Communicating Digital Content: Wired and Wireless Networks and Devices

10

iStockphoto.com / cofotoisme

OBJECTIVES

After completing this module, you will be able to:

1. Discuss the purpose of components required for successful communications (sending device, communications device, transmission media, and receiving device) and identify various sending and receiving devices
2. Differentiate among LANs, MANs, WANs, and PANs
3. Differentiate between client/server and peer-to-peer networks
4. Explain the purpose of communications software
5. Describe various network communications standards and protocols: Ethernet, token ring, TCP/IP, Wi-Fi, LTE, Bluetooth, UWB, IrDA, RFID, and NFC
6. Describe various types of communications lines: cable, DSL, ISDN, FTTP, T-carrier, and ATM
7. Describe commonly used communications devices: broadband modems, wireless modems, wireless access points, routers, network cards, and hubs and switches
8. Discuss ways to set up and configure a home network
9. Differentiate among physical transmission media: twisted-pair cable, coaxial cable, and fiber-optic cable
10. Differentiate among wireless transmission media: infrared, broadcast radio, cellular radio, microwaves, and communications satellite

Communications

The process in which two or more computers or devices transfer data, instructions, and information is known as digital communications. Today, even the smallest computers and devices can communicate directly with one another, with hundreds of computers on a corporate network, or with millions of other computers around the globe — often via the Internet.

Figure 10-1 shows a sample communications system. Some communications involve cables and wires; others are sent wirelessly through the air. For successful communications, you need the following:

- A **sending device** that initiates an instruction to transmit data, instructions, or information
- A communications device that connects the sending device to transmission media

Figure 10-1 A simplified example of a communications system. Some devices that serve as sending and receiving devices are (a) servers, (b) desktops, (c) laptops, (d) tablets, (e) smartphones and headsets, (f) portable media players, (g) handheld game devices, and (h) GPS receivers in vehicles. Transmission media consist of phone and power lines, cable television and other underground lines, microwave stations, and satellites.

- **Transmission media**, or a *communications channel*, on which the data, instructions, or information travel
- A communications device that connects the transmission media to a receiving device
- A **receiving device** that accepts the transmission of data, instructions, or information

As shown in Figure 10-1, all types of computers and mobile devices serve as sending and receiving devices in a communications system. This includes servers, desktops, laptops, tablets, smartphones, portable media players, handheld game devices, and GPS receivers. Communications devices, such as modems, wireless access points, and routers, connect transmission media to a sending or receiving device. Transmission media can be wired or wireless.

This module presents types of networks, along with various types of communications lines and devices, and transmission media.

Networks

As discussed in Module 1, a **network** is a collection of computers and devices connected together via communications devices and transmission media. A network can be internal to an organization or span the world by connecting to the Internet. Many home and business users create a network to facilitate communications, share hardware, share data and information, share software, and transfer funds (Figure 10-2):

- **Facilitate communications.** Using a network, people communicate efficiently and easily via email, Internet messaging, chat rooms, blogs, wikis, online social networks, video calls, online meetings, videoconferences, VoIP, text messaging, and more. Some of these communications occur within an internal network. Other times, they occur globally over the Internet.

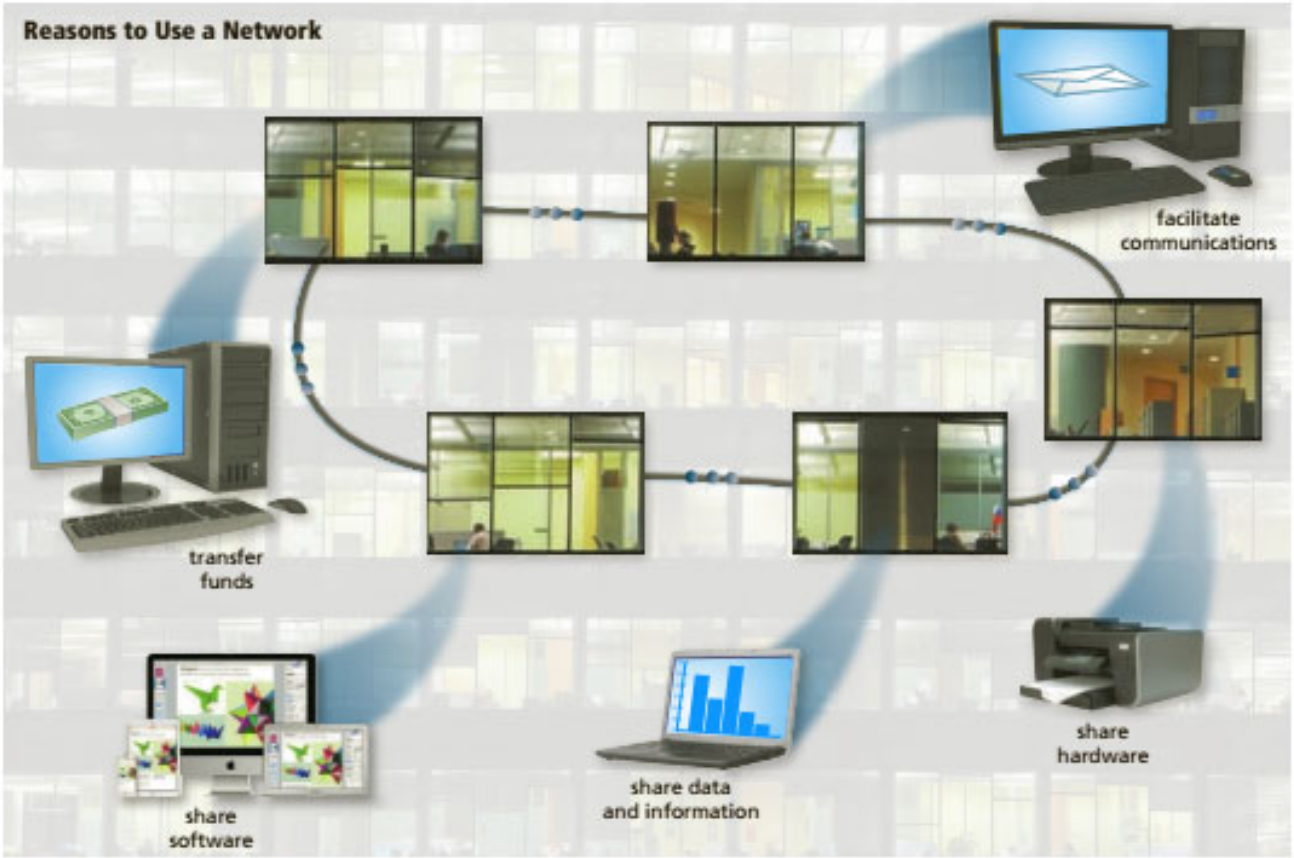


Figure 10-2 Networks facilitate communications; enable sharing of hardware, data and information, and software; and provide a means for transferring funds.

- **Share hardware.** Each computer or device on a network can be provided access to hardware on the network. For example, each computer and mobile device user can access a printer on the network, as they need it. Thus, home and business users create networks to save money on hardware expenses.
- **Share data and information.** Any authorized user can access data and information stored on a network. A large company, for example, might have a database of customer information. Any authorized employee can access the database using a computer or mobile device connected to the network.

  Most businesses use a standard, such as *EDI* (*electronic data interchange*), that defines how business documents travel across transmission media. For example, businesses use EDI to send bids and proposals, place and track orders, and send invoices.
- **Share software.** Users connected to a network can access software on the network. To support multiple users' software access, vendors often sell versions of their software designed to run on a network or as a web app on the Internet. These network and Internet subscription versions usually cost less than buying individual copies of the software for each computer. The license fees for these programs typically are based on the number of users or the number of computers or mobile devices attached to the network.
- **Transfer funds.** *Electronic funds transfer* (*EFT*) allows users connected to a network to exchange money from one account to another via transmission media. Both businesses and consumers use EFT. Examples include wire transfers, use of credit cards and debit cards, direct deposit of funds into bank accounts, online banking, and online bill payment.

BTW

Sharing Network Software

When you use a network to share software, you sometimes have to install the software on your computer, and a server on the network manages the licenses.

Instead of using the Internet or investing in and administering an internal network, some companies hire a value-added network provider for network functions. A *value-added network* (*VAN*) provider is a third-party business that provides networking services such as EDI services, secure data and information transfer, storage, or email. Some VANs, such as PayPal, charge an annual or monthly fee; others charge by the service used.

CONSIDER THIS

What is an intranet?

Recognizing the efficiency and power of the Internet, many organizations apply Internet and web technologies to their internal networks. An *intranet* (intra means within) is an internal network that uses Internet technologies. Intranets generally make company information accessible to employees and facilitate collaboration within an organization. Files on an intranet generally are not accessible from the Internet.

One or more servers on an intranet host an organization's internal webpages, applications, email messages, files, and more. Users locate information, access resources, and update content on an intranet using methods similar to those used on the Internet. A company hosts its intranet on servers different from those used to host its public webpages, apps, and files.

Sometimes a company uses an *extranet* (extra means outside or beyond), which allows customers or suppliers to access part of its intranet. Package shipping companies, for example, allow customers to access their intranet via an extranet to print air bills, schedule pickups, and track shipped packages as the packages travel to their destinations.

LANs, MANs, WANs, and PANs

Networks usually are classified as a local area network, metropolitan area network, wide area network, or personal area network. The main difference among these classifications is their area of coverage.

LAN A **local area network (LAN)** is a network that connects computers and devices in a limited geographical area, such as a home, school, office building (Figure 10-3), or closely positioned group of buildings. Each computer or device on the network, called a *node*, often shares resources, such as printers, large hard drives, and programs. Often, the nodes are connected via cables.

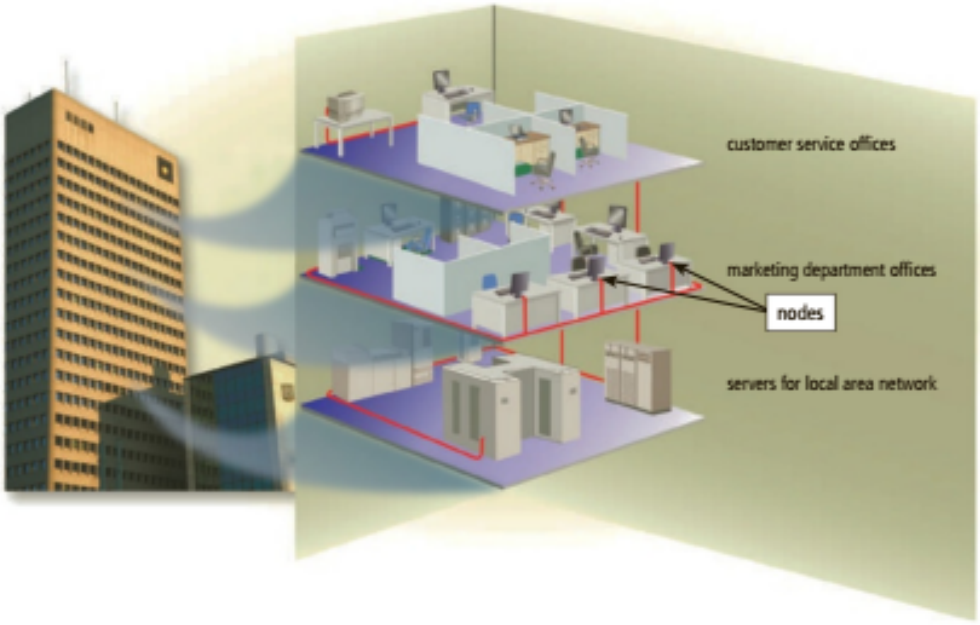


Figure 10-3 Computers and devices on different floors access the same LAN in an office building. Computers and devices on the network often are identified as nodes.
Xtav Photography / Shutterstock.com

A **wireless LAN (WLAN)** is a LAN that uses no physical wires. Computers and devices that access a wireless LAN must have built-in wireless capability or the appropriate wireless network card, USB adapter, or other wireless device. A WLAN may communicate with a wired LAN for access to its resources, such as software, hardware, and the Internet (Figure 10-4).

