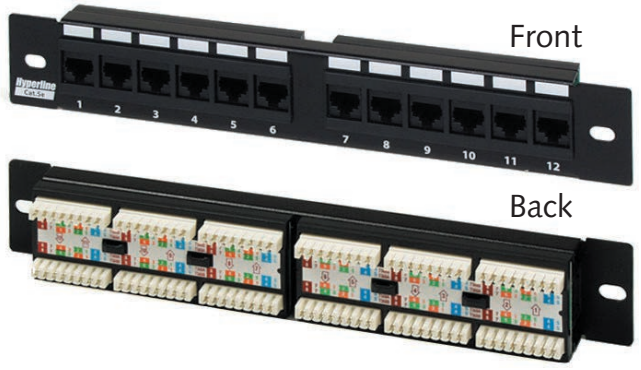


Figure 4-6 Patch panel front and back

Courtesy of Hyperline Systems

- *Distribution racks*—Distribution racks (also called 19-inch racks because the upright rails are 19 inches apart) hold network equipment, such as routers and switches, plus patch panels and rack-mounted servers. They're usually found in wiring closets and equipment rooms. Figure 4-7 shows a typical distribution rack.

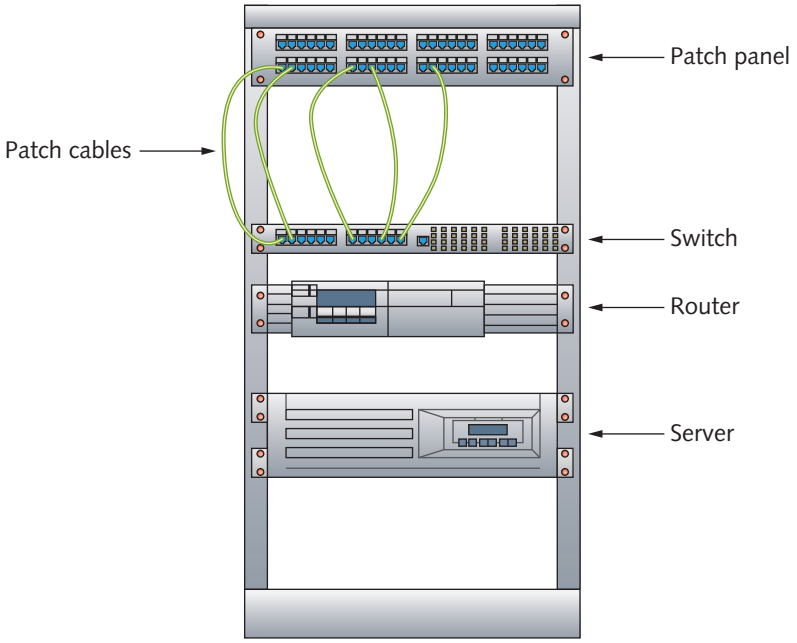


Figure 4-7 A distribution rack

The following sections explain how to use these components to construct a cable plant.

Structured Cabling: Managing and Installing a UTP Cable Plant

Entire books are written on cable installation and management, and the details are beyond the scope of this book. However, understanding some basic methods and terminology of cable installation and management gives you a good foundation. As mentioned, the TIA/EIA developed the document "568 Commercial Building Wiring Standard," which specifies how network media should be installed to maximize performance and efficiency. This standard defines what's often referred to as "structured cabling."

Note

The 568 Commercial Building Wiring Standard covers all media types, but the discussion in this section focuses on UTP cabling, the most common media for LANs and internetworks.

Structured cabling specifies how cabling should be organized, regardless of the media type or network architecture. Although a variety of logical topologies can be used, structured cabling relies on an extended star physical topology. TIA/EIA 568 can be applied to any network size and divides the details of a cable plant into six components. A small LAN in a 10-computer business might need only two or three of these components, but large networks typically use most or all of these components:

- Work area
- Horizontal wiring
- Telecommunications closets
- Equipment rooms
- Backbone or vertical wiring
- Entrance facilities

Network cabling standards are designed to ensure adherence to standards for equipment rooms and wiring closets, including limitations on media, which helps limit the possible reasons for network failure or poor performance. If the network cable plant is in good working order and meets standards, a network administrator's job is easier. Structured cabling facilitates troubleshooting as well as network upgrades and expansion.

Work Area

The **work area**, as the name suggests, is where workstations and other user devices are located—in short, the place where people work. Faceplates and wall jacks are installed in the work area, and patch cables connect computers and printers to wall

jacks, which are connected to a nearby telecommunications closet. Patch cables in the work area should be less than 6 meters long (about 20 feet). The TIA/EIA 568 standard calls for at least one voice and one data outlet on each faceplate in each work area. The connection between a wall jack and a telecommunications closet is made with horizontal wiring. Figure 4-8 shows the components of the work area.

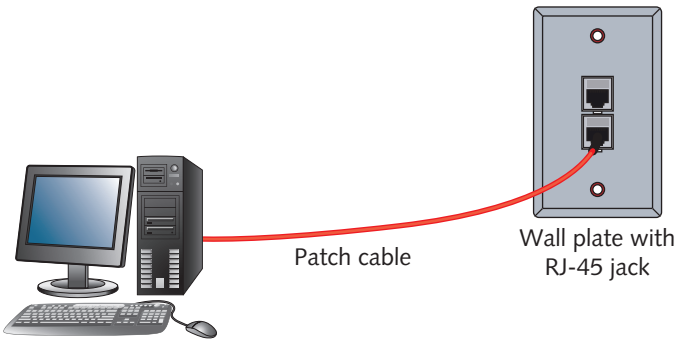


Figure 4-8 Work area components

Horizontal Wiring

Horizontal wiring runs from the work area's wall jack to the telecommunications closet and is usually terminated at a patch panel. Acceptable horizontal wiring types include four-pair Cat 5e or Cat 6/6a or two fiber-optic cables. The total maximum distance for horizontal wiring is up to 100 meters, which includes the cable running from the wall jack to the patch panel plus all patch cables. However, horizontal wiring from the wall jack to the patch panel should be no longer than 90 meters to allow up to 10 meters for patch cables.

Telecommunications Closet

The **telecommunications closet (TC)** provides connectivity to computer equipment in the nearby work area. In small installations, it can also serve as the entrance facility (explained later in "Entrance Facilities"). Typical equipment includes patch panels to terminate horizontal wiring runs, switches to provide network connectivity, and patch cables to connect patch panels to switches. In smaller installations, network servers can be housed in the TC. Larger installations usually have connections from the TC to an equipment room (discussed next). A telecommunications closet that houses the cabling and devices for work area computers is referred to as an **intermediate distribution frame (IDF)**. Figure 4-9 shows the relationship and connections between the work area, horizontal wiring, and IDF.

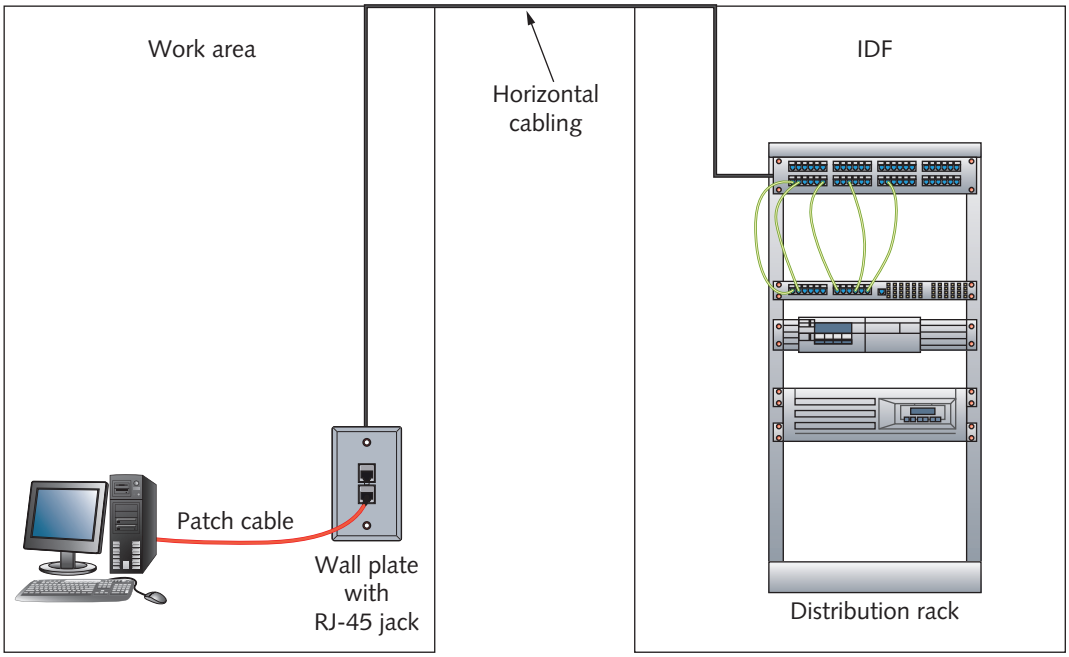


Figure 4-9 Work area, horizontal wiring, and IDF

Equipment Rooms

The **equipment room** houses servers, routers, switches, and other major network equipment and serves as a connection point for backbone cabling running between IDFs. An equipment room that's the connection point between IDFs is called a **main distribution frame (MDF)** or "main cross-connect." An MDF can be the main cross-connect of backbone cabling for the entire network, or it might serve as the connecting point for backbone cabling between buildings. In multi-building installations, each building often has its own MDF.

Backbone Cabling

Backbone cabling (or vertical cabling) interconnects IDFs and MDFs. This cabling runs between floors or wings of a building and between buildings to carry network traffic destined for devices outside the work area. It's often fiber-optic cable but can also be UTP if the distance between rooms is less than 90 meters. When it connects buildings, backbone cabling is almost always fiber optic because of UTP's distance limitations and because fiber doesn't propagate lightning strikes or electrical imbalances between buildings. Multimode fiber-optic cable can extend up to 2000 meters, whereas single-mode fiber can reach distances up to 3000 meters when used as backbone cabling between the MDF and IDFs. Figure 4-10 shows how backbone cabling can connect IDFs to an MDF.