Figure 10-4 Computers and mobile devices on a WLAN may communicate via a wireless access point with a wired LAN to access its hardware, software, Internet connection, and other resources.
iStockphoto.com / SKrow; Scanrail1 / Shutterstock.com; iStockphoto.com / 123render; iStockphoto.com / pictafolio; iStockphoto.com / Mancherie; Natalia Siverina / Shutterstock.com; Ruslan Kudrin / Shutterstock.com

Figure 10-5 A simplified example of a WAN.

MAN A *metropolitan area network* (*MAN*) is a high-speed network that connects local area networks in a metropolitan area, such as a city or town, and handles the bulk of communications activity across that region. A MAN typically includes one or more LANs, but covers a smaller geographic area than a WAN.

A MAN usually is managed by a consortium of users or by a single network provider that sells the service to the users. Local and state governments, for example, regulate some MANs. Phone companies, cable television providers, and other organizations provide users with connections to the MAN.

WAN A **wide area network (WAN)** is a network that covers a large geographic area (such as a city, country, or the world) using a variety of wired and wireless transmission media (Figure 10-5). A WAN can be one large network or can consist of multiple LANs connected together. The Internet is the world's largest WAN.

PAN A **personal area network (PAN)** is a network that connects computers and devices in an individual's workspace using wired and wireless technology. Devices include smartphones, digital cameras, printers, and more. A PAN may connect devices through a router using network cables or directly using special USB cables. PANs also may use Bluetooth or Wi-Fi technology. A *body area network* (*BAN*), sometimes called a body sensor network (BSN), is a type of PAN that wirelessly connects sensors worn by, carried by, implanted in, or attached to a human body. Read Ethics & Issues 10-1 to consider how BANs are used to monitor medical data.

ETHICS & ISSUES 10-1

Would You Use a BAN to Monitor Medical Data?

By wearing, carrying, implanting, or attaching small devices to a person's body, medical professionals can track vital signs and monitor heart rhythms, breathing rates, and much more via a BAN, which uses low-powered sensors to collect data. The BAN sends the collected data wirelessly to an Internet-connected device, which relays the data to a medical data server. In some cases, the data transmits directly to emergency services. Some devices also automatically can dispense medications based on the data collected.

Because of these devices, a patient may not have to visit a medical facility to receive treatment. Heart patients, diabetics, or those with asthma or other similar conditions can perform regular daily activities while wearing the device. If it collects any unusual data, the patient can receive medical resources immediately. First responders also use these devices. A fire chief, for example, can monitor firefighters' body temperature and oxygen levels as they battle a fire.

The disadvantages of BANs include data validity and security. What happens if a device stops working or its data becomes corrupt? Serious health complications could result if the patient is not monitoring conditions via another technique. For example, devices that administer medication could cause an overdose or underdose if not working properly. Medical data is highly sensitive. An unscrupulous individual could intercept vital signs and other personal data during transfer, violating a patient's confidentiality. Privacy advocates also have concerns about nonmedical uses of BANs. The FCC (Federal Communications Commission) controls the registration of MBANs (medical BANs). The FCC regulates the radio frequency in which an MBAN can transmit data. Some types of MBANs are restricted to be used only within a licensed medical facility.

Consider This: Should insurance companies be required to pay for BANs? Why or why not? Would you use a BAN for a medical condition? Why or why not?

Network Architectures

The configuration of computers, devices, and media on a network is sometimes called the *network architecture*. Two examples of network architectures are client/server or peer-to-peer.

Client/Server On a **client/server network**, one or more computers act as a server, and the other computers on the network request services from the server (Figure 10-6). A **server** controls access to the hardware, software, and other resources on the network and provides a centralized storage area for programs, data, and information. The **clients** are other computers and mobile devices on the network that rely on the server for its resources. For example, a server might store an organization's email messages. Clients on the network, which include any users' connected computers or mobile devices, access email messages on the server. Both wired and wireless networks can be configured as a client/server network.

Although it can connect a smaller number of computers, a client/server network architecture typically provides an efficient means to connect 10 or more computers. Most client/server networks require a person to serve as a network administrator because of the large size of the network.

As discussed in Module 3, some servers are dedicated servers that perform a specific task. For example, a network server manages network traffic (activity), and a web server delivers requested webpages to computers or mobile devices.

Figure 10-6 As illustrated by the communications in this simplified diagram, on a client/server network, one or more computers act as a server, and the client computers and mobile devices access the server(s). Connections can be wired or wireless and may occur through a communications device.

iStockphoto.com / scanrail; iStockphoto.com / SKrow; Scanrail1 / Shutterstock.com; Anan Chincha / Shutterstock.com; iStockphoto.com / luismmolina

Peer-to-Peer A *peer-to-peer (P2P) network* is a simple, inexpensive network architecture that typically connects fewer than 10 computers. Each computer or mobile device, called a *peer*, has equal responsibilities and capabilities, sharing hardware (such as a printer), data, or information with other computers and mobile devices on the peer-to-peer network (Figure 10-7). Peer-to-peer networks allow users to share resources and files located on their computers and to access shared resources found on other computers on the network. Peer-to-peer networks do not have a common file server. Instead, all computers can use any of the resources available on other computers on the network. For example, you might set up a P2P network between an Android tablet and a Windows laptop so that they can share files using Bluetooth or so that you can print from the tablet to a printer accessible to all devices on the network. Both wired and wireless networks can be configured as a peer-to-peer network.

P2P networks are ideal for very small businesses and home users. Some operating systems include a P2P networking tool that allows users to set up a peer-to-peer network. Many businesses also see an advantage to using P2P. That is, companies and employees can exchange files using P2P, freeing the company from maintaining a network server for this purpose. Business-to-business e-commerce websites find that P2P easily allows buyers and sellers to share company information such as product databases.

Figure 10-7 As illustrated by the communications in this simplified diagram, each computer or mobile device on a P2P network shares its hardware and software with other computers and mobile devices on the network. Connections can be wired or wireless and may occur through a communications device.

Alex Staroseltsev / Shutterstock.com; iStockphoto.com / 123render; Sergey Peterman / Shutterstock.com; Scanrail1 / Shutterstock.com; Source: Microsoft

CONSIDER THIS

What is P2P file sharing?

P2P file sharing, sometimes called a *file sharing network*, describes a network configuration on which users access one another's hard drives and exchange files directly via a file sharing program. As more users connect to the network, each user has access to shared files on other users' hard drives. When users sign out of the network, others no longer have access to their hard drives.

Communications Software

Communications software consists of programs and apps that (1) help users establish a connection to another computer, mobile device, or network; (2) manage the transmission of data, instructions, and information; and (3) provide an interface for users to communicate with one another. The first two often are provided by or included as tools with an operating system or bundled with a communications device. The third is provided by applications such as email, FTP, browser, discussion boards, chat rooms, Internet messaging, videoconferencing, and VoIP.

Sometimes, communications devices are preprogrammed to accomplish communications tasks. Some routers, for example, contain firmware for various protocols. Other communications devices require separate communications software to ensure proper transmission of data. Communications software works with the network standards and protocols (presented in a later section) to ensure data moves through the network or the Internet correctly.

Tech Feature 10-1: Mobile Communications

Users often communicate with one another via mobile computers and devices. Read Tech Feature 10-1 to learn about communications options for mobile devices and associated data plans.

TECH FEATURE 10-1

Mobile Communications

After visiting your parents for the weekend, you receive an email message from your mom asking about your trip home. You respond that it was fine and that you were able to send text messages over the Internet to your sister because the bus had a Wi-Fi connection. Meanwhile, your roommate sends you a text message with directions to the restaurant where you are meeting for dinner. That night, you chat on Facebook with a classmate about your homework and catch up on your friends' updates. You see your brother is online and is live streaming from the baseball game he is attending. From email and text messages to voice and video calls, computers and mobile devices offer many ways to communicate.

Email is best for sharing longer, detailed messages. For shorter or time-sensitive messages, consider using the following forms of immediate communications.

Text/Picture/Video Messaging

Text, picture, and video messages often take the place of phone conversations among many people, who find exchanging these messages to be less intrusive and more efficient than voice conversations. SMS (short message service) text messages are messages of 300 or fewer characters sent from one user to another through a mobile service provider's cell phone tower. With MMS (multimedia message service), users also can send and receive photos, videos, and audio files. Occasional users might subscribe to a text-messaging plan, where providers charge a small fee for each message sent or received. In contrast, avid users, who send frequent text, picture, or video messages, might subscribe to an unlimited plan. To avoid paying fees to mobile service providers for sending text messages, some people opt for free messaging apps and services available via third-party providers. These services send messages over the Internet rather than a provider's network. Some of these services are free when both parties subscribe. Free messaging apps often include advertising content alongside the messages.

Internet Messaging

With Internet messaging services, you can send text or media messages in real time to other online users. To access an Internet messaging service, you need the service's desktop, web, or mobile app, and an Internet connection on your computer or mobile device. Users with accounts on multiple Internet messaging services often use an Internet messaging aggregator app to manage contact lists and chat on different Internet messaging networks simultaneously.

Some providers allow you to merge your text/picture/video (SMS and MMS) and Internet messages so that you can see messages of both types from the same contact in a single conversation.

Voice and Video Calling

VoIP services, such as Skype and FaceTime, also provide voice and video calling services over the Internet. These often are much less expensive than making phone calls over a mobile service provider's network. It also is possible to make calls from a VoIP program to a mobile or landline phone. Voice and video calling require large amounts of bandwidth. As a result, some carriers prohibit the use of calling services over their networks, requiring users to connect via Wi-Fi to make these calls. Read Ethics & Issues 10-2 to consider video calling and other issues associated with communications technologies and medical care.

Data Plans

Your mobile device's data plan enables you to access the Internet through your mobile service provider's network when Wi-Fi is not available. Without a data plan, you must use Wi-Fi or a wired connection to access the Internet on your computer or mobile device. Some mobile service providers offer an unlimited data plan for your device, while many offer limited data plans. If you exceed your data limit in a given month, additional fees apply. By monitoring your data usage to see how much you use on average over a few months, you can decide on the best plan for you. Some carriers offer a shared data plan that provides an allotted amount of data to be shared across several smartphones, tablets, laptops, gaming devices, and mobile hot spots. Using Wi-Fi when available to access the Internet will save on data usage charges if you have a limited data plan.

Consider This: Think about how you use different forms of mobile communications to share information or communicate with your family, friends, or coworkers as part of your daily routine. For what purposes do you generally send email messages or text messages? After exchanging text messages, when might you make a phone call or use VoIP service to talk in real time? Under what circumstances is each form of communication most efficient?

ETHICS & ISSUES 10-2

Do the Benefits of Telemedicine Outweigh the Risks?

After your doctor asks you several questions, she gives you a diagnosis and sends a prescription to your local pharmacy electronically. Instead of walking out of the exam room, you turn off your tablet's webcam, receiving medical care without leaving your home. *Telemedicine* is the use of communications and information technology to provide and assist with medical care. Patients use telemedicine to communicate with a doctor, nurse, or pharmacist from their home or workplace. Healthcare professionals benefit from collaborating and consulting with specialized physicians in other locations.

Proponents of telemedicine state that its use can provide healthcare access to patients in remote areas, or those who are unable to leave their home safely. The Mayo Clinic is testing in-office kiosks which enable employees to videoconference with a medical professional to diagnose minor health conditions without the employee having to leave work. Another benefit of telemedicine is in cases where spread of infectious disease is a concern.

Some healthcare experts state that the cost of the equipment and time spent training healthcare professionals outweighs the benefits. The inability of healthcare professionals to perform hands-on tasks, such as take a temperature or examine the patient's ears or throat, can lead to misdiagnosis or an incomplete exam. If a patient requires immediate care, such as for an allergic reaction, a medical professional is not on hand to give treatment, causing delays. Insurance companies may require physicians to have medical licenses in the state where the patient resides in order to cover the expenses. Privacy advocates warn that hackers can access shared data or spy on videoconferences between doctors and patients.