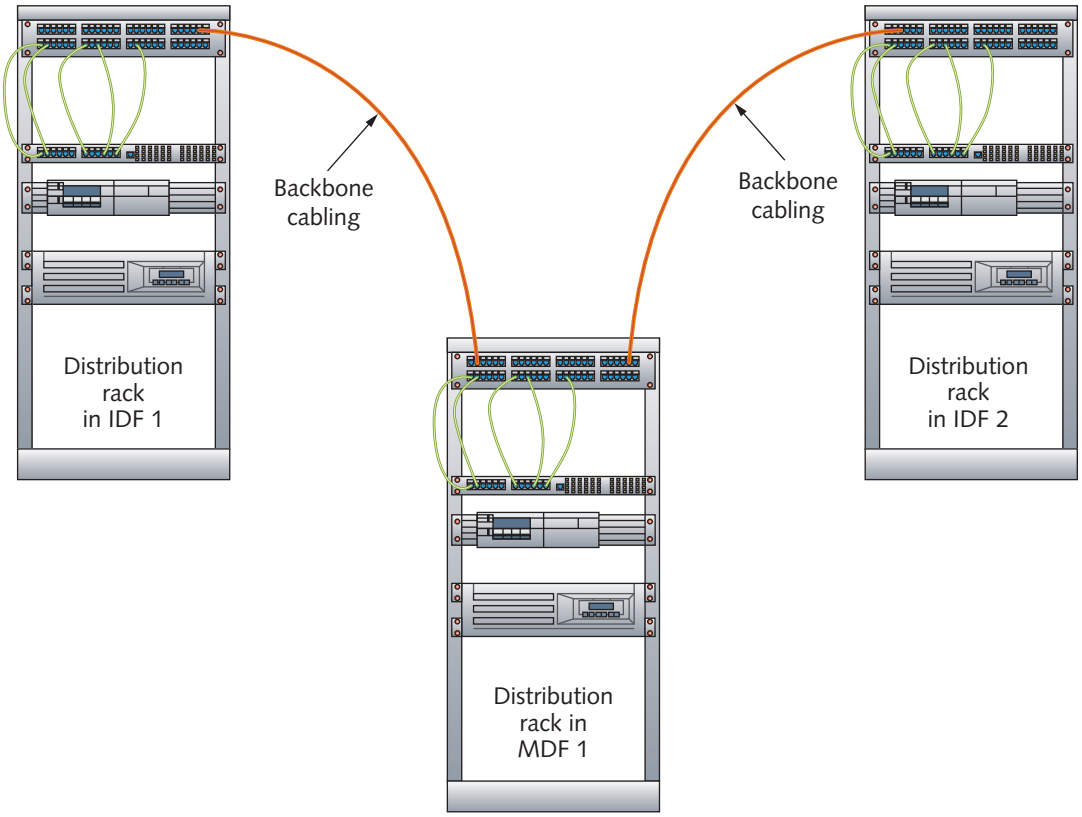


Figure 4-10 Backbone cabling connects IDFs and MDFs

Entrance Facilities

An **entrance facility** is the location of the cabling and equipment that connects an organization's network to a third-party telecommunications provider. It can also serve as an equipment room and the MDF for all backbone cabling. This location is also where a connection to a WAN is made and where an organization's LAN equipment ends and a third-party provider's equipment and cabling begins—also known as the **demarcation point**.

Installing UTP Cabling

One skill required of a network technician is terminating UTP cables. Cable **termination** means putting RJ-45 plugs on a cable to make a patch cable or punching down cable wires into terminal blocks on a jack or patch panel. To create a patch panel, a technician needs the following tools:

- Bulk UTP cabling
- Wire cutters or electrician's scissors
- Cable stripper

- Crimping tool
- Cable tester
- RJ-45 plugs

To terminate cable at an RJ-45 jack or a patch panel, you need the following tools:

- Bulk UTP cabling
- Wire cutters or electrician's scissors
- Cable stripper
- Type 110 punchdown tool
- Cable tester
- RJ-45 jack and patch panel

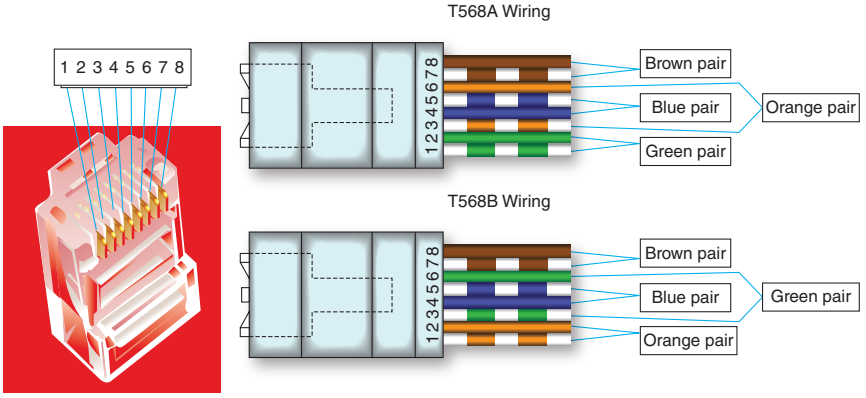
Some of these tools are shown in Figure 4-11.

Figure 4-11 Cable installation and termination tools

The quality of the tools needed for cable installation varies considerably, usually according to cost. If you expect to be doing a lot of cable termination, it pays to invest in high-quality tools, particularly a cable tester. If you're installing only a few dozen to a few hundred cables, you might get away with less expensive tools and a basic cable

tester. However, if you have a cable-installation business, you want high-quality tools, including a cable tester that certifies the cable plant for the category of cable installed.

Hands-On Project 4-1 walks you through making a patch cable. One of the most important aspects of making a cable or terminating a cable at a jack or patch panel is to get the colored wires arranged in the correct order. There are two competing standards for the arrangement of wires: TIA/EIA 568A and TIA/EIA 568B. Either standard is okay to follow, as long as you stick to one throughout your network. Figure 4-12 shows the arrangement of wires for both standards for 10/100 Ethernet and Gigabit Ethernet.



Pin #	T568A Color	T568B Color	Fast Ethernet function	Gigabit Ethernet function
1	White/green	White/orange	Tx+	Bidirectional+
2	Green	Orange	Tx−	Bidirectional−
3	White/orange	White/green	Rx+	Bidirectional+
4	Blue	Blue	*Unused*	Bidirectional+
5	White/blue	White/blue	*Unused*	Bidirectional−
6	Orange	Green	Rx−	Bidirectional−
7	White/brown	White/brown	*Unused*	Bidirectional+
8	Brown	Brown	*Unused*	Bidirectional−

Figure 4-12 TIA/EIA 568A and 568B cable pinouts

Straight-Through versus Crossover Cable

When you make a standard patch cable, you use the same wiring standards on both ends of the cable so that each wire is in the same corresponding location on both ends of the cable (pin 1 goes to pin 1, pin 2 to pin 2, and so forth). This type of cable is also called a **straight-through cable**. Another type of cable, called a **crossover cable**, uses the 568B standard on one end and the 568A standard on the other end. This arrangement crosses the transmit and receive wires so that transmit signals on one end connect to receive signals on the other end. This type of cable is often

needed when you connect two devices of the same type to one another—for example, connecting a hub to a hub, a switch to a switch, a hub to a switch, or a PC to a PC. However, for a 1000BaseT crossover cable, you have to cross the blue and brown pins because they're used in 1000BaseT. Table 4-3 shows the pinout for a 1000BaseT crossover cable. This configuration also works for a 10BaseT or 100BaseT crossover cable, even though the brown and blue pins aren't used.

Table 4-3 Pinout for a 1000BaseT crossover cable

Pin	Connector 1	Connector 2
1	White with orange stripe	White with green stripe
2	Orange	Green
3	White with green stripe	White with orange stripe
4	Blue	White with brown stripe
5	White with blue stripe	Brown
6	Green	Orange
7	White with brown stripe	Blue
8	Brown	White with blue stripe

Medium Dependent Interface

Network devices connecting with RJ-45 plugs over twisted-pair cabling are classified as **medium dependent interface (MDI) devices** or **MDI crossed (MDI-X) devices**. You might even see these abbreviations on some switches. For communication to take place between two devices, the wires one device transmits on must be connected to the wires the other device receives on, and vice versa. For example, the 568 standards have pins 1 and 2 labeled as transmit and pins 3 and 6 labeled as receive. Clearly, not all devices can transmit on pins 1 and 2 and receive on pins 3 and 6; otherwise, a standard patch cable wouldn't work between these devices because one device's transmit signals would be going to the transmitter of the other device—like having a phone's earpiece at your mouth and the mouthpiece at your ear.

MDI devices transmit on pins 1 and 2 and receive on pins 3 and 6. Examples include PC NICs and routers. MDI-X devices, usually hubs and switches, receive on pins 1 and 2 and transmit on pins 3 and 6. Therefore, a straight-through patch cable works for the most common connection of a PC NIC to a switch. When a switch needs to be connected to a switch (or a PC to a PC), you use a crossover cable so that the transmit and receive wires get crossed, and you end up with transmit going to receive and vice versa. Thankfully, developers of NICs, switches, and routers have started doing this job for you by making "auto-sensing" ports on some devices. Auto-sensing means a port can detect whether you're trying to connect transmit wires to transmit wires, and the port reconfigures its

transmit and receive wires, thus making a crossover cable unnecessary. Not all devices support auto-sensing, so it's best to have crossover cables handy in case you need them. Table 4-4 lists common types of devices and the type of cable required to connect them if they don't support auto-sensing. Hubs and switches use the same connection type, so when you see a switch in the table, a hub uses the same type of cable.

Table 4-4 Device connections and cable type

Device	Connected to	Type of cable
Switch	Switch	Crossover
Switch	Router	Straight-through
Switch	PC	Straight-through
Router	Router	Crossover
Router	PC	Crossover
PC	PC	Crossover

Note

Another type of cable you might run across is called a "rollover cable," which is designed to connect a PC's serial communication port and a Cisco device's console port for configuring the Cisco device. You use terminal emulation software, such as PuTTY, to get a command-line interface prompt from the Cisco device so that you can enter commands to view and change its configuration. A rollover cable reverses all eight wires; in other words, the wires on one end are connected to pins 1 through 8, and on the other end, they're connected to pins 8 through 1. So, pin 1 goes to pin 8, pin 2 to pin 7, pin 3 to pin 6, and so forth.

Hands-On Project 4-1: Making a Patch Cable

Time Required: 20 minutes
Objective: Create a 568B straight-through patch cable.
Required Tools and Equipment: Wire cutter and cable stripper, RJ-45 crimping tool, 2 to 4 feet of Cat 5e or Cat 6 cable, two RJ-45 plugs, and a cable tester (optional)
Description: In this project, you make a patch cable according to the instructions. The instructor will inspect the cable for the correct wire order and strain relief. If possible, use a cable tester to test for conductivity and wiremap, at a minimum.

1. Strip approximately 2 inches of the outer jacket off one end of the cable with the cable stripper. Be careful not to nick the inner wires' insulation. Most UTP cable strippers are calibrated to score the cable's outer jacket so that you can simply break it off. Cable

strippers differ in the techniques you use with them, so refer to the instructions that came with yours or ask your instructor.

2. Untwist the four pairs of wires.
3. Here comes the tricky part: Arrange the wires from left to right (as you're looking down on them) so that they're in the following order: white with orange stripe, orange, white with green stripe, blue, white with blue stripe, green, white with brown stripe, and brown. This order adheres to the 568B wiring standard (see Figure 4-13).

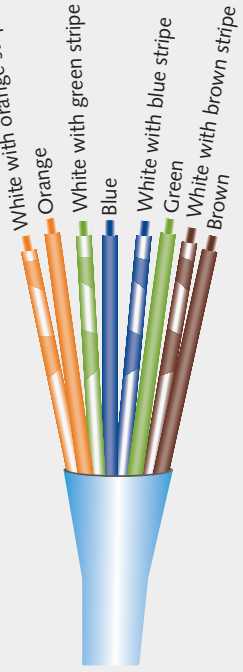


Figure 4-13 The correct arrangement of wires

4. Clip the eight wires so that a little more than a half-inch of wire extends beyond the outer jacket.
5. While holding the RJ-45 plug in one hand with the clip facing away from you, insert the eight wires into the connector, making sure the tops of wires extend to the front of the connector and the cable jacket goes far enough into the connector so that the jacket will be caught by the crimp bar (see Figure 4-14).

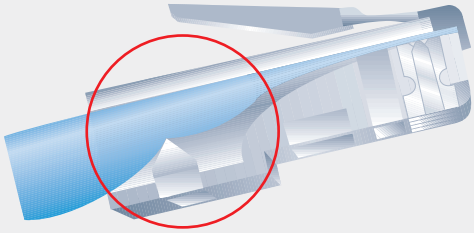


Figure 4-14 Correct RJ-45 plug installation

6. Now insert the RJ-45 connector into the crimping tool, and make sure the wires don't slip. Squeeze the handle on the crimping tool firmly. It might take a little hand strength or using two hands, depending on the crimping tool's quality. This tool does two things. First, it forces the eight small contacts at the top of the plug down onto the wires; the contacts are pushed just far enough in that they slice through the insulation on each wire, thereby making an electrical contact with the wire. Second, the strain-relief bar is pushed in to grab the cable's outer jacket, making it more difficult to pull the wires out of the plug.
7. Repeat the process for the other end of the cable, and test with a cable tester, if available. Congratulations! You have made a patch cable. Where do you find patch cables in structure cabling installations? Describe the connections they make.

_____

_____

8. Keep your tools handy for the next project.

Hands-On Project 4-2: Terminating UTP Cable

Time Required: 20 minutes
Objective: Terminate UTP cable at a patch panel and an RJ-45 jack.
Required Tools and Equipment: Wire cutter and cable stripper, 2 to 4 feet of Cat 5e or Cat 6 cable, 110 punchdown tool, Cat 5e or Cat 6 patch panel (a 568A or 568B patch panel can be used; 568B panels are more common), RJ-45 jack, and a cable tester (optional)
Description: In this project, you punch down one end of a cable to the back of a patch panel.

1. Strip approximately 2 inches of the outer jacket off one end of the cable with the cable stripper. Be careful not to nick the inner wires.
2. Leave the wire pairs twisted. Arrange the wires according to the color coding on your patch panel. The color coding will vary, depending on whether it's a 568A or 568B patch panel, and the wires might be arranged in a straight line or split between the two rows of terminals.
3. Center the cable so that each wire is equally distant from the terminal in which it will be placed. On each wire pair, separate the wires about one-half inch or less from the end of the jacket so that the two wires form an oval, and slip the wire pair over its middle terminal (see Figure 4-15). Pull each wire pair down firmly so that the wires stay in place.
4. Next, use the 110 punchdown tool. Place the tool over each wire so that the slot in the tool lines up with the wire. The tool's blade should be facing the end of the wires, not the cable jacket (see Figure 4-16).
5. Push the punchdown tool down firmly until you hear it snap. Don't be afraid to give it a good, hard push. The blade should cut the wire or at least score it so that you can gently twist the end off. Do this for all eight wires.

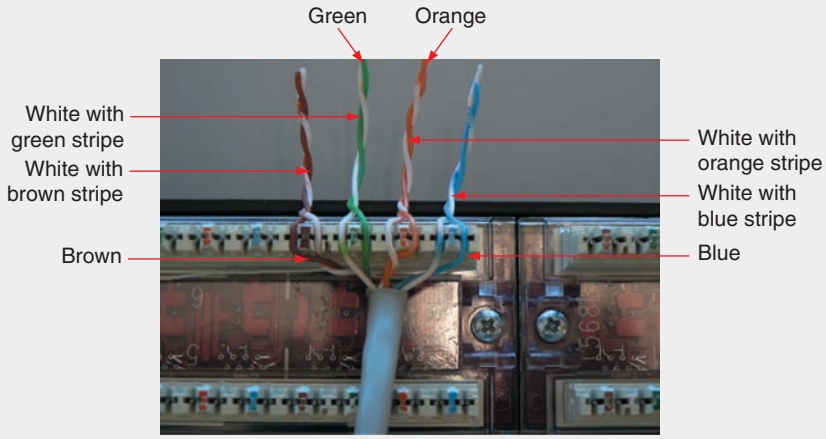


Figure 4-15 Placing wires on the patch panel terminals

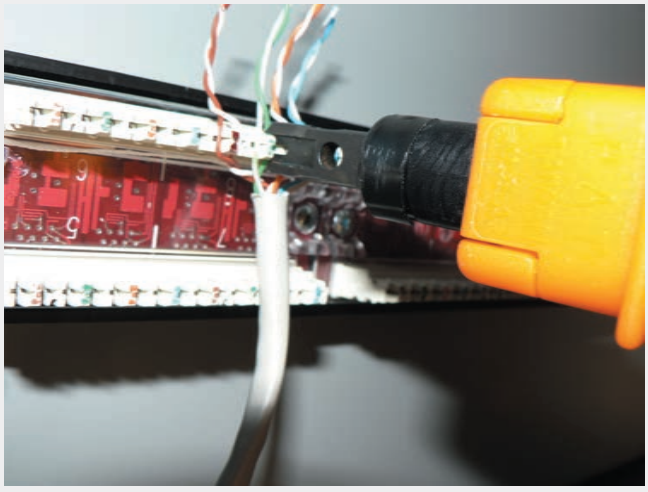


Figure 4-16 Positioning the punchdown tool

6. That's it! A correct termination should have no more than one-half inch of untwisted wire outside the jacket. Repeat this process for the other end of the cable, but this time, terminate the cable onto an RJ-45 jack. In structured cabling, what's the run of cable called that goes from a wall jack to a patch panel?

_____

7. Keep your cables and tools ready for the next project.

Hands-On Project 4-3: Conducting End-to-End Testing

Time Required: 10 minutes
Objective: Test your terminations and patch cable with a live connection.
Required Tools and Equipment: The patch cable you made, an additional patch cable, the patch panel and RJ-45 jack to which you terminated the cable, a lab computer, and a switch
Description: Working in groups of at least two, use the patch cable you made to connect a lab computer to the RJ-45 jack you punched down. Using an additional patch cable, connect the patch panel to a switch. Then use the `ping` command to verify connectivity between computers.

1. Using the patch cable you made in Hands-On Project 4-1, connect your lab computer's NIC to the RJ-45 jack you punched down in Hands-On Project 4-2.
2. Using the additional patch cable, connect the port on the patch panel you punched down to a switch.
3. Turn on the PC and the switch, if necessary.
4. Verify that you have a link light at the switch and at your lab computer's NIC. Log on to your computer, and give your computer's IP address to another student who's connected to the switch.
5. Ping another student's computer after getting his or her IP address. If the ping is successful, your cable termination was a success.
6. If you're sharing computers, allow the next group of students to test their cabling.
7. Shut down your computer if no one else is using it for testing.

Why Two Transmit and Two Receive Wires?

As you can see from the cable pinout diagrams shown previously in Figure 4-12, one wire pair in 10BaseT and 100BaseT Ethernet is used for transmit (labeled Tx+/Tx-) and one wire pair is used for receive (labeled Rx+/Rx-). The plus and minus symbols indicate that the wires carry a positive or negative signal. This **differential signal** mitigates the effects of crosstalk and noise on the cable. It does so because a bit signal is transmitted as a positive voltage and a negative voltage (V). For example, if a 1 bit is defined as +2V, the bit is transmitted as +2V on one wire and -2V on the other wire. The receiver reads the difference between the two values, which is 4V. EMI and crosstalk manifest as positive voltages, so what happens if the signal is hit by a burst of EMI that adds 1V to the signal? You have the following:

Original signal with no EMI:

Transmit+	Transmit+	Differential result
+2V	-2V	+4V

Signal with EMI adding 1V to both transmit+ and transmit- wires:

Transmit+	Transmit+	Differential result
+2V + 1V = 3V	-2V + 1V = -1V	+4V

As you can see, the result stays at +4V in both cases because the differential signal effectively cancels out the EMI. However, this canceling effect works only if the same amount of EMI is imposed on both wires. The closer the wires are, the more likely it is that EMI will affect both wires equally. This phenomenon is one reason for using twisted wires: The wires are so tightly coupled that both external EMI and crosstalk are likely to affect both wires equally and be canceled out.

Although UTP is the most common media type for LANs, it has its limitations in bandwidth, noise susceptibility, and length. In addition, UTP wiring shouldn't be used outside to connect between buildings. Copper wire is susceptible to the elements, and its electrical conducting properties change slightly depending on the temperature. A more important reason not to use any type of copper wire between buildings is that it can carry a harmful electrical charge based on the ground potential between buildings if they are fed from different transformers. When any of these limitations eliminate UTP as an option, fiber-optic cable is the likely solution.

Fiber-Optic Cable

Fiber-optic cable trades electrical pulses for pulses of light to represent bits. Because no electrical signals ever pass through the cable, fiber-optic cabling is as immune to electrical interference as any medium can get. Therefore, light pulses are unaffected by EMI and RFI. This characteristic also makes fiber-optic cables highly secure. They emit no external signals that might be detected, unlike electrical or broadcast media, thereby eliminating the possibility of electronic eavesdropping. In particular, fiber-optic cable is a good medium for high-bandwidth, high-speed, long-distance data transmission because of its lower attenuation characteristics and vastly higher bandwidth potential. Commercial implementations at 10, 40, and 100 Gbps are currently in use.

Figure 4-17 shows a typical fiber-optic cable. A slender cylinder of glass fiber called the "core" is surrounded by a concentric layer of glass known as the cladding. The fiber is then jacketed in a thin, transparent plastic material called the "buffer." These three components make up what's labeled as the optical fiber in this figure. The fiber is optionally surrounded by an inner sheath made of colored plastic. A strengthening material, usually made of Kevlar, comes next, followed by an outer sheath. Sometimes the core consists of plastic rather than glass fibers; plastic is more flexible and less sensitive to damage than glass, but attenuation is more of a problem with plastic than with glass.

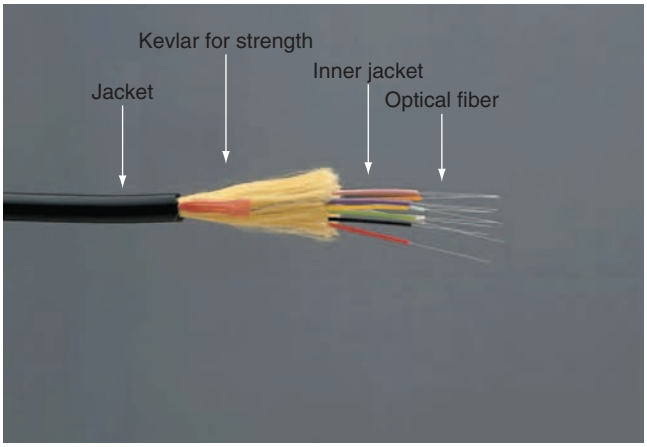


Figure 4-17 Fiber-optic cable

In most cases, the fiber-optic strand carries data in only one direction, meaning fiber-optic network connections typically consist of two or more strands, each in a separate inner sheath. However, these cables can also be enclosed in a single sheath. Just as you have UTP patch cables, you also find fiber-optic patch cables, usually to connect from a fiber-optic patch panel to a switch or router. Fiber-optic cable used as backbone cabling often comes in bundles of 12 or more fiber strands. Even if you're using only two strands at first, it's a good idea to run cable containing more fiber than you need, in case a strand breaks during installation or you need additional strands for future growth.

Some testing has shown that glass fibers can carry several terabits (1000 gigabits) per second (Tbps). There's really no end in sight for the bandwidth capacity of optical fiber. As network bandwidth needs increase and the limits of copper wire are reached, fiber-optic cable might eventually replace copper for all types of network connections. Table 4-5 summarizes fiber-optic cable characteristics.