Consider This: Have you ever used telemedicine to communicate with your healthcare provider? Why or why not? Would you use a kiosk at your workplace to communicate with a healthcare provider? Why or why not? Is it practical to rely on telemedicine to provide care to people in remote areas? Why or why not?

Network Communications Standards and Protocols

Today's networks connect terminals, devices, and computers from many different manufacturers across many types of networks. For the different devices on various types of networks to be able to communicate, the network must use similar techniques of moving data through the network from one application to another.

To alleviate the problems of incompatibility and ensure that hardware and software components can be integrated into any network, various organizations such as ANSI (American National Standards Institute) and IEEE (Institute of Electrical and Electronics Engineers) propose, develop, and approve network standards. A *network standard* defines guidelines that specify the way computers access the medium to which they are connected, the type(s) of medium used, the speeds used on different types of networks, and the type(s) of physical cable and/or the wireless technology used. Hardware and software manufacturers design their products to meet the guidelines specified in a particular standard, so that their devices can communicate with the network. A standard that outlines characteristics of how two devices communicate on a network is called a *protocol*. Specifically, a protocol may define data format, coding schemes, error handling, and the sequence in which data transfers over a network.

Table 10-1 identifies some of the more widely used network communications standards and protocols for both wired and wireless networks. The following sections discuss each of these standards and protocols.

Table 10-1 Network Communications Standards and Protocols

Name	Type	Sample Usage
Ethernet	Standard	LAN
Token ring	Standard	LAN
TCP/IP	Protocol	Internet
Wi-Fi	Standard	Hot spots
LTE	Standard	Mobile phones
Bluetooth	Protocol	Wireless headset
UWB	Standard	Inventory tracking
IrDA	Standard	Remote control
RFID	Protocol	Tollbooth
NFC	Protocol	Mobile phone payment

CONSIDER THIS

Do network standards and protocols work together?

Network standards and protocols often work together to move data through a network. Some of these standards define how a network is arranged physically, while others specify how messages travel along a network. Thus, as data moves through a network from one program to another, it may use one or more of these standards.

BTW

Data Transfer Rates

Mbps (megabits per second) is one million bits per second, and *Gbps* (gigabits per second) is one billion bits per second.

Ethernet

Ethernet is a network standard that specifies no central computer or device on the network (nodes) should control when data can be transmitted. That is, each node attempts to transmit data when it determines the network is available to receive communications. If two computers or devices on an Ethernet network attempt to send data at the same time, a collision will occur. When this happens, the computers or devices resend their messages until data transfer is successful.

The Ethernet standard defines guidelines for the physical configuration of a network (e.g., cabling, network devices, and nodes). Ethernet currently is the most popular network standard for LANs because it is relatively inexpensive and easy to install and maintain. Depending on the transmission media used, Ethernet networks have data transfer rates that range from 10 Mbps for home/small office users to 100 Gbps for enterprise users.

Token Ring

The **token ring** standard specifies that computers and devices on the network share or pass a special signal, called a token, in a unidirectional manner and in a preset order. A *token* is a special series of bits that functions like a ticket. The device with the token can transmit data over the network. Only one token exists per network. This ensures that only one computer transmits data at a time. Although token ring is not as widely used today, many networks use the concept of a token.

The token ring standard defines guidelines for the physical configuration of a network (e.g., cabling, network cards, and devices). Some token ring networks connect up to 72 devices. Others use a special type of wiring that allows up to 260 connections. The data transfer rate on a token ring network ranges from 4 Mbps to 16 Mbps.

TCP/IP

Short for Transmission Control Protocol/Internet Protocol, **TCP/IP** is a network protocol that defines how messages (data) are routed from one end of a network to the other. TCP/IP describes rules for dividing messages into small pieces, called *packets*; providing addresses for each packet; checking for and detecting errors; sequencing packets; and regulating the flow of messages along the network.

TCP/IP has been adopted as the network standard for Internet communications. Thus, all hosts on the Internet follow the rules defined in this standard. As shown in Figure 10-8, Internet communications also use other standards, such as the Ethernet standard, as data is routed to its destination.

When a computer sends data over the Internet, the data is divided into packets. Each packet contains the data, as well as the recipient (destination), the origin (sender), and the sequence information used to reassemble the data at the destination. Each packet travels along the fastest individual available path to the recipient's computer or mobile device via routers. This technique of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data is called *packet switching*. Read Secure IT 10-1 for another use of packets.

How Communications Standards Might Work Together

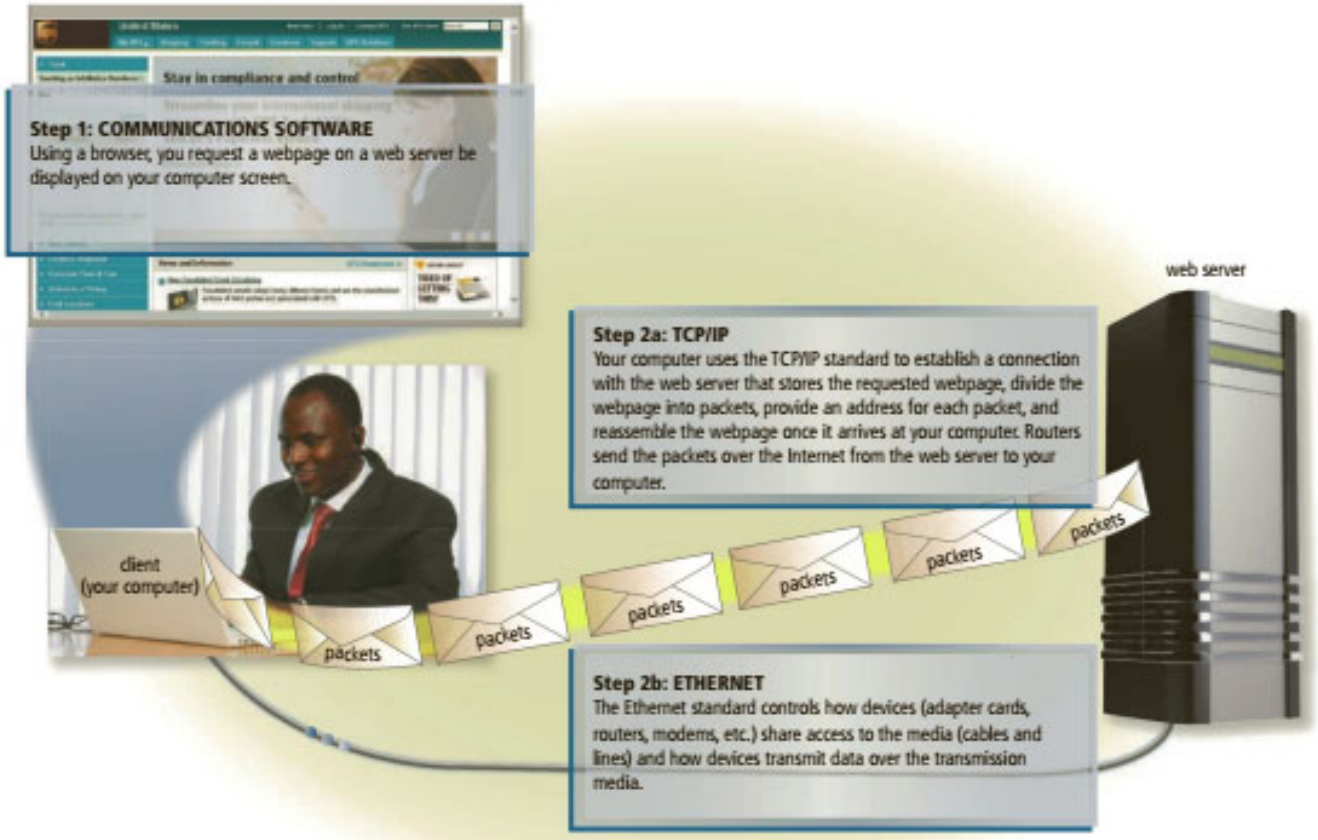


Figure 10-8 This figure illustrates how Internet communications use TCP/IP and Ethernet to ensure that data travels correctly to its destination.

lenetstan / Shutterstock.com; iStockphoto.com / luiammolina

SECURE IT 10-1

Monitoring Network Traffic

Network monitoring software constantly assesses the status of a network and sends an email or text message, usually to the network administrator, when it detects a problem. These messages may state that an outage has occurred, the server's available memory space is near capacity, a new user account has been added, or some other critical event has developed.

Monitoring software can measure the amount of network traffic, graph network usage, determine when a specific program uses the network, and show the bandwidth used by each computer or mobile device. On networks that use the TCP/IP protocol, for example, *packet sniffer software* monitors and logs packet traffic for later analysis. Packet sniffing can detect problems, such as why traffic is flowing slowly.

The software also can play a security role, including identifying unusual or excessive network activity. For example, it can flag a remote computer always connected to the network or someone making repeated attempts to sign in to an account. Hackers use packet sniffer software to hijack a computer, which means they capture a user's packets and then reconstruct the contents of webpages that were visited, obtain user names and passwords, and trace photos and videos viewed.

Consider This: How would you determine if your employer or school has network monitoring software? Would you change your computer activities, including browsing certain websites, if you knew the software could track your computer or mobile device usage?

CONSIDER THIS

Can IP addresses be used to determine a computer or device's location?

In many cases, you can determine a computer or a device's location from its IP address. For example, if an IP address begins with 132.170, a small amount of research will uncover that the University of Central Florida assigns IP addresses beginning with these numbers; however, additional research would be necessary to determine where the computer or mobile device is located on the network. Certain websites allow visitors to find a location by entering an IP address. Some web apps infer your approximate location from your IP address when GPS is not available in order to provide you with local information or nearby search results.

Wi-Fi

Computers and devices that have the appropriate wireless capability can communicate via radio waves with other computers or devices using **Wi-Fi** (wireless fidelity), which identifies any network based on the 802.11 standards. Developed by IEEE, **802.11** is a series of network standards that specifies how two wireless devices communicate over the air with each other. Common standards include 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, and 802.11af, with data transfer rates ranging from 11 Mbps to 7 Gbps. Many devices support multiple standards. For example, a designation of 802.11 ac/b/g/n on a computer, router, or other device indicates it supports those four standards (ac, b, g, and n).

Wi-Fi sometimes is referred to as *wireless Ethernet* because it uses techniques similar to the Ethernet standard to specify how physically to configure a wireless network. Thus, Wi-Fi networks easily can be integrated with wired Ethernet networks. When a Wi-Fi network accesses the Internet, it works in conjunction with the TCP/IP network standard.

One popular use of the Wi-Fi network standard is in hot spots that offer mobile users the ability to connect to the Internet with their Wi-Fi-enabled wireless computers and devices. Many homes and small businesses also use Wi-Fi to network computers and devices wirelessly. In open or outdoor areas free from interference, the computers or devices should be within 300 feet of a wireless access point or hot spot. In closed areas, the wireless network range is about 100 feet. To obtain communications at the maximum distances, you may need to install extra hardware to extend or strengthen a wireless signal.

LTE

LTE (Long Term Evolution) is a network standard that defines how high-speed cellular transmissions use broadcast radio to transmit data for mobile communications. Developed by the Third Generation Partnership Project (3GPP), LTE has the potential of 100 Mbps *downstream rate*

(receiving data) and 30 Mbps *upstream rate* (sending data). Newer specifications are being developed that potentially can support a 1 Gbps downstream rate and a 500 Mbps upstream rate. Based on the TCP/IP network standard, LTE supports data, messaging, voice, and video transmissions. Many mobile service providers, such as AT&T and Verizon Wireless, offer LTE service.

Two competing standards for LTE are WiMax (Worldwide Interoperability for Microwave Access) and UMB (Ultra Mobile Broadband).

Bluetooth/Tech Feature 10-2

Bluetooth is a network protocol that defines how two Bluetooth devices use short-range radio waves to transmit data. The data transfers between devices at a rate of up to 3 Mbps. To communicate with each other, Bluetooth devices often must be within about 33 feet but can be extended to about 325 feet with additional equipment.