Table 4-5 Fiber-optic cable characteristics

Characteristic	Value
Maximum cable length	2 km (6562 ft) to 100 km (62.14 miles)
Bandwidth	10, 40, and 100 Gbps and higher
Bend radius	30 degrees per foot
Installation and maintenance	Difficult to install and reroute; sensitive to strain and bending
Cost	Most expensive of all cabling options
Connector type	Several types (see bulleted list in the next section)
Security	Not susceptible to eavesdropping
Interference rating	None; least susceptible of all cable types

Fiber-Optic Connectors

A wide variety of connectors can be used with fiber-optic media, depending on the light-emitting sources used to generate light pulses and the corresponding light-detecting sensors used to detect them. Figure 4-18 shows some connectors described in the following list:

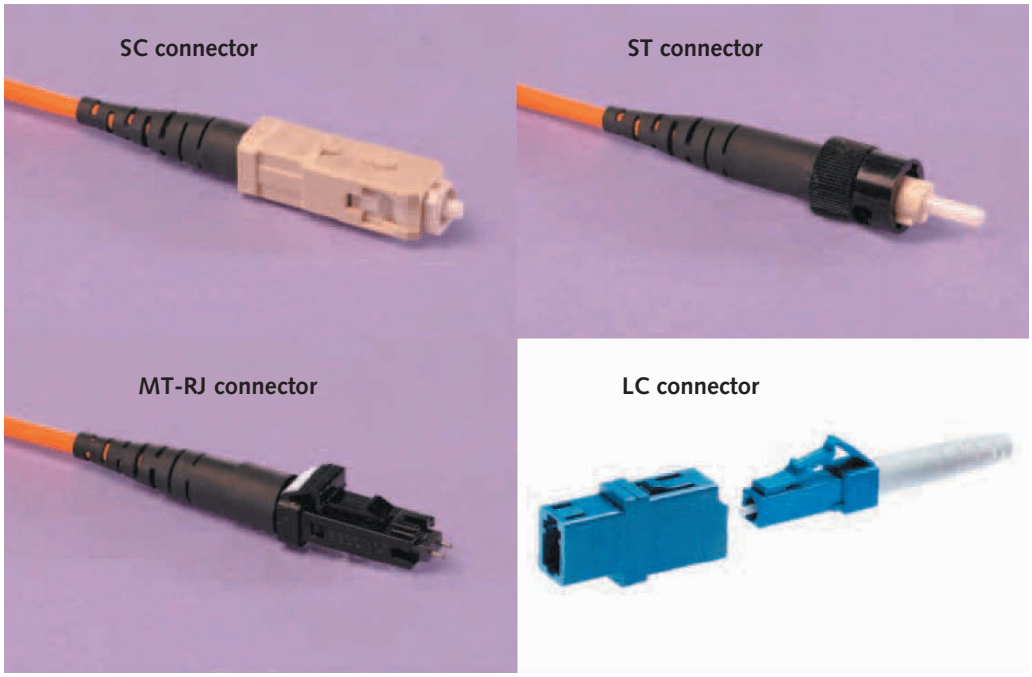


Figure 4-18 Fiber-optic connectors

- *Straight tip*—Straight tip (ST) connectors join fibers at cross-connects or to optical devices. They're used most often in Ethernet networks with fiber-optic cable as backbone cabling. An ST connector locks onto the jack when twisted.
- *Straight connection*—Straight connection (SC) connectors push on, which makes them easy to install and requires less space for an attachment. They make a strong connection and can be used when splicing fiber-optic cables. An SC connector is a one-piece component, with two receptacles for sending and receiving fibers. A notch in its jacket ensures the correct orientation when inserted.
- *Locking connection*—Locking connection (LC) connectors push on and pull off with an RJ-45-style latching mechanism. They're about half the size of SC connectors, which makes them good for high-density applications, in which many fibers are concentrated in one location.
- *Mechanical transfer registered jack*—A mechanical transfer registered jack (MT-RJ) connector looks a little like an RJ-45 connector. It provides a high-density

fiber-optic connection by using two fiber-optic cables. Compared with other connector types, MT-RJ connectors take only half the space for the same number of cable terminations. They're also easy to install and require only one connector for a two-fiber termination.

- *Fiber channel*—A fiber channel or ferrule connector (FC) is used in some measurement equipment applications and with single-mode lasers. This type of connector is less common than most of the others in this list for LAN and WAN applications.
- *Medium interface connector*—A medium interface connector (MIC) is used for Fiber Distributed Data Interface (FDDI). Like SC connectors, MIC connectors are one-piece constructions.
- *Subminiature type A*—The company Amphenol originally designed subminiature type A (SMA) connectors for microwave use and later modified them for fiber-optic use. Two SMA versions are widely available: The 905 uses a straight ferrule, which is a metal sleeve for strengthening the connector, and the 906 uses a stepped ferrule with a plastic sleeve to ensure precise alignment of fibers. Like ST connectors, SMAs use two connectors for each fiber strand.

Fiber-Optic Installation

Installing fiber-optic networks is somewhat more difficult and time consuming than copper media installation. However, advances in connector technology have made field termination of fiber-optic cables almost as fast and easy as copper terminations. The connectors and test equipment for termination are still considerably more expensive than their copper counterparts, but the trend toward easier, more affordable fiber-optic networks continues. Fiber-optic cable to the desktop, although not common, is becoming a feasible option for more companies.

There are several methods for terminating fiber-optic cables because of the many connectors and cable types available, so installation details are beyond the scope of this book. Before embarking on a fiber-optic termination task, you need to purchase a fiber-optic termination kit, which can range from several hundred to several thousand dollars. Some tools in a typical fiber-optic termination kit include the following:

- *Buffer tube stripper*—A tightly calibrated tool designed for stripping buffer tubes off the glass fiber strand without breaking the fiber
- *Cable stripper*—Used to remove the fiber cable's outer sheath; much like the cable stripper used with UTP
- *Crimper*—Used with connectors that use crimping as the method to fix the connector to the cable, such as MT-RJ connectors
- *Diamond cleaver*—Used to cut glass fiber cleanly without shattering the end
- *Inspection scope*—Used for examining the end of a fiber strand to make sure it's clean and polished
- *Polishing tool*—Used to polish the end of a cleaved (cut) strand of fiber

Fiber-Optic Cable Types

Fiber-optic cables come in two main types: single-mode fiber (SMF) cables, which include a single, extremely small-diameter fiber (typically 8 microns) at the core, and multimode fiber (MMF) cables, which use a considerably larger-diameter fiber (50 and 62.5 microns are standard sizes) at the core. SMF cable costs more and generally works with laser-based emitters but spans the longest distances and is used in higher-bandwidth applications. MMF cables cost less and work with lower-power light emitting diodes (LEDs), which span shorter distances.

In the past, fiber-optic cable's high cost and difficult installation meant it was used only when a network required extremely high bandwidth or needed to span long distances between wired network segments. However, because of the falling costs of fiber and its advantages in immunity to interference, high-bandwidth capability, and increased security, it's now used almost exclusively for all network backbone connections. It's also the medium of choice for long-haul telecommunications, in which large amounts of voice and data traffic are aggregated, such as between telecommunication providers and ISPs.

Cable-Testing Equipment

Network cable installers should have a variety of testing and troubleshooting gadgets in their toolkits. Cable-testing tools are used to detect incorrect terminations, breaks, shorts, excessive noise or crosstalk, and cable length, among other problems and characteristics. The following list describes some common tools for testing and troubleshooting wired networks:

- *Cable certifier*—As mentioned, cable certifiers do a full battery of tests to certify that a cable installation meets a particular wiring standard, such as Cat 5e, Cat 6, or Cat 6a. These tools check for total segment length, crosstalk, noise, wiremap, resistance, impedance, and the capability to transfer data at the maximum frequency rated for the cable. They do the most complete testing of the tools discussed in this list and therefore cost the most.
- *Basic cable tester*—This device varies by capability and cost. Most cable testers check for wiremap, shorts, and opens, and some also check for length and crosstalk. They're mostly intended to let installers know that wires have been terminated correctly, but they don't certify a cable for a particular category. Basic cable testers sometimes come with several ID plugs that help you identify the cable end you are testing. You plug several ID plugs into patch panel ports and the ID number (for example, 1, 2, 3) shows on the display of the cable tester at the other end of the cable, allowing you to quickly identify which cable goes to which patch panel port.
- *Tone generator*—This tool is used to locate both ends of the same wire. It issues a signal on one end of a wire, and a probe is used on the other end of the wire to verify continuity. The probe delivers an audible tone when it's touched to the

same wire as the tone generator. In some installations, dozens or hundreds of cables are installed in the work area, with the other end of the cables in an IDF. To match up the two ends of the cable, a technician places the tone generator on a wire in the work area, and the technician in the IDF touches each wire until the tone is heard. There are other methods to locate cables. For example, cable certifiers and some basic cable testers include remote ID plugs that are plugged into a patch panel's ports, and the end of the cable in the work area is plugged into the cable tester. The cable tester runs through its tests and displays the ID number of the remote ID plug to let the installer know to which patch panel port the cable is terminated.

- *Time domain reflectometer*—A TDR measures cable length by transmitting a signal on one end and measuring the time it takes for the reflection (signal bounce) to reach the end of the cable. TDRs are useful for finding a cable's total segment length and finding breaks. For example, if a cable is believed to be about 80 meters, but you don't have end-to-end continuity because of a break in the cable, a TDR can tell you approximately how far down the cable the break is located. A similar tool for fiber-optic cables, called an "optical time domain reflectometer (OTDR)," can also measure the location of breaks, bad connectors, and signal attenuation.
- *Multimeter*—This device can measure properties of electrical signals, such as voltage, resistance, impedance, and current. It's not often used to test communications cables but is handy for measuring DC and AC voltage and resistance levels on electrical circuits and power supplies. It can be used with some coaxial cable installations to measure impedance and test for shorts and opens.
- *Optical power meter*—An OPM measures the amount of light transmitted by a device on a fiber-optic cable and whether the amount of light on the cable's receiver meets the requirements for the device you're connecting. OPMs and OTDRs can be stand-alone devices but are also built into fiber-optic cable certifiers.

Wireless Networking

Certification

98-366 Understanding network infrastructure:

Understand wireless networking

Wireless technologies are playing a bigger role in all kinds of networks. Since 1990, wireless options have increased, and the cost of these technologies continues to

decrease. As wireless networking has become more affordable, demand has increased, and as it does, so does production of wireless equipment, which brings prices down even more. For this reason, wireless networks are now ubiquitous, with free Wi-Fi hotspots available in restaurants, coffee shops, shopping centers, and most places where a lot of paying customers can be found.

The adjective "wireless" might lead you to believe that wireless networks have no cabling of any kind. However, wireless networks are often used with wired networks to interconnect geographically dispersed LANs or groups of mobile users with wired servers and resources on a wired LAN. Networks that include both wired and wireless components are called "hybrid networks." Indeed, even in home or small business networks with workstations connecting to a wireless AP or router, the AP or router usually connects to the Internet via a wired connection to a cable modem or similar device. Probably the only truly wireless networks are ad hoc networks or small infrastructure networks put together for the purpose of sharing files among a small group of people.

Wireless Benefits

Wireless networking has a lot of appeal in many circumstances and can offer the following capabilities:

- Create temporary connections to existing wired networks.
- Establish backup or contingency connectivity for existing wired networks.
- Extend a network's span beyond the reach of wire-based or fiber-optic cabling, especially in older buildings where rewiring might be too expensive.
- Allow businesses to provide customers with wireless networking easily, thereby offering a service that gets customers in and keeps them there.
- Enable users to roam around an organization or college campus with their devices.

Each capability supports uses that extend the benefits of networking beyond conventional limits. Common applications for wireless networking technologies include the following:

- Ready access to data for mobile workers, such as doctors and nurses in hospitals or delivery personnel. For instance, United Parcel Service (UPS) drivers maintain connections to a server at the home office; their handheld computers send and receive delivery updates and status information via a network server over a wireless phone connection. Doctors can carry lightweight mobile devices so that they have wireless access to patient information at all times.
- Delivering network access to isolated facilities or disaster-stricken areas. For example, the Federal Emergency Management Agency (FEMA) uses battery-powered wireless technologies to install field networks in areas where power and connections might be unavailable.
- Access in environments where layout and settings change constantly. For instance, film studios often include wireless network components on the set

so that information is always available, no matter how the stage configuration changes.

- Improved customer services in busy areas, such as check-in or reception centers. For example, Hertz employees use handheld units to check in returned rental vehicles right in the parking lot.
- Network connectivity in structures, such as historical buildings, where in-wall wiring is impossible to install or prohibitively expensive.
- Home networks where running cables is inconvenient. More people who own multiple computers install inexpensive wireless networks so that family members can share Internet connections and files. Figure 4-19 shows an example of a home wireless network.

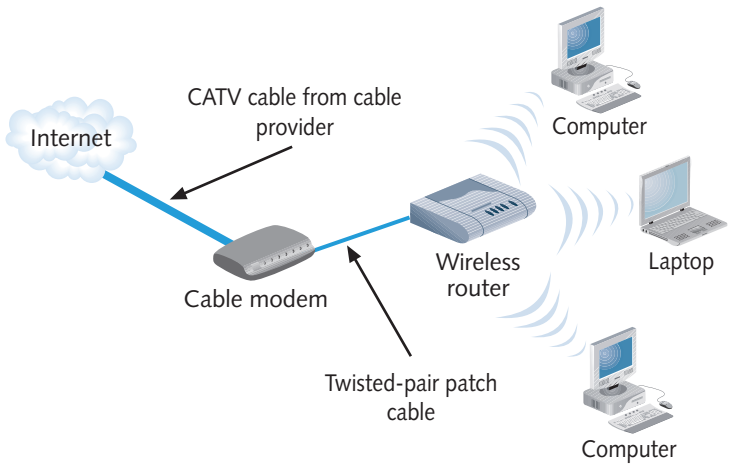


Figure 4-19 A typical home wireless network

Types of Wireless Networks

Depending on the role wireless components play in a network, wireless networks can be subdivided into the following categories:

- *Local area networks (LANs)*—In LANs, wireless components act as part of an ordinary LAN, usually to provide connectivity for mobile users or in changing environments, or perhaps across areas that couldn't otherwise be networked. Examples include older buildings where installing wiring is impractical or areas encompassing public or common property, where cabling might not be permitted.
- *Extended LANs*—In **extended LANs**, an organization might use wireless components to increase a LAN's span beyond normal distance limitations for

wire-based or fiber-optic cables, using a point-to-point arrangement (described in Chapter 3).

- *Internet service*—A company that wants to be a high-speed ISP but doesn't have a media infrastructure available, as cable and phone companies do, can use wireless technologies to bring Internet access to homes and businesses.
- *Mobile computing*—With mobile computing, users communicate by using a wireless networking medium, such as radio or cell phone frequencies, that enable them to move while remaining connected to a network.

Wireless LAN Components

The wireless components of most LANs behave like their wired counterparts, except for the media and related hardware. The operational principles are much the same: Attaching a network interface of some kind to a computer is still necessary, but the interface attaches to an antenna and an emitter rather than to a cable. Users can still access the network as though cable connects them to it.

Another component is required to link wireless users with wired users or resources. At some point on a cabled network, a transmitter/receiver device, called a **transceiver** or an access point (AP), must be installed to translate between wired and wireless networks. This device broadcasts messages in wireless format that must be directed to wireless users and relays messages sent by wireless users to resources or users on the wired side of its connection. An AP includes an antenna and a transmitter to send and receive wireless traffic but also connects to the wired side of the network. This connection enables the device to shuttle traffic back and forth between a network's wired and wireless sides.

Wireless LAN Transmission

All wireless communication depends on sending and receiving signals broadcast through the air to carry information between network devices. These signals take the form of waves in the electromagnetic (EM) spectrum. The frequency of the wave forms used for communication is measured in cycles per second, usually expressed as **hertz (Hz)**. The entire EM spectrum starts with low-frequency waves, such as those used for electrical power (60 Hz in the United States) and telephone (0 to 3 kilohertz [KHz] for traditional voice systems), and goes all the way through the visible light frequencies to the highest frequencies in existence, at which gamma rays and other high-energy particles operate.

In wireless communication, frequency affects the amount and speed of data transmission. The transmission's strength or power determines the distance that broadcast data can travel and still remain intelligible. In general, however, the principles governing wireless transmissions dictate that lower-frequency transmissions can carry less data more slowly over longer distances, and higher-frequency transmissions can carry more data faster over shorter distances.

The middle part of the EM spectrum is commonly divided into several named frequency ranges (bands). The following are the most common frequencies for wireless data communication:

- *Radio*—10 KHz to 300 MHz
- *Microwave*—300 MHz to 300 GHz
- *Infrared*—300 GHz to 400 THz (terahertz)

Note

Wi-Fi networks, as you can see, operate in the microwave category of frequencies.

The important principles to remember about a broadcast medium are the inverse relationship between frequency and distance and the direct relationships among frequency, data transfer rate, and bandwidth. It's also important to understand that higher-frequency technologies often use tight-beam broadcasts and require a clear line of sight between sender and receiver to ensure correct delivery.

Wireless LANs make use of four main technologies for transmitting and receiving data, as discussed in the following sections:

- Infrared
- Laser
- Narrowband (single-frequency) radio
- Spread-spectrum radio

Infrared LAN Technologies

Infrared (IR) wireless networks use infrared light beams to send signals between pairs of devices. These devices typically generate signals strong enough to prevent interference from light sources in most office environments. Infrared works well for LAN applications because of its high bandwidth, which makes 10 to 100 Mbps transmission rates easy to deliver. The four main kinds of infrared LANs include the following:

- Line-of-sight networks require an unobstructed view, or a clear line of sight, between the transmitter and receiver.
- Reflective wireless networks broadcast signals from optical transceivers near devices to a central hub, which then forwards signals to their intended recipients.
- Scatter infrared networks bounce transmissions off walls and ceilings to deliver signals from sender to receiver. TV remotes work in this fashion. This approach limits maximum reception distances to approximately 30 meters (100 feet). Because bounce technologies introduce signal delays, scatter infrared results in lower bandwidth than line of sight.

- Broadband optical telepoint networks provide broadband services. This technology offers high speed and wide bandwidth, can handle high-end multimedia traffic, and matches the capabilities of most wired networks.

IR transmissions are sometimes used for virtual docking connections that enable portable computing devices to communicate with wired computers or peripheral devices, such as printers. Even though infrared offers reasonable networking speeds and convenience, infrared LANs are hampered by the typical 100-foot distance limitation. Because infrared light is close in frequency to visible light (and most visible light sources emit strongly in infrared frequencies), infrared is prone to interference problems from fluorescent and other light sources in most work environments. These devices are often called **IrDA devices**, named after the Infrared Device Association, a trade association for designers and manufacturers of infrared equipment.

Laser-Based LAN Technologies

Laser-based transmissions also require a clear line of sight between sender and receiver. Any solid object or person blocking a beam interrupts data transmissions. To protect people from injury and excess radiation, laser-based LAN devices are subject to many of the same limitations as infrared but aren't as susceptible to interference from visible light sources.

Narrowband Radio LAN Technologies

Narrowband radio (also called "single-frequency radio") LANs use low-powered, two-way radio communication, much like what's used in taxis, police radios, and other private radio systems. The receiver and transmitter must be tuned to the same frequency to handle incoming and outgoing data. Unlike light-based communications, such as infrared or laser, narrowband radio requires no line of sight between sender and receiver, as long as both parties stay within the broadcast range of these devices—typically, a maximum range of approximately 70 meters (230 feet).

In the United States, government agencies, such as the Federal Communications Commission (FCC), regulate nearly all radio frequencies. Organizations that want frequencies for their exclusive use in specific locales must complete a time-consuming, expensive application process before being granted the right to use them. Because of the difficulty in securing exclusive use, the FCC sets aside certain frequencies for unregulated use, such as the ones at which cell phones and remote-control toys operate. As wireless networking and other forms of wireless communication become more popular, crowding of these frequencies could become a problem.

Depending on the frequency, walls or other solid barriers can block signals and prevent transmission and reception. Interference from other radio sources is also possible, particularly if the devices broadcast in the unregulated frequency ranges, as most wireless LAN technologies do. As with any broadcast technology, anyone within range of the network devices could eavesdrop on communications. For narrowband radio technologies, this range is quite short. Table 4-6 summarizes the characteristics of narrowband wireless LAN technologies.

Table 4-6 Narrowband wireless LAN characteristics

Characteristic	Value
Frequency ranges	Unregulated: 902–928 MHz, 2.4 GHz, 5.72–5.85 GHz
Maximum distance	50–70 m (164–230 ft)
Bandwidth	1–10 Mbps
Installation and maintenance	Easy to install and maintain
Interference	Highly susceptible
Cost	Moderate
Security	Highly susceptible to eavesdropping within range

Other single-frequency LAN technologies operate at higher power ratings. Networks of this type can usually transmit as far as the horizon and even farther by using repeater towers or signal-bouncing techniques. This kind of technology is well suited for communicating with mobile users but much more expensive than lower-powered alternatives. In addition, transmission equipment is more expensive and usually requires FCC licensing. Most users of this technology, even in the largest organizations, purchase this service from a communications carrier instead of operating their own facilities.

Lack of security can be a serious concern with this kind of networking technology. Anyone with the correct receiver can eavesdrop on communications, which explains why encryption of traffic is common for networks operating at these frequencies. Table 4-7 summarizes the characteristics of high-powered single-frequency radio networks.

Table 4-7 High-powered single-frequency LAN characteristics

Characteristic	Value
Frequency ranges	Unregulated: 902–928 MHz, 2.4 GHz, 5.72–5.85 GHz
Maximum distance	Line of sight, unless extension technologies are used
Bandwidth	1–10 Mbps
Installation and maintenance	Difficult, highly technical, requires licensing
Interference	Highly susceptible
Cost	Expensive to very expensive
Security	Highly susceptible to eavesdropping

Spread-Spectrum LAN Technologies

Spread-spectrum radio addresses several weaknesses of single-frequency communications, whether high or low power. Instead of using a single frequency, spread-spectrum uses multiple frequencies simultaneously, thereby improving

reliability and reducing susceptibility to interference. Also, using multiple frequencies makes eavesdropping more difficult.

The two main kinds of spread-spectrum communications are frequency hopping and direct-sequence modulation. Frequency hopping switches data between multiple frequencies at regular intervals. The transmitter and receiver must be tightly synchronized to maintain communication. The hardware handles the timing of hops and chooses the next frequency without sending any information about this activity, so eavesdropping is nearly impossible. Because frequency-hopping technologies use only one frequency at a time, however, their effective bandwidth is usually 1 Mbps or lower and seldom exceeds 2 Mbps.