A Bluetooth device contains a small chip that allows it to communicate with other Bluetooth devices. For computers and devices that are not Bluetooth-enabled, you can purchase a Bluetooth wireless port adapter that will convert an existing USB port into a Bluetooth port. Most current operating systems have built-in Bluetooth support. When connecting two devices using Bluetooth, the originating device sends a code to the connecting device. The codes must match to establish the connection. Devices that share a Bluetooth connection are said to be paired. Read Tech Feature 10-2 to learn about Bluetooth uses, advantages, and disadvantages.

TECH FEATURE 10-2

Bluetooth Technology

Most mobile devices and computers manufactured today are equipped with Bluetooth capability. One of the earliest and most popular uses of Bluetooth is to connect hands-free headsets to a mobile phone. Bluetooth has many additional uses, and device manufacturers are increasingly including Bluetooth technology.

Uses

You can use Bluetooth-enabled or Bluetooth-enhanced devices in many ways, including the following:

- Connect devices, such as mobile phones, portable media players, or GPS devices, with vehicle stereos, which use the vehicle's speakers to project sound (shown in the figure).
- Use GPS receivers to send directions to a mobile phone or GPS-enabled device.
- Transfer photos wirelessly from a digital camera to a laptop or server.
- Play music on a smartphone through the speakers on a computer or other Bluetooth-enabled device.
- Send signals between video game accessories, video game devices, and a television.
- Establish a PAN (personal area network).
- Allow communications between a computer and devices, such as a keyboard, printer, Smart TV, or mobile phone. Connecting these devices enables you to print documents, share calendar appointments, and more.
- Replace wired communications devices, such as bar code readers, with wireless devices to enhance portability.
- Transmit data from a medical device, such as a blood glucose monitor, to a mobile phone or other device.
- Change the channel, pause a program, or schedule a recording using a Bluetooth-compatible or Bluetooth-enabled television and remote control.
- Track objects that include tags or nodes used to send wireless signals read by a real-time location system.

(*Continued*)

Advantages and Disadvantages

Advantages of using Bluetooth technology include the following:

- If a device has Bluetooth capability, using Bluetooth technology is free.
- Although Bluetooth devices need to be near each other, they do not have to be in the same room, within the same line of sight, or facing each other.
- Bluetooth devices typically require low processing power and use little energy, so using Bluetooth technology will not drain a device's battery.
- Establishing a wireless Bluetooth connection is easy. With most Bluetooth-enabled devices, you simply click a Bluetooth shortcut or icon to enable Bluetooth. Once enabled, the devices usually immediately recognize a connection. (Before initial use, you may need to pair two Bluetooth devices so that they can communicate with each other. Read How To 3-1 in Module 3 for instructions about pairing Bluetooth devices.)
- Bluetooth connections have low security risks. If you want to secure a Bluetooth channel, you would define an identification number for the connection and create a PIN that you can distribute as needed. If the secured computer or device detects an unknown Bluetooth connection, you can choose to accept or reject it. Read Secure IT 10-2 to learn about security risks associated with using Bluetooth technology.
- Bluetooth technology is standardized globally, meaning it can be used to connect devices that are not the same make or model.
- Bluetooth connections have little risk of interference with other wireless networks because the strength of the wireless signals is weak and because of frequency hopping, which changes frequency channels periodically.

One disadvantage of Bluetooth technology is its low bandwidth. Because of its slow data transfer speeds, Bluetooth technology is not an ideal solution for replacing a LAN. Because Bluetooth-enabled mobile payment services are new, security risks may exist. Most agree that the advantages of Bluetooth technology far outweigh the disadvantages.

Consider This: Have you used Bluetooth technology to connect two devices? What devices did you connect, and what was your experience? In your opinion, what is the best reason to use Bluetooth? Why? What devices do you think will include Bluetooth technology in the future?

SECURE IT 10-2

Preventing Bluebugging

One reason why Bluetooth technology is so popular is because connections generally have low security risks, as described in Tech Feature 10-2. Despite this advantage, security experts have seen an increase in *Bluebugging*, which occurs when cyberthieves exploit Bluetooth devices that have been paired. Smartphones and other mobile devices are discoverable to other Bluetooth devices only for a short period when they first are turned on, but during this time the hackers can intercept the signals or use hardware that has the same identifying characteristics as the smartphone or other mobile device. Once hackers have intercepted a device, they take control and read or download personal data, place calls, monitor conversations, review text and email messages, and modify contacts.

Security experts recommend following these practices to prevent Bluebugging:

- Turn off Bluetooth capability if it is not required. Use a Bluetooth earpiece only when you need to be hands free.
- Use your device in a remote area. Bluebuggers often work in crowded and public places, such as shopping centers, parks, and public transportation, and they can intercept signals up to 30 feet away from the device.
- Prevent hackers from intercepting your device by pairing it for the first time in a secure location, such as your home.
- If Bluetooth is required, be certain the device's visibility setting is hidden and all paired devices are set to unauthorized so that the user must authorize each connection request.
- Upgrade your phone. Older devices are more vulnerable to these intrusions.

Consider This: Have you paired your phone with any Bluetooth devices? If so, did you pair them in a private location? Which of these guidelines will you follow to attempt to prevent Bluebugging?

UWB

UWB, which stands for **ultra-wideband**, is a network standard that specifies how two UWB devices use short-range radio waves to communicate at high speeds with each other. At distances of about 33 feet, the data transfer rate is 110 Mbps. At closer distances, such as about 6.5 feet, the transfer rate is at least 480 Mbps. UWB can transmit signals through doors and other obstacles. Because of its high transfer rates, UWB is best suited for transmission of large files, such as video, graphics, and audio. Examples of UWB uses include locating and tracking inventory, equipment, or personnel (especially in remote or dangerous areas).

IrDA

Some devices, such as television remote controls, use the **IrDA** (Infrared Data Association) standard to transmit data wirelessly to each other via infrared (IR) light waves. The devices transfer data at rates from 115 Kbps (thousand bits per second) to 4 Mbps between their IrDA ports. Infrared requires *line-of-sight transmission*; that is, the sending device and the receiving device must be in line with each other so that nothing obstructs the path of the infrared light wave. Because Bluetooth and UWB do not require line-of-sight transmission, these technologies are more widespread than IrDA.

RFID

RFID (*radio frequency identification*) is a protocol that defines how a network uses radio signals to communicate with a tag placed in or attached to an object, an animal, or a person. The tag, called a transponder, consists of an antenna and a memory chip that contains the information to be transmitted via radio waves. Through an antenna, an RFID reader, also called a transceiver, reads the radio signals and transfers the information to a computer or computing device. Read Secure IT 6-2 in Module 6 for uses of animal implants.

Depending on the type of RFID reader, the distance between the tag and the reader ranges from 5 inches to 300 feet or more. Readers can be handheld or embedded in an object, such as a doorway or a tollbooth (Figure 10-9).

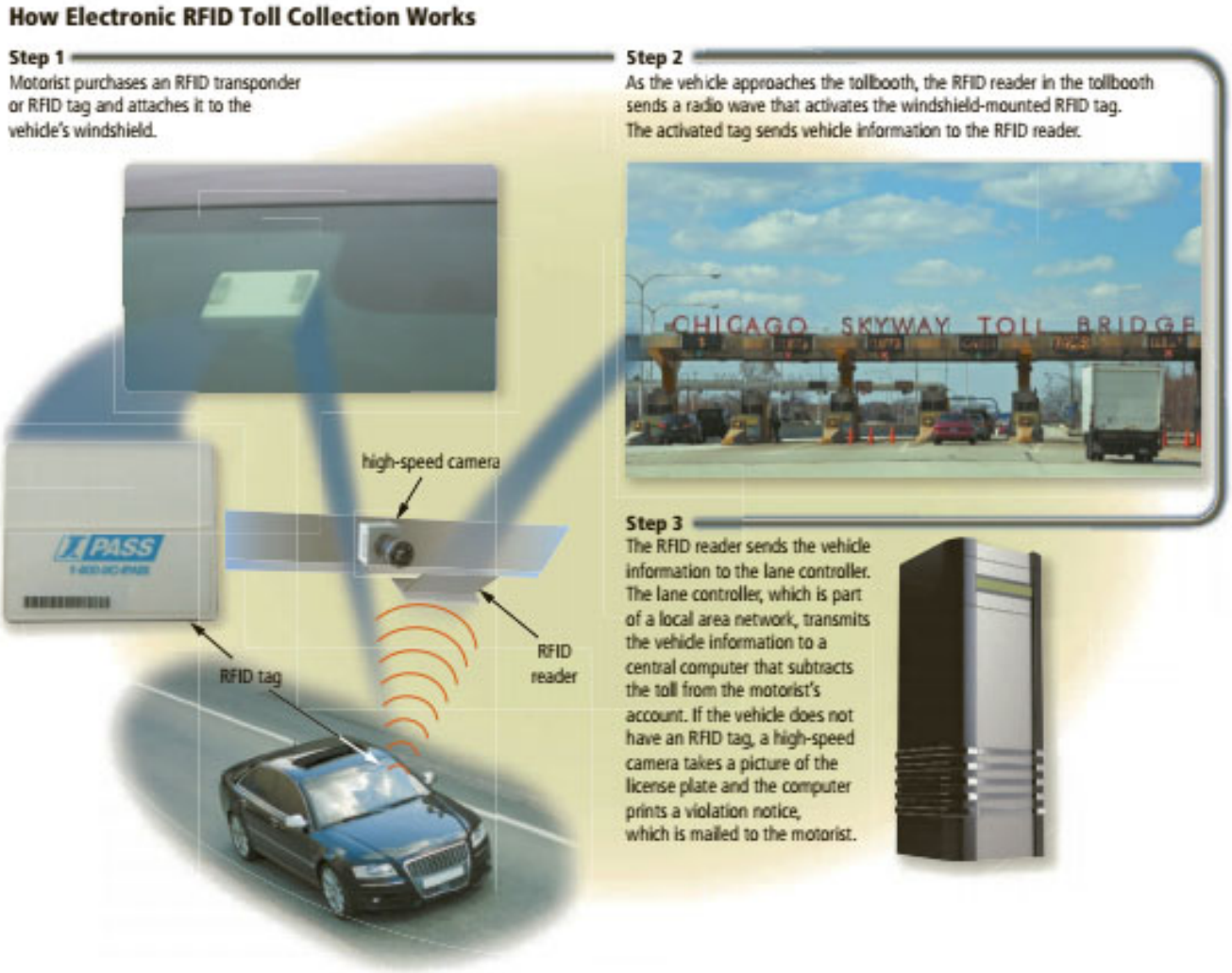


Figure 10-9 This figure shows how electronic RFID toll collection works.

Vibrant Image Studio / Shutterstock.com; iStockphoto.com / luismmolina; Courtesy of Misty Vermaat; Courtesy of Misty Vermaat; iStockphoto.com / benkrut

Figure 10-10 Some objects, such as credit cards, are NFC enabled. You also can program NFC tags yourself.
Alexander Kirch / Shutterstock.com; iStockphoto.com / cheyennecj; iStockphoto.com / pierrephoto

NFC

NFC (*near field communications*) is a protocol, based on RFID, that defines how a network uses close-range radio signals to communicate between two devices or objects equipped with NFC technology (Figure 10-10). Examples of NFC-enabled devices include smartphones, digital cameras, televisions, and terminals. Credit cards, tickets, and NFC tags are examples of objects that also use NFC technology. An NFC tag is a chip that can store small amounts of data. NFC tags are in a variety of objects, such as posters, ski lift tickets, business cards, stickers, and wristbands.

For successful communications, the devices or objects touch or are placed within an inch or two of each other. For example, you can touch two NFC-enabled phones together to transfer contacts, touch an NFC-enabled phone to an NFC tag to display a map, or hold an NFC-enabled phone near a parking meter to pay for parking. Contactless payment, such as the parking meter example, is a popular use of NFC technology. Other uses of NFC technology include sharing contacts or photos, downloading apps, and gaining access or admittance.

CONSIDER THIS

Can you buy a blank NFC tag?

Yes. Consumers can purchase blank NFC tags (shown in the bottom photo in Figure 10-10) at a reasonable cost and easily program them to perform certain actions. For example, you can use a mobile app to program an NFC tag to contain your home network user name and password. Visitors to your home can touch their phones to the NFC tag to access your home network without entering the user name and password.