Direct-sequence modulation breaks data into fixed-size segments called "chips" and transmits the data on several different frequencies at the same time. The receiving equipment knows what frequencies to monitor and how to reassemble the arriving chips into the correct sequences of data. It's even possible to transmit dummy data on one or more channels, along with real data on other channels, to make it more difficult for eavesdroppers to re-create the original data. Typically, these networks operate in unregulated frequencies and provide bandwidths from 2 to 6 Mbps, depending on the number of dummy channels used. The original 802.11 and 802.11b specifications use direct sequence spread spectrum (DSSS). Table 4-8 summarizes the characteristics of spread-spectrum LAN technologies.

Note

Orthogonal frequency divisional multiplexing (OFDM) is a spread-spectrum technology used by 802.11g and 802.11n running at 2.4 GHz and by the 802.11a 5 GHz and 802.16 WiMAX standards.

Table 4-8 Spread-spectrum LAN characteristics

Characteristic	Value
Frequency ranges	Unregulated: 902–928 MHz or 2.4 GHz, 5 GHz
Maximum distance	Limited to cell boundaries but often extends over several miles
Bandwidth	1–2 Mbps for frequency hopping, 2–6 Mbps for direct-sequence modulation
Installation and maintenance	Depends on equipment; ranges from easy to difficult
Interference	Moderately resistant
Cost	Inexpensive to moderate
Security	Not very susceptible to eavesdropping

Note

The term "cell boundary," as used in Table 4-8, refers to the service area or the radius of a viable signal produced by a wireless transmitter.

LAN Media Selection Criteria

In LANs and internetworks, there are three main media choices: UTP, fiber optic, and wireless. For UTP, the choices are usually Cat 5e, Cat 6, or Cat 6a for most applications, although you might opt for a shielded version. Fiber-optic cabling is often the top choice for connecting wiring closets and buildings, and possibly in electrically noisy environments and for ultra-high-speed connections to servers. Wireless networks typically supplement a wired network to accommodate mobile users or are used for SOHO networks that don't need the higher bandwidth wired networks can provide. Following is a summary of criteria to explore when you're having difficulty choosing between media types:

- *Bandwidth*—How fast must the network be? Higher bandwidth means more expensive cable and higher installation costs, which usually means fiber-optic cable. If you need a 40 or 100 Gigabit Ethernet network, fiber optic is really your only choice.
- *Budget*—How much money can you spend on cabling? Sometimes budget alone dictates a choice. A typical UTP cable installation costs $100 to $200 per cable run, whereas fiber optic might cost twice this much. Wireless media have no physical installation costs, but you need to install access points and verify connectivity from all locations.
- *Environmental considerations*—How electrically noisy is the deployment environment? How important is data security? Sometimes high-EMI environments or security requirements can dictate cable choices, regardless of other factors. The more weight either factor has, the more likely you are to choose fiber-optic cable (or in lower-bandwidth applications, a secure wireless network).
- *Span*—What kind of distance must the network span? Longer spans might require fiber-optic cabling or wireless technologies used between buildings. Strategic placement of small switches for use with UTP wiring gives UTP surprising reach in many office environments where workers tend to cluster in groups, even if these groups are widely scattered.
- *Existing cable plant*—For a new installation, only the previously listed criteria need to be considered, but for an upgrade, the existing cable plant must be considered. For example, if some existing cable is to remain, is it compatible with the speeds and new equipment that are planned?

Networks combining fiber-optic, UTP, and wireless media have almost become the norm, with fiber-optic cables providing a backbone that ties together clusters of devices networked with UTP cable through switches and wiring centers. With wireless networks, users can stay connected with their Wi-Fi-enabled phones, laptops, and tablets. Table 4-9 condenses the most important information for the cable types covered in this chapter.

Table 4-9 Comparison of LAN media characteristics

Type	Maximum cable length	Bandwidth	Installation	Interference	Cost
UTP	100 m	10–10,000 Mbps	Easy	High	Cheapest
STP	100 m	16–10,000 Mbps	Moderate	Moderate	Moderate
Fiber optic	2–100 km	100 Mbps–10 Gbps	Moderate	None	Most expensive
Wireless	100–300 feet	11–300 Mbps	Easy	Moderate	None for physical media

Chapter Summary

- Wired networking media come in two main categories: copper and fiber optic. Cable characteristics include bandwidth rating, maximum segment length, susceptibility to interference and eavesdropping, and cable grade.
- Twisted-pair cabling comes in shielded or unshielded varieties. Most networks use UTP, but STP can be used in electrically noisy environments. Cat 5e and Cat 6 are the most common cable types in networks today.
- Twisted-pair cabling components consist of connectors, patch cable, jacks, patch panels, and distribution racks. A structured cabling plant consists of work areas, horizontal wiring, telecommunications closets (IDFs), equipment rooms (MDFs), backbone cabling, and entrance facilities.
- Fiber-optic cable uses pulses of light to represent bits and is immune to EMI, RFI, and electronic eavesdropping. Commercial implementations of up to 100 Gbps are in use. Each network connection requires two strands of fiber-optic cable: one for transmitting and one for receiving. Fiber-optic cable comes in single-mode or multimode; single-mode uses lasers and can carry data longer distances, and multimode uses LEDs.
- Wireless networks can be subdivided into LANs, extended LANs, and mobile computing. The components of a wireless LAN are a NIC, an antenna, and a transceiver or an access point. Wireless networks send signals in the form of electromagnetic waves. Different network

types use different frequencies for signal transmission.

- Different technologies are used to transmit and receive data, including infrared, laser, narrowband radio, and spread-spectrum radio. Infrared can deliver speeds up to 100 Mbps and is used in some LAN applications. Laser-based technologies require line of sight between sender and receiver, as does infrared, but laser isn't as susceptible to interference from other light sources. Narrowband radio uses low-powered, two-way radio communication and is highly susceptible to interference. Spread-spectrum LANs are the most common and are used for 802.11 b/g/n Wi-Fi networks.
- Criteria for choosing LAN media include needed bandwidth, budget, environmental factors, the distance the network must span, and the existing cable plant, if any. Networks combining fiber-optic, UTP, and wireless have become the norm.

Key Terms

backbone cabling
cable plant
cable segment
crossover cable
crosstalk
datagrade
demarcation point
differential signal
electromagnetic interference (EMI)
encoding
entrance facility
equipment room
extended LAN
fiber-optic cable
hertz (Hz)
horizontal wiring
infrared (IR)
intermediate distribution frame (IDF)
IrDA devices
main distribution frame (MDF)
MDI crossed (MDI-X) devices
medium dependent interface (MDI) devices
narrowband radio
patch cable
radio frequency interference (RFI)
RJ-45 jack
RJ-45 plug
spread-spectrum radio
straight-through cable
structured cabling
telecommunications closet (TC)
termination
transceiver
twisted-pair (TP) cable
voicegrade
work area

Review Questions

1. Which of the following is a common characteristic of a networking medium? (Choose all that apply.)
   a. Bandwidth rating
   b. Interference susceptibility
   c. Broadband rating
   d. Maximum segment length
2. Which of the following types of fiber-optic connectors provides high density and requires only one connector for two cables?
   a. SC
   b. ST
   c. MT-RJ
   d. RJ-45
3. Which of the following conditions requires cables not to exceed a recommended maximum length?

a. Diminution
b. Capacitance
c. Bandwidth
d. Attenuation

4. Which of the following is the process for representing bit signals on the medium?
a. Encryption
b. Encoding
c. Decryption
d. Decoding

5. What happens to signals as they travel the length of the medium?
a. They decode.
b. They amplify.
c. They attenuate.
d. They implode.

6. Which of the following is UTP susceptible to? (Choose all that apply.)
a. EMI
b. Crosstalk
c. Signal enhancement
d. LEDs

7. The space between a false ceiling and the true ceiling where heating and cooling air circulates is called the _____.
a. Duct-equivalent airspace
b. Conduit
c. Return air
d. Plenum

8. What type of connector is used most commonly with TP network wiring?
a. RJ-11
b. RJ-45
c. BNC
d. MT-RJ

9. You have been hired to install a network at a large government agency that wants to reduce the likelihood of electronic eavesdropping on its network. What type of cable is most resistant to eavesdropping?
a. UTP
b. STP
c. Coaxial
d. Fiber optic

10. Which of the following is a characteristic of unshielded twisted-pair cable? (Choose all that apply.)
a. Consists of four wires
b. Commonly used in physical bus topologies
c. Has a distance limitation of 100 meters
d. Is susceptible to electrical interference

11. Which of the following is a characteristic of fiber-optic cabling? (Choose all that apply.)
a. Can be used in electrically noisy environments
b. Requires only a single strand of fiber for network connections
c. Carries data over longer distances than UTP
d. Has low bandwidth

12. You're preparing to install a conventional Ethernet network in your new office building, but your boss tells you to be ready to handle a switchover to 1 Gbps Ethernet next year. What types of cable could you install? (Choose all that apply.)
a. Cat 5
b. Fiber optic
c. Cat 4
d. Cat 6
e. Coax

13. When two cables run side by side, signals traveling down one wire might interfere with signals traveling on the other wire. What is this phenomenon called?
a. RFI
b. Attenuation
c. Impedance
d. Crosstalk

14. What characteristic of twisted-pair cabling helps mitigate the effects of crosstalk?
    a. Differential signals
    b. Copper conductors
    c. Four pairs of wires
    d. 100-ohm impedance
15. Which cabling category is specified for 25GBaseT and 40GBaseT networks?
    a. Cat 6a
    b. Cat 7
    c. Cat 7a
    d. Cat 8
16. Which of the following is a wiring standard for twisted-pair cable connections? (Choose all that apply.)
    a. IEEE 802.3a
    b. TIA/EIA 568A
    c. IEEE 802.3b
    d. TIA/EIA 568B
17. Which of the following is a component of a structured cabling system? (Choose all that apply.)
    a. Patch cables
    b. RJ-11 plugs
    c. Coax cable
    d. Horizontal wiring
18. Where are you most likely to find backbone cabling? (Choose all that apply.)
    a. MDF
    b. In the work area
    c. Between IDFs
    d. Connecting a work area to an IDF
19. Which of the following is a tool needed to make a patch cable? (Choose all that apply.)
    a. 110 punchdown tool
    b. Cable stripper
    c. Crimping tool
    d. RJ-45 jack
20. Which type of connection is most likely to require a crossover cable?
    a. PC to hub
    b. Hub to router
    c. Router to switch
    d. PC to router
21. Which UTP limitations can be solved by fiber-optic cable? (Choose all that apply.)
    a. Bandwidth
    b. EMI susceptibility
    c. Installation cost
    d. Segment length
22. How many strands of fiber-optic cable are typically used for a network connection?
    a. 1
    b. 2
    c. 4
    d. 8
23. Which statement is true about fiber-optic cables?
    a. MMF uses lasers and has a thicker core.
    b. SMF uses lasers and has a thinner core.
    c. MMF uses LEDs and has a thinner core.
    d. SMF uses LEDs and has a thicker core.
24. When might you want to use a rollover cable?
    a. To connect a PC to another PC
    b. To connect a router to a switch
    c. To add a switch to a LAN
    d. To configure a Cisco device
25. Which of the following wireless technologies does the original 802.11b wireless standard use?
    a. Infrared
    b. Narrowband radio
    c. Frequency hopping
    d. Direct-sequence spread spectrum

Packet Tracer Labs

Packet Tracer Lab 4-1: Using Straight-Through and Crossover Cables

Time Required: 10 minutes

Objective: Use Packet Tracer to connect devices using straight-through cables and crossover cables.

Required Tools and Equipment: A computer with Packet Tracer installed, and Packet Tracer file vlab4-1.pkt, which is available from the Cengage Web site

Description: In this project, you run Packet Tracer to see when to use straight-through cables and crossover cables. Figure 4-20 shows the initial topology for this lab.