Communications Lines

A **dedicated line** is a type of always-on physical connection that is established between two communications devices. Businesses often use dedicated lines to connect geographically distant offices. Dedicated lines can be either analog or digital. Digital lines increasingly are connecting home and business users to networks around the globe because they transmit data and information at faster rates than analog lines.

Digital dedicated lines include cable television lines, DSL, ISDN lines, FTTP, T-carrier lines, and ATM. Table 10-2 shows speeds of various dedicated digital lines.

Table 10-2 Speeds of Various Dedicated Digital Lines

Type of Line	Transfer Rates
Cable	256 Kbps to 100 Mbps or higher
DSL	256 Kbps to 8.45 Mbps
FTTP	5 Mbps to 300 Mbps
Fractional T1	128 Kbps to 768 Kbps
T1	1.544 Mbps
T3	44.736 Mbps
ATM	155 Mbps to 622 Mbps, can reach 10 Gbps

Cable

The cable television (CATV) network provides high-speed Internet connections, called *cable Internet service*. The CATV signal enters a building through a single line, usually a coaxial cable. This cable connects to a modem (discussed in the next section), which typically attaches to your computer via an Ethernet cable. Home and small business users often subscribe to cable Internet service.

DSL

DSL (*Digital Subscriber Line*) transmits on existing standard copper phone wiring. Some DSL installations include a dial tone, providing users with both voice and data communications. These DSL installations often require that filters be installed to reduce noise interference when voice communications share the same line. DSL is a popular digital line alternative for the small business or home user.

ADSL is a popular type of DSL. As shown in Figure 10-11, *ADSL* (*asymmetric digital subscriber line*) is a type of DSL that supports faster downstream rates than upstream rates. ADSL is ideal for Internet access because most users download more information from the Internet than they upload.

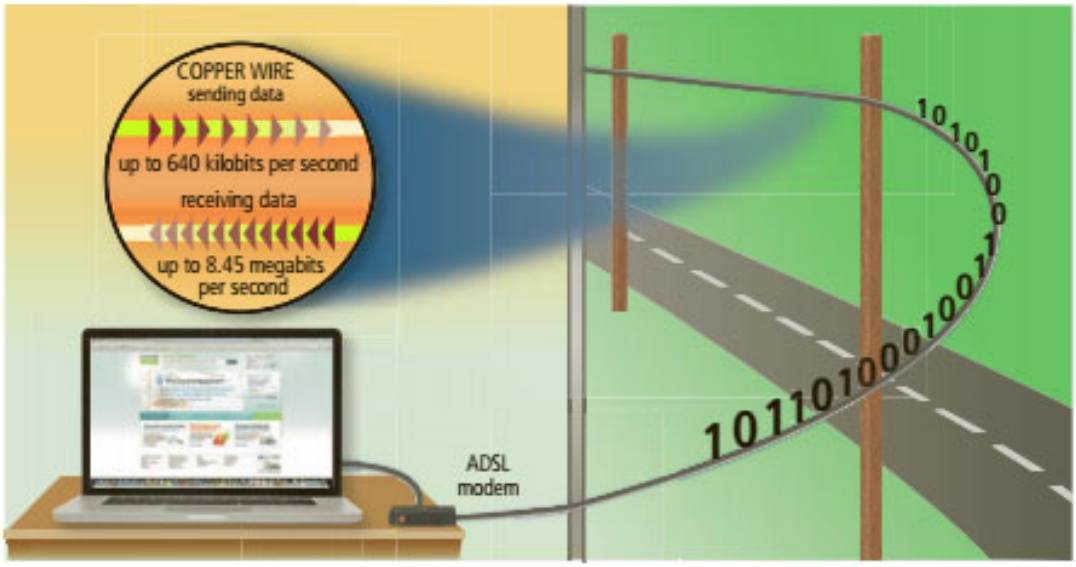


Figure 10-11 ADSL connections transmit data downstream (receiving) at a much faster rate than upstream (sending).
artjazz / Shutterstock.com

CONSIDER THIS

Which is a better choice, DSL or cable Internet service?
Each has its own advantages. DSL uses a line that is not shared with other users in the neighborhood. With cable Internet service, by contrast, users might share the node with up to hundreds of other cable Internet users. Simultaneous access by many users can cause the cable Internet service to slow down. Cable Internet service, however, has widespread availability and usually has faster transmission rates.

FTTP

FTTP, which stands for **Fiber to the Premises**, uses fiber-optic cable to provide extremely high-speed Internet access to a user's physical permanent location.

- *FTTH* (*Fiber to the Home*) provides home users with Internet access via fiber-optic cable.
- *FTTB* (*Fiber to the Building*) refers to small businesses that use fiber-optic cables to access the Internet.

With FTTP service, an optical terminal at your location receives the signals and transfers them to a router connected to a computer. As the cost of installing fiber decreases, more homes and businesses are expected to choose FTTP.

T-Carrier

A **T-carrier line** is any of several types of long-distance digital phone lines that carry multiple signals over a single communications line. Whereas a standard phone line carries only one signal, digital T-carrier lines use multiplexing so that multiple signals share the line. T-carrier lines provide very fast data transfer rates. Only medium to large companies usually can afford the investment in T-carrier lines because these lines are so expensive.

The most popular T-carrier line is the *T1 line*. Businesses often use T1 lines to connect to the Internet. Home and small business users purchase *fractional T1*, in which they share a connection to the T1 line with other users. Fractional T1 is slower than a dedicated T1 line, but it also is less expensive. Users who do not have other high-speed Internet access in their areas can opt for fractional T1. With fractional T1 lines, the data transfer rates become slower as additional users are added.

A *T3 line* is equal in speed to 28 T1 lines. T3 lines are quite expensive. Main users of T3 lines include large corporations, phone companies, and ISPs connecting to the Internet backbone. The Internet backbone itself also uses T3 lines.

ATM

ATM (Asynchronous Transfer Mode) is a service that carries voice, data, video, and media at very high speeds. Phone networks, the Internet, and other networks with large amounts of traffic use ATM. Some experts predict that ATM eventually will become the Internet standard for data transmission, replacing T3 lines.

BTW

Transmission Media

Computers process data as digital signals. Data, instructions, and information travel along transmission media in either analog or digital form, depending on the transmission media.

Communications Devices

A **communications device** is any type of hardware capable of transmitting data, instructions, and information between a sending device and a receiving device. At the sending end, a communications device sends the data, instructions, or information from the sending device to transmission media. At the receiving end, a communications device receives the signals from the transmission media.

The following pages describe a variety of communications devices: modems, wireless access points, routers, network cards, and hubs and switches.

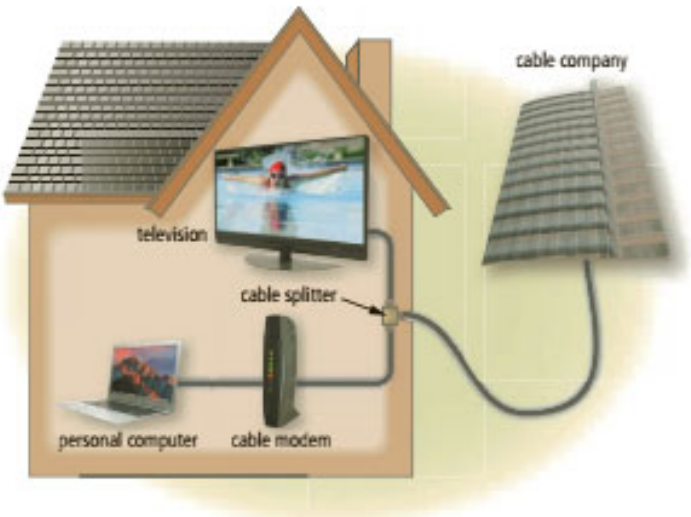


Figure 10-12 A typical cable modem installation.

bridgit / iStockphoto.com; image100 / Alamy Stock Photo; iStockphoto.com / SKrow; Pablo Eder / Shutterstock.com

Digital Modems: Cable, DSL, and ISDN

A *broadband modem*, also called a *digital modem*, is a communications device that sends and receives data and information to and from a digital line. Three types of broadband modems are cable modems, DSL modems, and ISDN modems. These modems typically include built-in Wi-Fi connectivity.

A **cable modem** is a broadband modem that sends and receives digital data over the CATV network. To access the Internet using the CATV service, as shown in Figure 10-12, the CATV provider installs a splitter inside your house. From the splitter, one part of the cable runs to your televisions and the other part connects to the cable modem. Many CATV providers include a cable modem as part of the installation; some offer a rental plan, and others require that you purchase one separately. A cable modem usually is an external device, in which one end of a cable connects to a CATV wall outlet and the other end plugs in a port on a computer.

A **DSL modem** is a broadband modem that sends digital data and information from a computer to a DSL line and receives digital data and information from a DSL line. Similarly, an *ISDN* (Integrated Services Digital Network) *modem* is a broadband modem that sends digital data and information from a computer to an ISDN line and receives digital data and information from an ISDN line. DSL and ISDN modems usually are external devices, in which one end connects to the phone line and the other end connects to a port on the computer.

BTW
Cable and DSL
Cable and DSL are more widely used than ISDN.

CONSIDER THIS

What are dial-up modems?

A *dial-up modem* is a communications device that converts digital signals to analog signals and analog signals to digital signals, so that data can travel along an analog phone line. For example, a dial-up modem connected to a sending computer converts the computer's digital signals into analog signals. The analog signals then can travel over a standard phone line. A dial-up modem connected to a receiving computer converts the analog signals from a standard phone line into digital signals that the computer can process.

A dial-up connection must be reestablished each time the modem is used. With transfer rates of only up to 56 Kbps, dial-up connections also are much slower than broadband connections. For these reasons, dial-up connections are used only in remote areas or where high-speed or wireless options are not available.

Wireless Modems

Some mobile users have a *wireless modem* that uses a mobile service provider's network to connect to the Internet wirelessly from a computer or mobile device (Figure 10-13). Wireless modems, which have an external or built-in antenna, are available as USB adapters and other devices.

Figure 10-13 Wireless modems allow users to access the Internet wirelessly using a mobile service provider's network. Some manufacturers refer to the type of wireless modem shown in this figure as a USB modem.
iStockphoto.com / nelinitpictures

Some smartphones also can function as a wireless modem, called a *mobile hot spot*, when tethered to a personal computer or mobile device. Read How To 10-1 for instructions about using your phone as a mobile hot spot.

HOW TO 10-1

Use Your Phone as a Mobile Hot Spot

If you are in a location without a wireless Internet connection, you may be able to access the Internet from your desktop or mobile computer if you enable your smartphone as a mobile hot spot. When you enable a phone as a mobile hot spot, the phone acts as a wireless access point. You then can connect (tether) your desktop or mobile computer to the phone and utilize the data plan on your phone to access the Internet. If you have a limited data plan with your mobile service provider, you should be careful not to use your phone as a hot spot too often. While the speed from a mobile hot spot might not be as fast as your home or office network, it should be more than sufficient for performing tasks such as browsing the web or sending and receiving email messages that contain mostly text.

The next steps describe how to use your phone as a mobile hot spot:

1. Contact your mobile service provider and determine whether your plan allows for your phone to be used as a mobile hot spot. Using your phone as a mobile hot spot may carry an additional monthly charge.
2. Determine whether your phone has built-in functionality to be used as a mobile hot spot. If not and if supported by your service plan, you may be able to download a separate app that allows your phone to function as a mobile hot spot.
3. Access your phone's settings and enable the mobile hot spot. Your phone should display the SSID and password to access the hot spot. Read How To 5-2 in Module 5 for additional information about SSIDs.
4. Connect to the mobile hot spot on a computer or mobile device using the SSID and password displayed in the previous step.
5. When you are finished using the hot spot, disconnect from the wireless network on your computer and disable the hot spot feature on your phone.

Consider This: How can you determine how much data you are using on your smartphone's data plan?