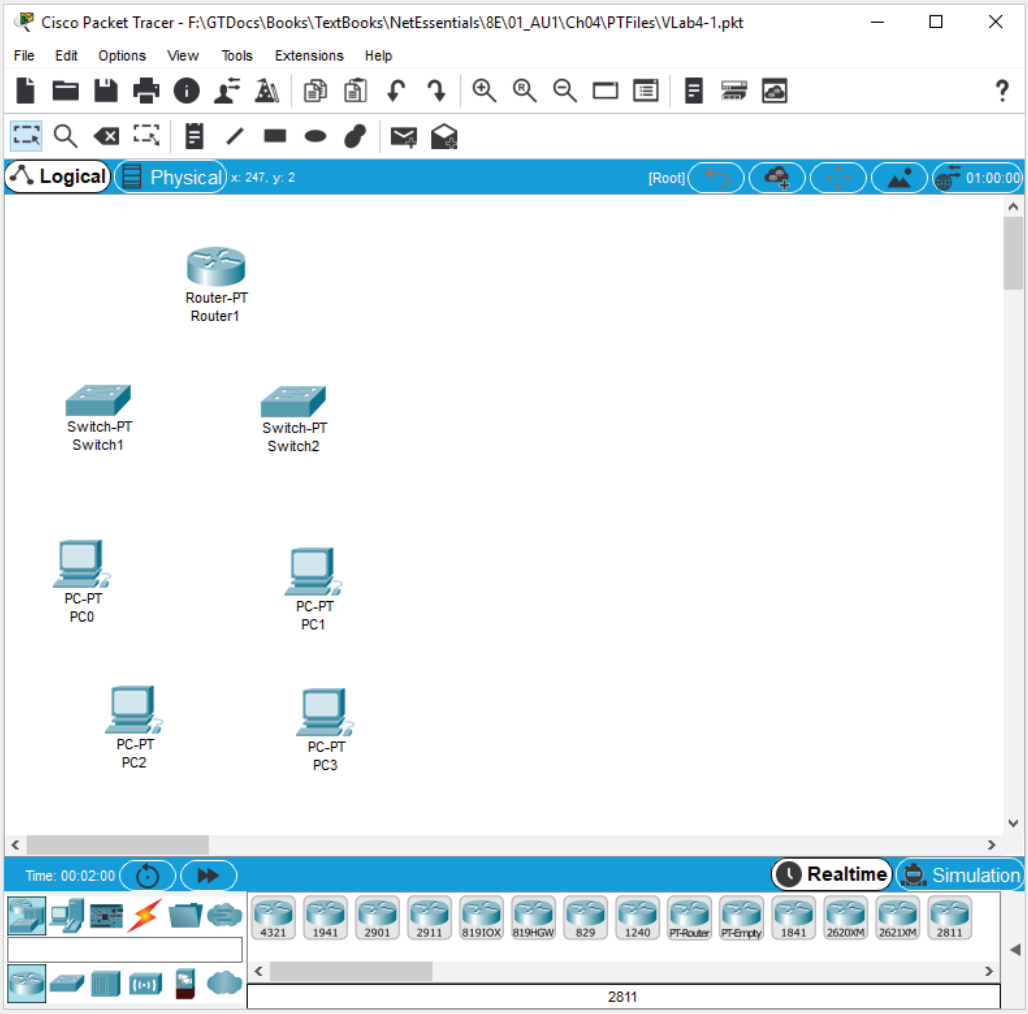


Figure 4-20 Packet Tracer Lab 4-1 topology

Source: Cisco Systems, Inc.

1. Open vlab4-1.pkt in Packet Tracer by double-clicking the file.
2. Click the **Connections** icon in the top row of device types. In the middle pane, click the **Copper Straight-Through** cable.
3. Next, click **Switch1**. You see a list of available ports to which to connect the cable. Select **FastEthernet0/1** from the list. In the same way, click **Router1** and then select **FastEthernet0/0**. After a short time, two green arrows appear on the connection, indicating a good link between the two devices.
4. Next, click the **Copper Cross-Over** cable (the straight dotted line), then click **Switch2** and **FastEthernet0/1**, and then click **Router1** and **FastEthernet1/0**. You see two red arrows on the connection because connecting a switch to a router requires a straight-through cable.
5. Next, click the **Copper Straight-Through** cable, click **Switch1** and **FastEthernet1/1**, and then click **Switch2** and **FastEthernet1/1**. Again, you see two red arrows because connecting two similar devices (in this case, two switches) requires a crossover cable. To delete the connection, click the **Delete** icon, which is the third icon from the left, next to the magnifying glass icon. Then click the cable between the two switches. Press **Esc** or click the **Selection** icon to return to Selection mode.
6. Click the **Copper Cross-Over** cable, click **Switch1** and **FastEthernet1/1**, and then click **Switch2** and **FastEthernet1/1**. After a short wait, you see the two green arrows, indicating a good link.
7. Connect PC0 to Switch1 and PC1 to Switch2 using the copper straight-through cable.
8. Connect PC2 to PC3 using the straight-through cable. Again, the connection doesn't work because similar devices (in this case, two PCs) require a crossover cable. Delete the connection and redo it using the crossover cable. Your topology should look like Figure 4-21.
9. Close Packet Tracer. Click **No** when you are prompted to save your work.

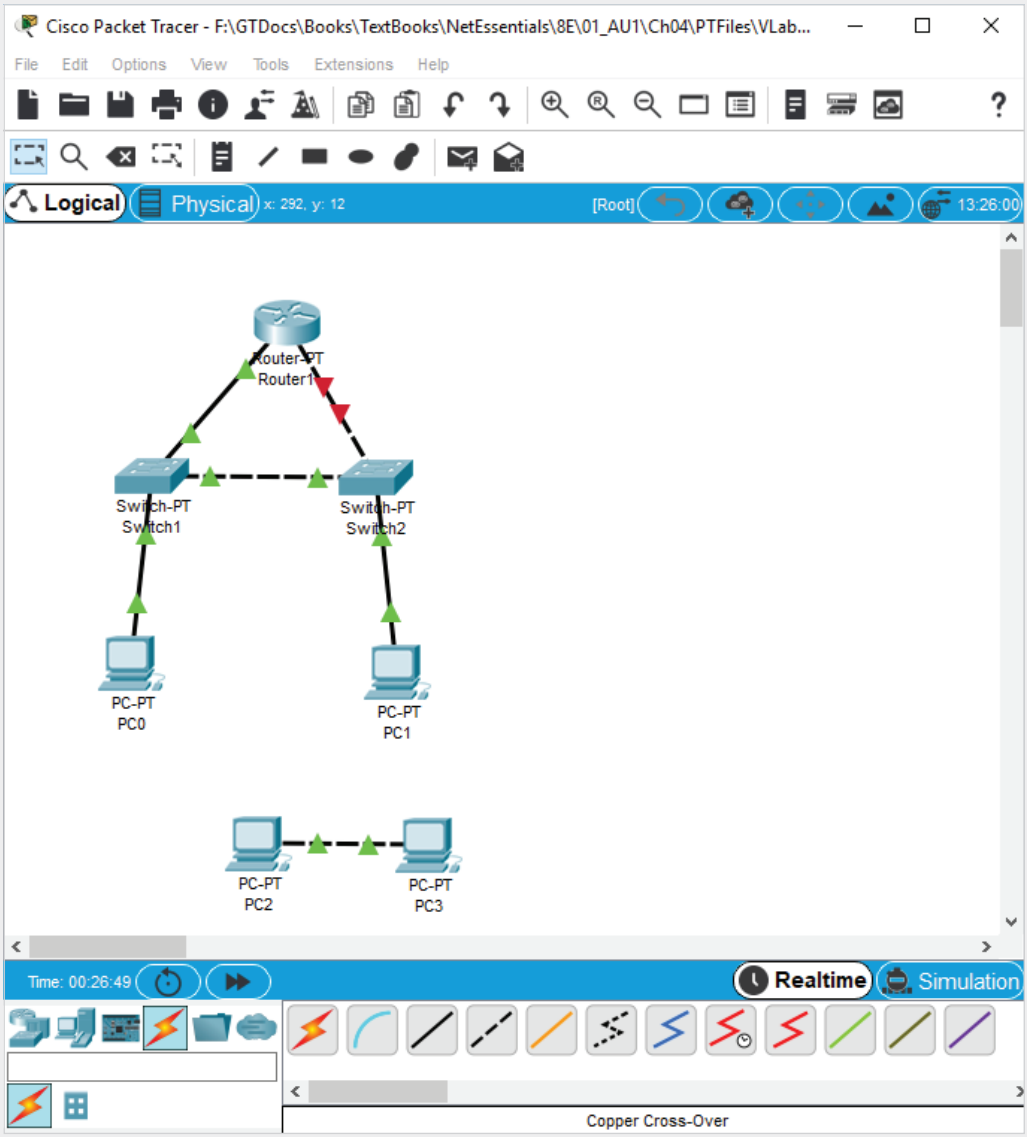


Figure 4-21 The completed topology for Packet Tracer Lab 4-1

Source: Cisco Systems, Inc.

Packet Tracer Lab 4-2: Using Fiber-Optic Cables

Time Required: 10 minutes

Objective: Use Packet Tracer to connect devices using fiber-optic cables.

Required Tools and Equipment: A computer with Packet Tracer installed, and Packet Tracer file vlab4-2.pkt, which is available from the Cengage Web site

Description: In this project, you run Packet Tracer and make device connections using fiber-optic cable.

1. Open vlab4-2.pkt in Packet Tracer by double-clicking the file.
2. Click the **Connections** icon in the top row of device types. In the middle pane, click the **Fiber** cable. (Hover your mouse over the connections to see which one is the fiber cable.)
3. Next, click **Switch1** and **FastEthernet4/1**, and then click **Router1** and **FastEthernet4/0**. Notice how the fiber connections appear to have ports for two cables. That's because most fiber-optic connections require two cables, one for transmit and one for receive.
4. Next, make the connection between Switch2 and the router, using FastEthernet4/1 on Switch2 and FastEthernet5/0 on Router1. Functionally, there's little difference when making the connection between devices using fiber-optic or copper cable. The primary reason you might choose fiber-optic connections is if the environment is electrically noisy or the distance between devices exceeds the limits of copper cable. The topology will look like Figure 4-22.