Peter Bernik / Shutterstock.com

Figure 10-14 Wireless access point.
iStockphoto.com / waturlan

Wireless Access Points

A *wireless access point* (WAP) is a central communications device that allows computers and devices to transfer data wirelessly among themselves or to a wired network using wireless technologies, such as Wi-Fi (Figure 10-14). Wireless access points have high-quality internal or external antennas for optimal signals. For the best signal, some manufacturers suggest positioning the wireless access point at the highest possible location and using a device to strengthen your wireless signal. Read How To 10-2 for tips to strengthen your wireless signal. A wireless access point either connects to a router via an Ethernet or other cable or is part of a router.

HOW TO 10-2

Strengthen Your Wireless Signal

If you reside in a large apartment or house and use a wireless network, you may find that you either experience poor network performance or you are unable to access the network in certain locations. These problems may be related to a weak wireless signal in your home. Various options are available to strengthen a wireless signal to increase network performance and ensure you have a wireless connection throughout your home. The following points describe how to strengthen a wireless signal:

- If your wireless router or wireless access point has an antenna(s), make sure the antenna(s) is extended completely.
- If you are able to remove the antenna(s) from your wireless router or wireless access point, consider replacing it with a wireless signal booster. Check your device's and the wireless signal booster's documentation to determine whether it will work with your device.
- If possible, position the wireless router or wireless access point in a central location of your home and away from appliances or other electronic devices that may degrade the signal.
- Purchase a range extender for your wireless router or wireless access point. Some range extenders are compatible only with specific wireless routers or wireless access points, and others are universal. Make sure the range extender you purchase is compatible with your device. Once installed, follow the range extender's instructions to enable it on your network.
- If you still experience problems with the strength of your wireless signal after following the suggestions above, consider replacing your wireless router or wireless access point with a newer model.

Consider This: What problems may arise if your wireless network's range extends beyond the confines of your home? How can you determine the range of your wireless network?

Routers

A *router* is a communications device that connects multiple computers or other routers together and transmits data to its correct destination on a network. A router can be used on a network of any size. On the largest scale, routers along the Internet backbone forward data packets to their destination using the fastest available path. For smaller business and home networks, a router allows multiple computers and mobile devices to share a single broadband Internet connection, such as through a cable modem or DSL modem (Figure 10-15).

If the network has a separate router, it connects to the router via a cable. Similarly, if the network has a separate wireless access point, it connects to the router via a cable. Many users, however, opt for routers that provide additional functionality:

- A *wireless router* is a device that performs the functions of a router and also a wireless access point.
- A *broadband router* is a device that performs the functions of a router and also a broadband modem.

Figure 10-15 Through a router, home and small business networks can share access to a broadband Internet connection, such as through a cable or DSL modem.

Copyright 2013 NETGEAR; iStockphoto.com / SKrow; iStockphoto.com / Dane Wirtzfeld / Elenium; Kitch Bain / Shutterstock.com; Scanrail1 / Shutterstock.com; Pablo Eder / Shutterstock.com; 112508601 / Shutterstock.com

BTW
Hardware Firewall
To prevent unauthorized users from accessing files and computers, many routers are protected by a built-in firewall, called a *hardware firewall*. Some also have built-in antivirus protection.

- A *broadband wireless router* is a device that performs the functions of a router, a wireless access point, and a cable or DSL modem.
- A *mobile broadband wireless router* is a device that performs the functions of a router, a wireless access point, and a wireless modem (Figure 10-16). Consumers use mobile broadband wireless routers to create a mobile hot spot.

These combination devices eliminate the need for a separate wireless access point and/or modem on a network. These routers also enable you easily to configure and secure the device against unauthorized access.

CONSIDER THIS

How many connections can a router support?
Although a router may be able to connect more than 200 wired and/or wireless computers and mobile devices, the performance of the router may decline as you add connections. Some mobile service providers limit the number of connections to their mobile broadband wireless routers.

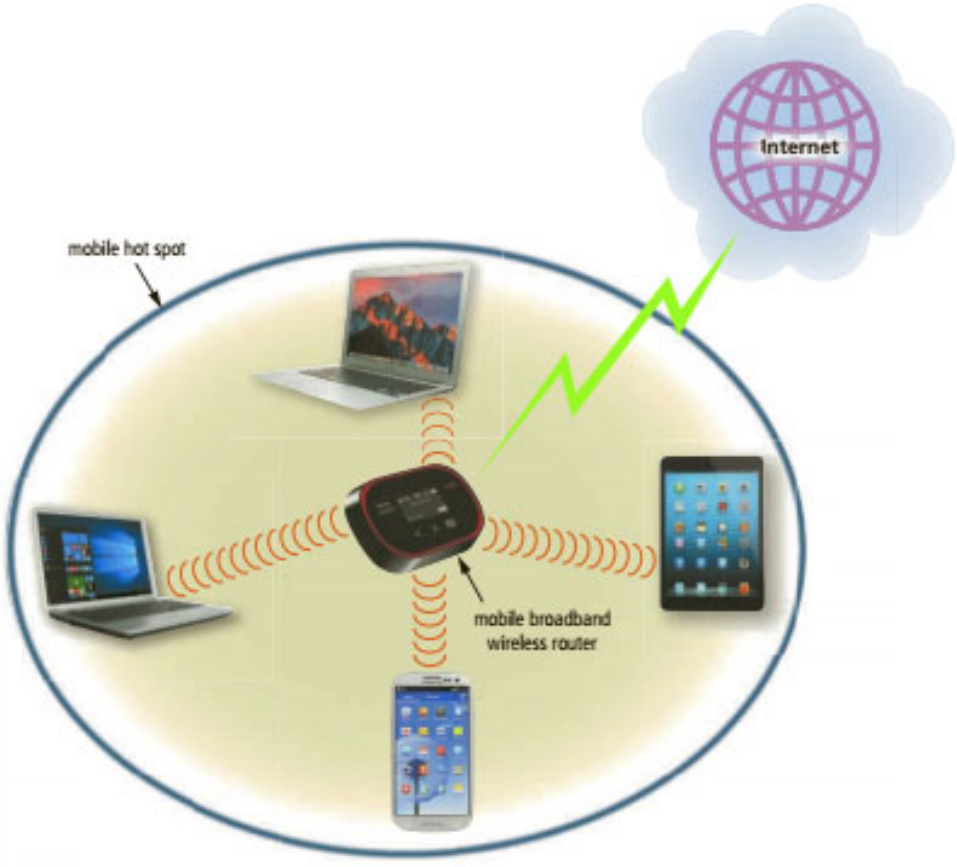


Figure 10-16 Through a mobile broadband wireless router, users can create a mobile hot spot via 3G or 4G mobile broadband Internet service.
Courtesy of Verizon Wireless; iStockphoto.com / SKrow; iStockphoto.com / Dane Wirtzfeld / Elenium; iStockphoto.com / Moncherie; Alex Staroseltsev / Shutterstock.com

BTW
Motherboards
Many computers and mobile devices have motherboards that integrate networking capability, eliminating the need for a separate network card.

Network Cards

A *network card*, sometimes called a *network interface card* (*NIC* pronounced nick), is a communications device that enables a computer or device that does not have built-in networking capability to access a network. The network card coordinates the transmission and receipt of data, instructions, and information to and from the computer or device containing the network card.

Network cards are available in a variety of styles. A network card for a desktop is an adapter card that has a port to which a cable connects (Figure 10-17). A network card for mobile computers and devices is in the form of a USB adapter or other device. A network card follows the guidelines of a particular network communications standard, such as Ethernet or token ring.

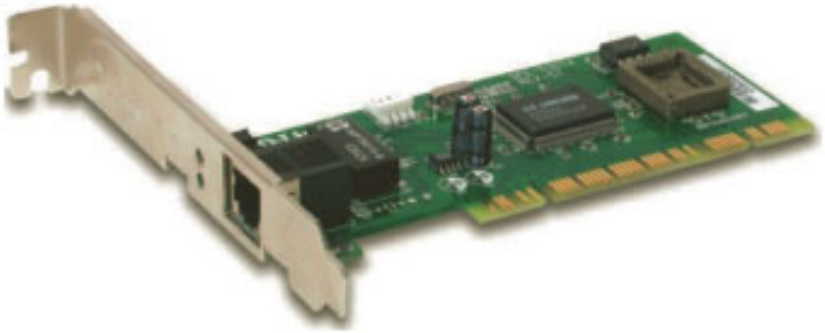


Figure 10-17 Network card for a desktop computer.
Courtesy of D-Link Corporation

Hubs and Switches

Today, thousands of computer networks exist, ranging from small networks operated by home users to global networks operated by widespread telecommunications firms. Interconnecting these many types of networks requires various types of communications devices. A *hub* or *switch* is a device that provides a central point for cables in a network (Figure 10-18). Larger networks typically use a hub, while smaller networks use a switch. Some hubs and/or switches include routers. That is, the hub or switch receives data from many directions and then forwards it to one or more destinations.

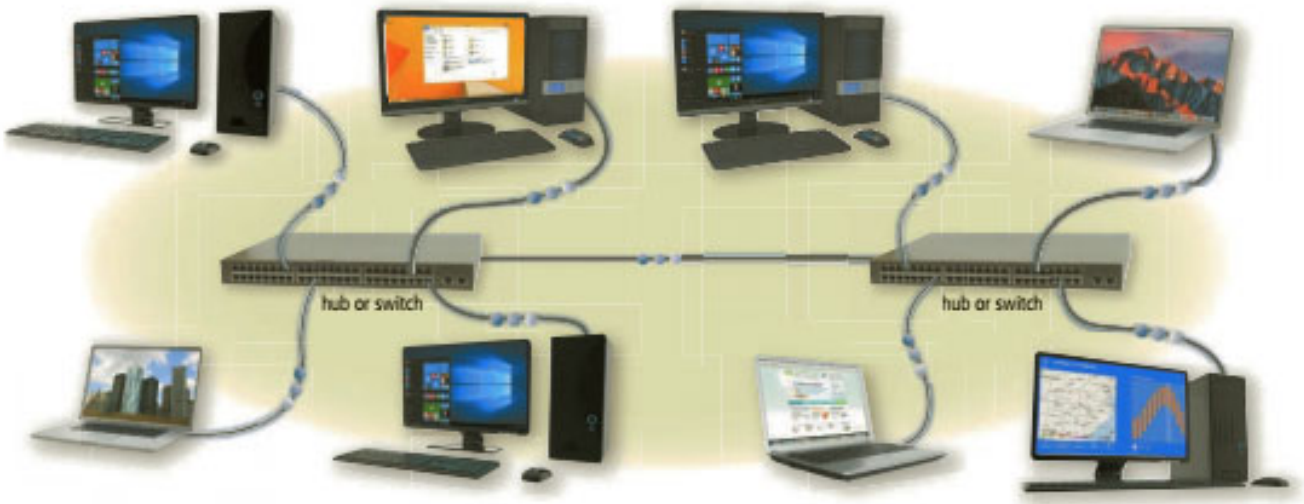


Figure 10-18 A hub or switch is a central point that connects several devices in a network together, as well as connects to other networks, as shown in this simplified diagram.
Courtesy of D-Link Corporation; iStockphoto.com / sweetym; Scanrail1 / Shutterstock.com; Scanrail1 / Shutterstock.com; iStockphoto.com / skodonnell; Natalia Siverina / Shutterstock.com; iStockphoto.com / skodonnell; iStockphoto.com / sweetym; Alex Staroseltsev / Shutterstock.com; iStockphoto.com / sweetym

Home Networks

Many home users connect multiple computers and devices together in a **home network**. Vendors typically offer home networking packages that include all the necessary hardware and software to network your home using wired or wireless techniques. You no longer need extensive knowledge of networks to set up a home network. For example, desktop operating systems often enable you to connect all computers in your house to a home network easily. Read Secure IT 10-3 to learn how to detect if an intruder is accessing your network.

SECURE IT 10-3

Detecting an Intruder Accessing Your Wireless Home Network

One of the largest Internet security threats is *IP hijacking*, which occurs when cyberthieves tap into home routers or cable modems or other Internet access point to intercept a paid Internet service. Some cyberthieves use the connection to commit illegal acts; others just steal the Internet connection. The incidences of IP hijacking are growing, and catching thieves is a difficult task for law enforcement officials.

Unscrupulous people hijack Internet service in one of two ways. Either the network has no security, or the thieves determine the network name and password and then reprogram their modem's settings to duplicate the network's settings. The Electronic Communications Privacy Act (ECPA) and a lack of funding prevent fraud examiners from investigating and prosecuting many IP hijackers.

Experts recommend using the following steps to determine if someone is accessing a wireless network without permission:

- **Sign in to the administrative interface.** The modem's user's guide will provide instructions to view wireless clients actively using a wireless access point.
- **Count the number of connected devices.** Each device connected wirelessly to the network should be displayed in a table that shows, at a minimum, the device's name, MAC address, and IP address. (Read How To 5-2 in Module 5 for additional information about MAC address controls.) Wireless devices that might be connected to the network include smartphones, game consoles, DVD players, and other hardware. If the number of devices seems extraordinarily high, use a MAC lookup website, which can help you to determine the manufacturer of wireless devices in the list.
- **Secure the network.** The router's manufacturer's website should provide instructions about upgrading the security strength. Change the default network name and password, and be certain to use the latest wireless encryption technology. Enable the router's firewall and, if possible, use "stealth mode" to make the network less visible to outsiders. Disable the feature that allows users to administer the router wirelessly, so that changes can be made only when using a physical connection with an Ethernet cable.

Consider This: If you use a wireless router, have you taken any of these steps to prevent IP hijacking? Which steps will you now take? Do you know anyone who has had a cyberthief access his or her network?

Tech Feature 10-3: Planning and Designing Your Home Network

As with any network, a home network's basic purpose is to share resources and connect devices. You can use a home network to share files and folders or to allow multiple devices to share a printer. Read Tech Feature 10-3 to learn about planning and designing your home network.

TECH FEATURE 10-3

Planning and Designing Your Home Network

A home network enables you to use a common Internet connection among many computers and mobile devices. Other uses include connecting entertainment devices, such as digital video recorders (DVRs) and televisions, to the Internet and establishing a connection between devices in order to play multiplayer games.

Before purchasing hardware, or contracting a network expert to set up your network, consider how your network will be used, and by whom. Ask yourself the following questions:

- What devices will connect to the network? The number of devices, as well as the operating system or platform on which the devices operate will determine the speed and strength needed to run your wireless network.

- How large of a range do you need, and where will most of the use take place? If you have a small apartment, your needs will differ from those with a large home.
- How many users typically will be using the network, how will they use it, and for what purposes? The number of users affects the capabilities of the network and determines whether you need to define permissions for certain users or devices.
- How secure do you need your network? Hiding the network name, requiring passwords, or having a user with network administration capabilities can help ensure your network is safe from unauthorized use.

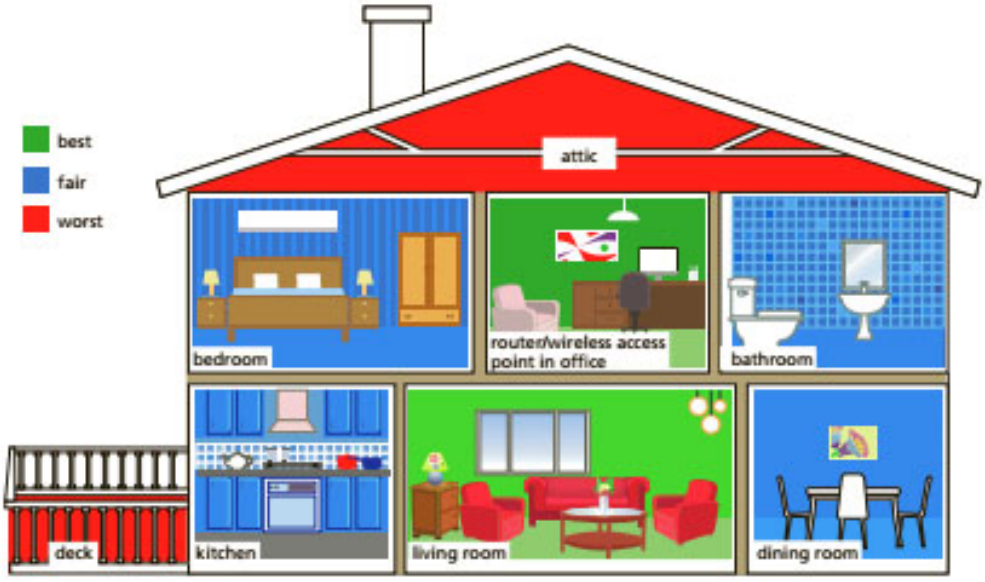
A home network can be as simple as using a cable to connect two devices. More complex home networks include wireless technologies that connect several devices to one another and to the Internet. Hardware needed for a wireless, Internet-connected home network includes the following:

- A modem, such as a cable or DSL modem, that connects to an ISP and establishes the Internet connection for the network
- A router, which establishes the connection between the Internet and all computers and devices on the home network and also enables the devices to communicate with one another
- A wireless access point, often included as part of the router, in order to connect wireless devices
- Computers and devices, such as desktops, laptops, tablets, smartphones, televisions, cable set-top boxes, or a VoIP phone, that you connect to the home network

Once you configure your wireless network, you can create user names and user groups. Names and groups establish network users, who can share files (such as documents, music, and photos), as well as devices (such as printers), with others connected to the network.

Maintaining the network involves monitoring the security settings and network activity, establishing connections to new devices as needed, and enhancing the wireless signal if necessary. Wireless home network speeds and ranges vary. The strength of the wireless signal affects the range of the network. Read How To 10-2 earlier in this module for instructions about strengthening a wireless signal.

Consider This: Do you have a home network? What devices are connected to it? Is your network password protected? Why or why not? Is the signal weaker in certain areas in your home? If so, where? What can you do to increase the effectiveness and security of your network?



An Example of Sending a Request over the Internet Using a Variety of Transmission Media

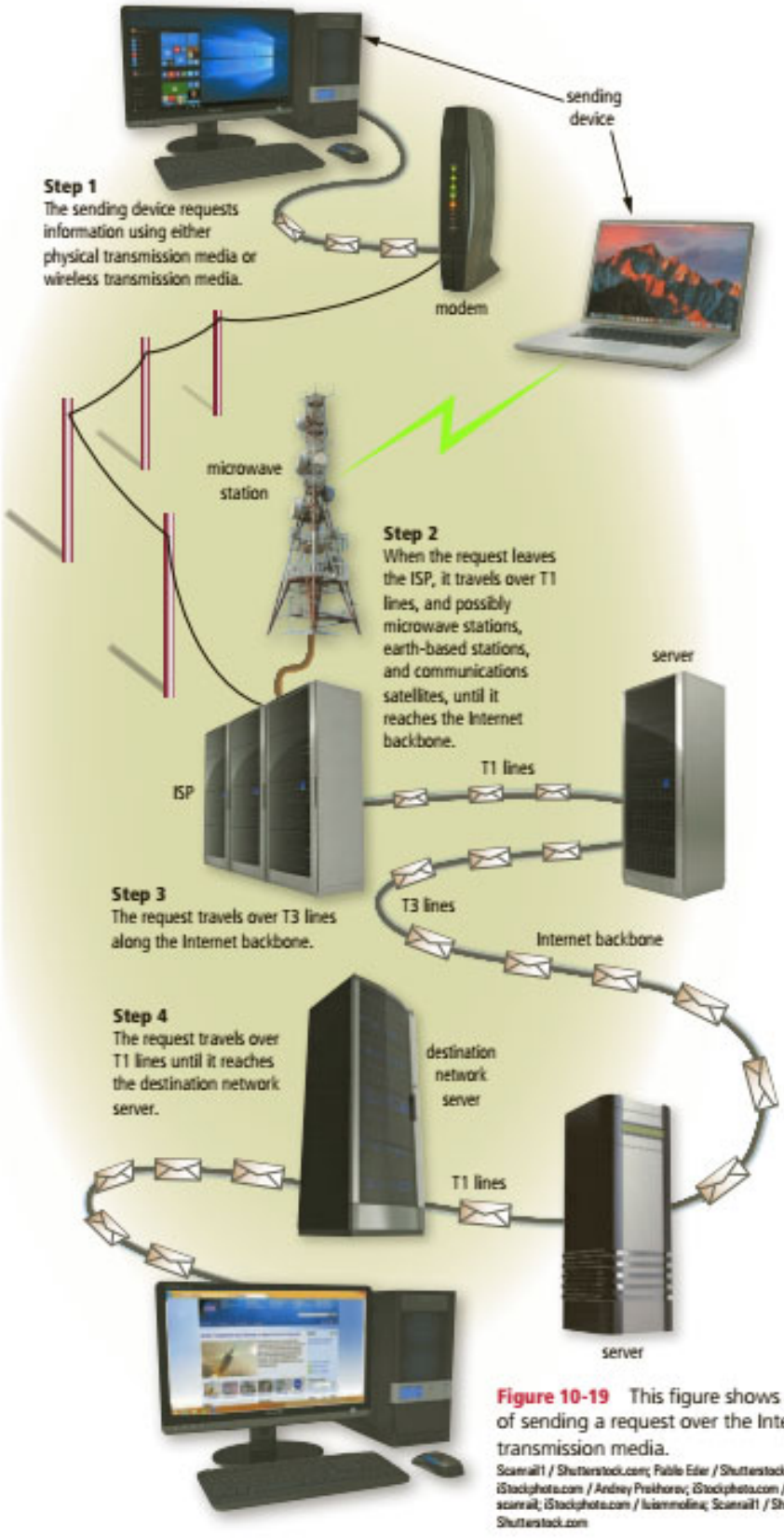


Figure 10-19 This figure shows a simplified example of sending a request over the Internet using a variety of transmission media.

Transmission Media

Transmission media consist of materials or substances capable of carrying one or more communications signals. When you send data from a computer or mobile device, the signal that carries the data may travel over various transmission media. This is especially true when the transmission spans a long distance. Figure 10-19 illustrates the variety of transmission media, including both physical and wireless, used to complete a data request over the Internet. Although many media and devices are involved, the entire communications process could take less than one second.

Broadband media transmit multiple signals simultaneously. The amount of data, instructions, and information that can travel over transmission media sometimes is called the **bandwidth**. The higher the bandwidth, the more data transmitted. For transmission of text only, a lower bandwidth is acceptable. For transmission of music, graphics, photos, virtual reality images, or 3-D games, however, you need a higher bandwidth. When the bandwidth is too low for the application, you will notice a considerable slowdown in system performance.

Latency, with respect to communications, is the time it takes a signal to travel from one location to another on a network. Several factors that negatively can affect latency include the distance between the two points, the type of transmission media, and the number of nodes through which the data must travel over the network. For best performance, bandwidth should be high and latency low. Read Ethics & Issues 10-3 to consider whether ISPs should be able to control Internet usage.

ETHICS & ISSUES 10-3

Should ISPs Be Allowed to Control Your Internet Usage?

People often compare the early days of the Internet and web to a wild frontier. ISPs simply offered customers an Internet connection and exerted no control over how the customer used the connection. This is similar to a phone company, which does not control who a customer calls, the length of a call, or the reason for the call. Online gaming, VoIP, video and audio streaming, and the use of web apps and cloud services led to an increased reliance on the Internet. Because of these increases, ISPs are attempting to regulate and limit their customers' usage.

Capping is a practice ISPs use that provides a certain amount of data usage at the optimal speed. Once a customer has used his or her allotted amount, the customer's Internet access is restricted, is slowed, or incurs additional costs. *Throttling* occurs when a network reduces upload and download speeds of certain high-data users at peak times in order not to tie up network resources for a small pool of users.

Controversy surrounds capping and throttling practices. Providers argue that caps are necessary to regulate traffic and ensure equal access to the Internet for all of its users. Critics argue that ISPs use limits to unfairly increase customer fees. Legislators are attempting to resolve the issues surrounding *net neutrality*, which is the concept of an open Internet, accessible to all users, without interference from ISPs or other third-parties. Proposals include standardizing how data transfer rates are measured and involving the Federal Communications Commission (FCC). The FCC would evaluate the regulations to ensure that ISPs intend merely to regulate traffic, rather than make a profit. It would examine whether caps or throttling are appropriate for low-usage times, such as in the middle of the night, and other related issues.