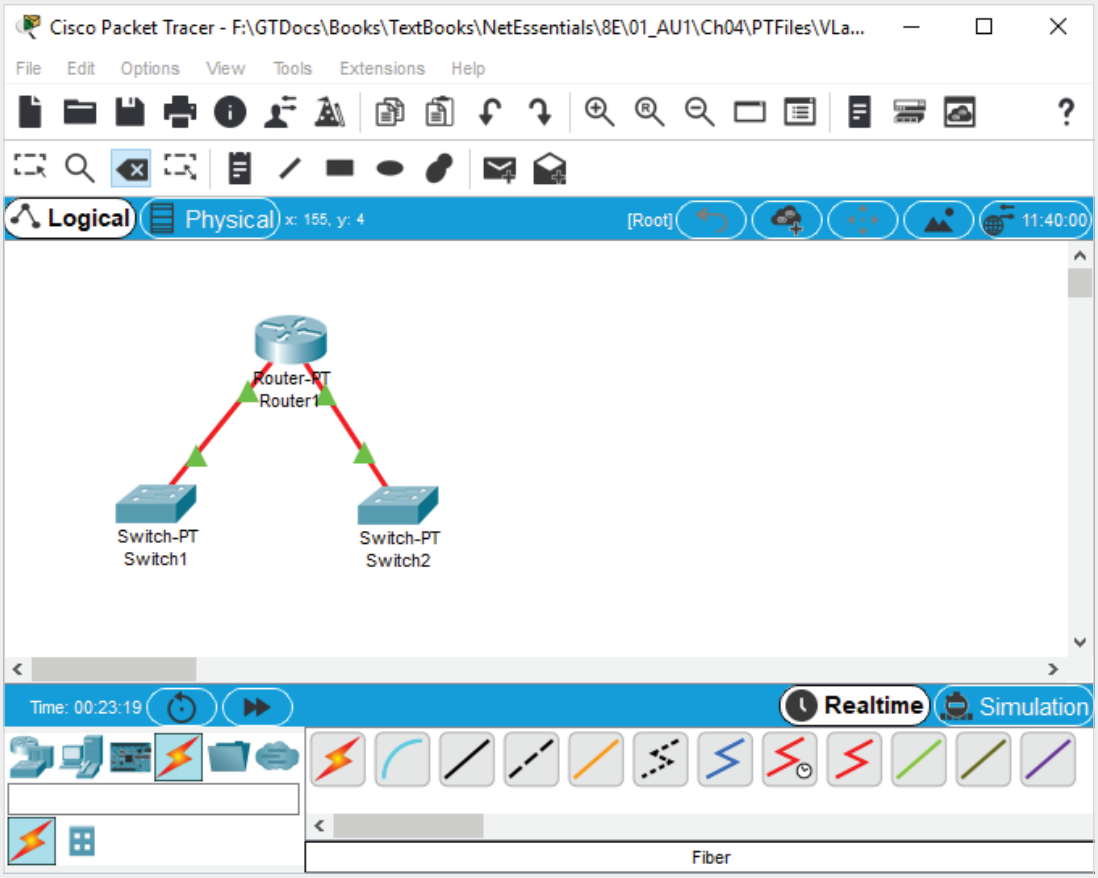


Figure 4-22 The completed topology for Packet Tracer Lab 4-2

Source: Cisco Systems, Inc.

Packet Tracer Lab 4-3: Using a Rollover Cable

Time Required: 10 minutes

Objective: Use Packet Tracer to communicate with a router using a rollover cable.

Required Tools and Equipment: A computer with Packet Tracer installed, and Packet Tracer file vlab4-3.pkt, which is available from the Cengage Web site

Description: In this project, you run Packet Tracer and connect a terminal emulation program on a PC to a router using a rollover cable.

1. Open vlab4-3.pkt in Packet Tracer by double-clicking the file.
2. Click the **Connections** icon in the top row of device types. In the middle pane, click the blue **Console** cable. (In Cisco parlance, a rollover cable is often referred to as a console cable because it is used to connect to the console port on a Cisco router.)
3. Next, click **PC0** and **RS 232**, and then click **Router1** and **Console**. A console cable is not used to transfer network data between devices; it is only used to establish a communication link between a serial port (RS 232) on a PC and the serial console connection on a router so the router can be configured via its command-line interface.
4. Click **PC0** and then click the **Desktop** tab. From the Desktop tab, click **Terminal**. You see the Terminal Configuration window, as shown in Figure 4-23. In this window, you can set various communication parameters depending on what the connection requires. The default selections work for this connection, so just click **OK**.

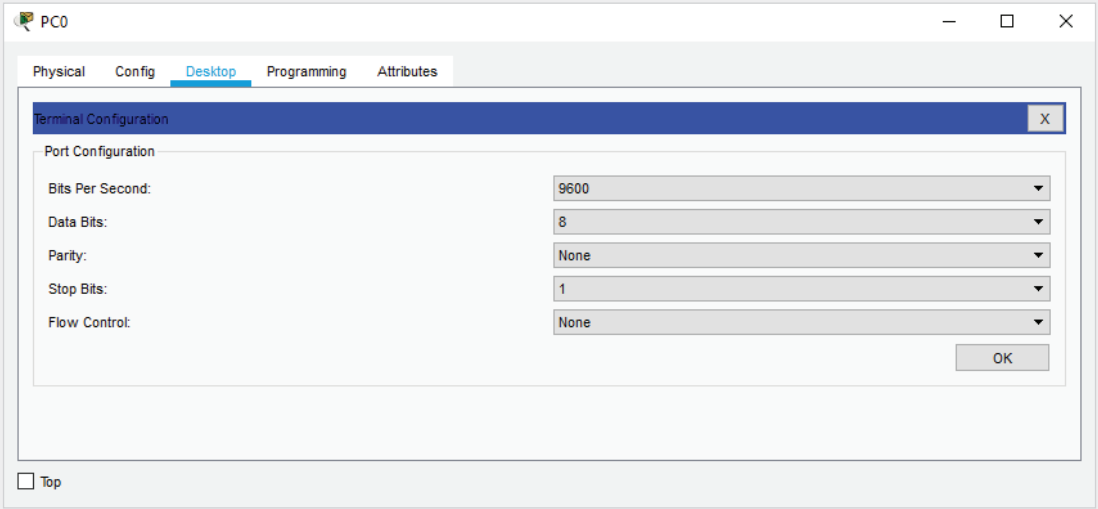


Figure 4-23 The Terminal Configuration window

Source: Cisco Systems, Inc.

5. You can now configure the router with command-line commands. You will learn how to perform this task later in the book. For now, close the PC0 configuration window and close Packet Tracer.

Critical Thinking

The following activities give you critical thinking challenges. Challenge labs give you an opportunity to use the skills you have learned to perform a task without step-by-step instructions. Case projects offer a practical networking setup for which you supply a written solution.

Challenge Lab 4-1: Creating a 1000BaseT Crossover Cable

Time Required: 20 minutes

Objective: Create a 1000BaseT crossover cable.

Required Tools and Equipment: Wire cutter and cable stripper, RJ-45 crimping tool, 2 to 4 feet of Cat 5e or Cat 6 cable, two RJ-45 plugs, and two devices that support 1000BaseT (which can be two PCs with 1000BaseT NICs or two 1000BaseT switches)

Description: In this challenge lab, you create a crossover cable that supports 1000BaseT Ethernet and test it between two devices. Then you verify that the devices connect at 1000BaseT speed.

- How is a 1000BaseT crossover cable different from a 100BaseT crossover cable?

  _____

- How did you verify that the devices connected at 1000BaseT?

  _____

Challenge Lab 4-2: Creating a Rollover Cable

Time Required: 20 minutes

Objective: Create a rollover cable.

Required Tools and Equipment: Wire cutter and cable stripper, RJ-45 crimping tool, 2 to 4 feet of Cat 5e or Cat 6 cable, two RJ-45 plugs, a Cisco-managed device (such as a switch or a router with a console port), a PC with terminal emulation software installed (such as PuTTY), and a DB-9-to-RJ-45 adapter

Description: In this challenge lab, you create a rollover cable, using the DB-9-to-RJ-45 adapter to connect the PC's DB-9 serial port to one end of the rollover cable and the other end to the device's console port. If the PC doesn't have a DB-9 serial port, USB-to-RJ-45 serial port adapters are available. Run PuTTY to connect to the managed switch or router's console. You might need to research the PuTTY settings required to make the connection.

- Why might you need a rollover cable?

  _____

- What's the pinout for a rollover cable?

  _____

Case Project 4-1

During the design of most real-world networks, you'll discover that using more than one type of networking medium is common. The usual reasons for needing more than one type of medium include the following:

- Two or more areas must be interconnected, and the distance separating them is greater than the maximum segment length for the type of medium used in (or best suited for) each area.
- A connection must pass through a high-interference environment (across some large transformers, near heavy-duty electrical motors, and so on). Failure to use a different type of medium increases the risk of impeding data flow. This reason is especially common for choosing fiber-optic cable or wireless in many networks, particularly when connecting floors in an office building and the only available pathway is the elevator shaft.
- Certain parts of an internetwork might have to carry more traffic than other parts. Typically, the segment where traffic aggregates is the backbone, a common cable segment that interconnects subsidiary networks. (Think of a tree trunk as the backbone and its major branches as cable segments.) Often, a higher-capacity cable is used for a backbone (for example, fiber-optic cable or Cat 6 cable rated for Gigabit Ethernet), along with a higher-speed networking technology for attachments to the backbone. This arrangement means outlying segments might use conventional 10 or 100 Mbps Ethernet, and the backbone uses 1 Gbps or 10 Gbps Ethernet.

Using this information, suggest solutions that involve at least two types of networking media, if possible, to address the following problems:

- A—XYZ Corp. is planning a new network. Engineers in the design shop must have connections to accountants and salespeople in the front office, but all routes between the two areas must traverse the shop floor, where arc welders and metal-stamping equipment create potent amounts of EMI and RFI. Given that both the design shop and front office use 10BaseT (twisted-pair Ethernet), how might you interconnect these two areas? What medium guarantees immunity from interference?
- B—After the front-office network at XYZ Corp. is set up, an accountant realizes that if the loading dock connected to the network, dock workers could log incoming and outgoing shipments and keep the inventory more current. Even though the loading dock is nowhere near the shop floor, the dock is 1100 feet from the front office. What kinds of cable will work to make this connection? What kind would you choose and why?
- C—ABC Company occupies three floors in a 10-story building, where the elevator shaft provides the only path to all these floors. In addition, users on the 9th and 10th floors must access a collection of servers on the 8th floor. Explain what kind of connections would work in the elevator shaft. If more than one choice is possible, pick the best option and explain the reasons for your choice. Assuming that interfloor connections might someday need to run at much higher speeds, reevaluate your choice. What's the best type of medium for open-ended bandwidth needs? Explain your answer.

Case Project 4-2

XYZ Corp.'s facilities in Nashua, New Hampshire, are two office buildings 400 feet apart, each with its own LAN. To connect the two networks, you plan to dig a trench and lay cable in conduit between the two buildings. You want to use fiber-optic cable, but your budget-conscious facilities manager wants to use 100 Mbps Ethernet over twisted-pair cable. Which of the following reasons can you use to justify fiber-optic cable in this case, and why?

- a: Twisted pair won't span a 400-foot distance.
- b: Fiber-optic cable is cheaper and easier to work with than twisted pair.
- c: Twisted pair is a conductive cable and can therefore carry current based on the difference in ground potential between the two buildings.
- d: Fiber-optic cable leaves more room for growth and future needs for increased bandwidth than twisted pair does.

Case Project 4-3

TVBCA has just occupied a historic building in downtown Pittsburgh where 15 employees will work. Because of codes for historic buildings, TVBCA isn't permitted to run cables inside walls or ceilings.

Required result: Employees must be able to share files and printers, as in a typical LAN environment, without using cables.

Optional desired results: Employees must be able to use their laptops or tablets and move freely throughout the office while maintaining a network connection. Because of the size of some computer-aided design (CAD) files that employees often use, data transfer speeds should be at least 100 Mbps and the connection should be secure.

Proposed solution: Install an 802.11ac wireless access point and configure each mobile device to connect to the AP with WPA2 encryption. Which of the following results does the proposed solution deliver? Explain your answer.

- a: The proposed solution delivers the required result and both optional desired results.
- b: The proposed solution delivers the required result and only one of the two optional desired results.
- c: The proposed solution delivers the required result but neither optional desired result.
- d: The proposed solution does not deliver the required result.