Consider This: Should ISPs control your Internet usage? Why or why not? Are data caps at peak usage times reasonable? Why or why not? Should the government enforce net neutrality? Why or why not?

Physical Transmission Media

Physical transmission media use wire, cable, and other tangible materials to send communications signals. These wires and cables typically are used underground or within or between buildings. Ethernet and token ring LANs use physical transmission media.

Table 10-3 lists the transfer rates of LANs using various physical transmission media. The following sections discuss each of these types.

Table 10-3 Transfer Rates for Physical Transmission Media Used in LANs

Type of Cable and LAN	Maximum Transfer Rate
Twisted-Pair Cable	
• 10Base-T (Ethernet)	10 Mbps
• 100Base-T (Fast Ethernet)	100 Mbps
• 1000Base-T (Gigabit Ethernet)	1 Gbps
• Token ring	4 Mbps to 16 Mbps
Coaxial Cable	
• 10Base2 (ThinWire Ethernet)	10 Mbps
• 10Base5 (ThickWire Ethernet)	10 Mbps
Fiber-Optic Cable	
• 10Base-F (Ethernet)	10 Mbps
• 100Base-FX (Fast Ethernet)	100 Mbps
• FDDI (Fiber Distributed Data Interface) token ring	100 Mbps
• Gigabit Ethernet	1 Gbps
• 10-Gigabit Ethernet	10 Gbps
• 40-Gigabit Ethernet	40 Gbps
• 100-Gigabit Ethernet	100 Gbps

Twisted-Pair Cable

One of the more widely used transmission media for network cabling and landline phone systems is twisted-pair cable. **Twisted-pair cable** consists of one or more twisted-pair wires bundled together (Figure 10-20). Each *twisted-pair wire* consists of two separate insulated copper wires that are twisted together. The wires are twisted together to reduce **noise**, which is an electrical disturbance that can degrade communications.

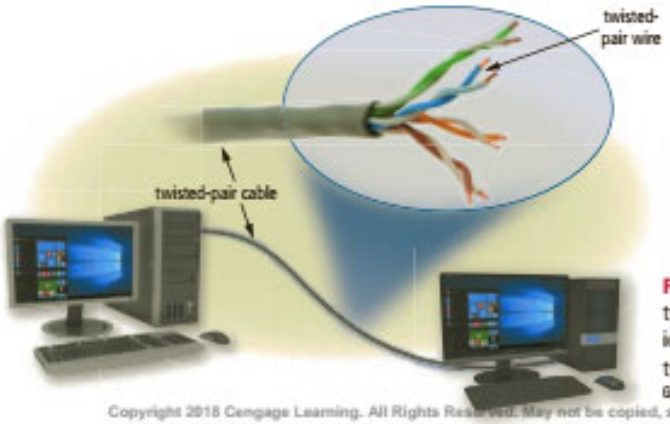


Figure 10-20 A twisted-pair cable consists of one or more twisted-pair wires. Each twisted-pair wire usually is color coded for identification. Landline phone networks and LANs often use twisted-pair cable.

Galushko Sergey / Shutterstock.com; iStockphoto.com / 123render; Scanrail1 / Shutterstock.com

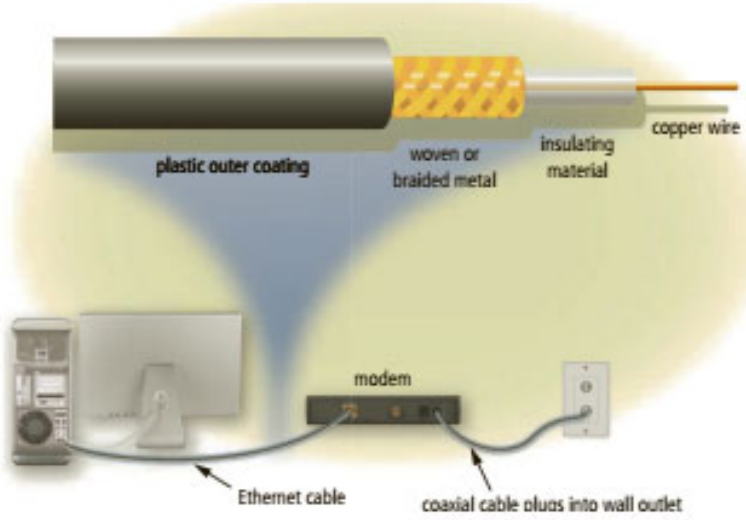


Figure 10-21 On coaxial cables, data travels through a copper wire. This simplified illustration shows a computer connected to a modem, which also is connected to the CATV network through a coaxial cable.

Coaxial Cable

Coaxial cable, often referred to as *coax* (pronounced KO-ax), consists of a single copper wire surrounded by at least three layers: (1) an insulating material, (2) a woven or braided metal, and (3) a plastic outer coating (Figure 10-21).

CATV network wiring often uses coaxial cable because it can be cabled over longer distances than twisted-pair cable. Most of today's computer networks, however, do not use coaxial cable because other transmission media, such as fiber-optic cable, transmit signals at faster rates.

Fiber-Optic Cable

The core of a **fiber-optic cable** consists of dozens or hundreds of thin strands of glass or plastic that use light to transmit signals. Each strand, called an *optical fiber*, is as thin as a human hair. Inside the fiber-optic cable, an insulating glass cladding and a protective coating surround each optical fiber (Figure 10-22).

Fiber-optic cables have the following advantages over cables that use wire, such as twisted-pair and coaxial cables:

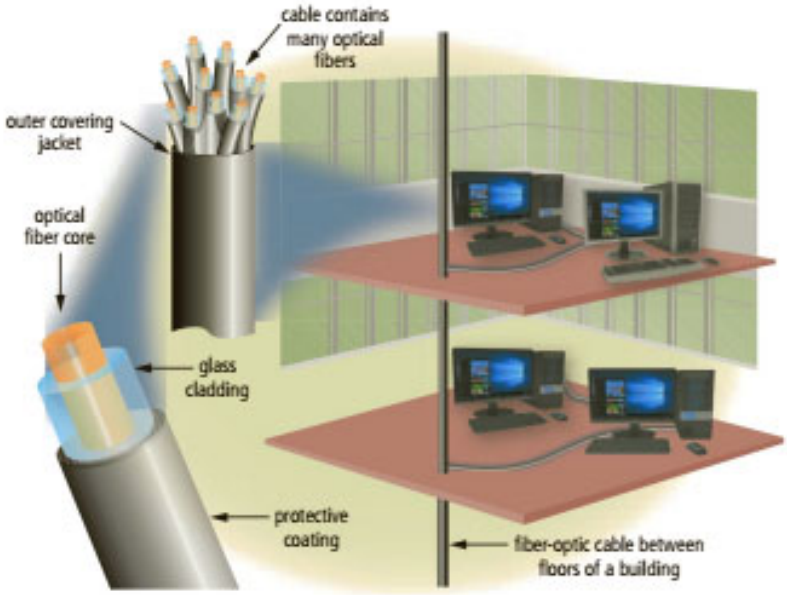


Figure 10-22 A fiber-optic cable consists of hair-thin strands of glass or plastic that carry data as pulses of light, as shown in this simplified example.

- Capability of carrying significantly more signals than wire cables
- Faster data transmission
- Less susceptible to noise (interference) from other devices, such as a copy machine
- Better security for signals during transmission because they are less susceptible to noise
- Smaller size (much thinner and lighter weight)

Disadvantages of fiber-optic cable are it costs more than twisted-pair or coaxial cable and can be difficult to install and modify. Despite these limitations, many phone companies replaced original analog phone lines with fiber-optic cables, enabling them to offer fiber-optic Internet access to home and business users. Businesses also use fiber-optic cables in high-traffic networks or as the backbone in a network.

Wireless Transmission Media

Wireless transmission media send communications signals through the air or space. Many users opt for wireless transmission media because it is more convenient than installing cables. In addition to convenience, businesses use wireless transmission media in locations where it is impossible to install cables. Read How To 10-3 for instructions about adding a printer to a wireless network.

HOW TO 10-3

Add a Wireless Printer to a Home/Small Office Network

Adding a wireless printer to a home or small office network has several advantages. For example, multiple computers and mobile devices on the network can use the printer. You also can place the printer anywhere in the home or office, as long as it is within range of the wireless signal. For example, a wireless router can be on the first floor of your house, and a wireless printer can be on the second floor. The following steps describe how to add a wireless printer to a home/small office network:

1. Determine the location to install the wireless printer. This location must have an electrical outlet for the printer and also be within range of the wireless network. You can check the strength of wireless signals in your home or office by walking around with a mobile computer or device while connected to the network and monitoring the signal strength.
2. Be sure to place the printer on a stable surface.
3. Access the printer's settings and navigate to the network settings.
4. Connect to the wireless network in your home or small office. If necessary, specify the encryption key for your network.
5. Enter any remaining required information.
6. Install the printer software on the computer(s) from which you want to print to the wireless printer. During the installation process, you will select the wireless printer that you have connected and configured. If the printer does not appear, return to Step 4 and try connecting the printer to the wireless network again. If the problem persists, consider contacting the printer's manufacturer.
7. Verify the computers are able to print successfully to the wireless printer.

Consider This: What are some ways to prevent some computers or mobile devices on your network from printing on your wireless printer?

iStockphoto.com / btrenkel

Types of wireless transmission media used in communications include infrared, broadcast radio, cellular radio, microwaves, and communications satellites. Table 10-4 lists transfer rates of various wireless transmission media, which are discussed in the following sections.

Table 10-4 Wireless Transmission Media Transfer Rates

Medium		Maximum Transfer Transmission Rate
Infrared		115 Kbps to 4 Mbps
Broadcast radio	• Bluetooth	1 Mbps to 24 Mbps
	• 802.11b	11 Mbps
	• 802.11a	54 Mbps
	• 802.11g	54 Mbps
	• 802.11n	300 Mbps
	• 802.11ac	500 Mbps to 1 Gbps
	• 802.11ad	up to 7 Gbps
	• UWB	110 Mbps to 480 Mbps
Cellular radio	• 2G	9.6 Kbps to 144 Kbps
	• 3G	144 Kbps to 3.84 Mbps
	• 4G	Up to 100 Mbps
Microwave radio		Up to 10 Gbps
Communications satellite		Up to 2.56 Tbps

Infrared

As discussed earlier in the module, infrared (IR) is a wireless transmission medium that sends signals using infrared light waves. Mobile computers and devices, such as a mouse, printer, and smartphone, may have an IrDA port that enables the transfer of data from one device to another using infrared light waves.

Broadcast Radio

Broadcast radio is a wireless transmission medium that distributes radio signals through the air over long distances, such as between cities, regions, and countries, and short distances, such as within an office or home.

For radio transmissions, you need a transmitter to send the broadcast radio signal and a receiver to accept it. To receive the broadcast radio signal, the receiver has an antenna that is located in the range of the signal. Some networks use a transceiver, which both sends and receives signals from wireless devices. Broadcast radio is slower and more susceptible to noise than physical transmission media, but it provides flexibility and portability.

Bluetooth, UWB, and Wi-Fi communications technologies discussed earlier in this module use broadcast radio signals. Bluetooth and UWB are alternatives to infrared communications, with the latter designed for high-bandwidth transmissions. Hot spots use Wi-Fi.

BTW

Data Transfer Rates

Tbps (terabits per second) is one trillion bits per second.

Cellular Radio

Cellular radio is a form of broadcast radio that is in wide use for mobile communications, specifically wireless modems and mobile phones (Figure 10-23). A mobile phone uses high-frequency radio waves to transmit voice and digital data messages. Because only a limited number of radio frequencies exist, mobile service providers reuse frequencies so that they can accommodate the large number of users. Some users install an amplifier or booster to improve the signal strength. Read Secure IT 10-4 to consider issues related to fake cell towers.

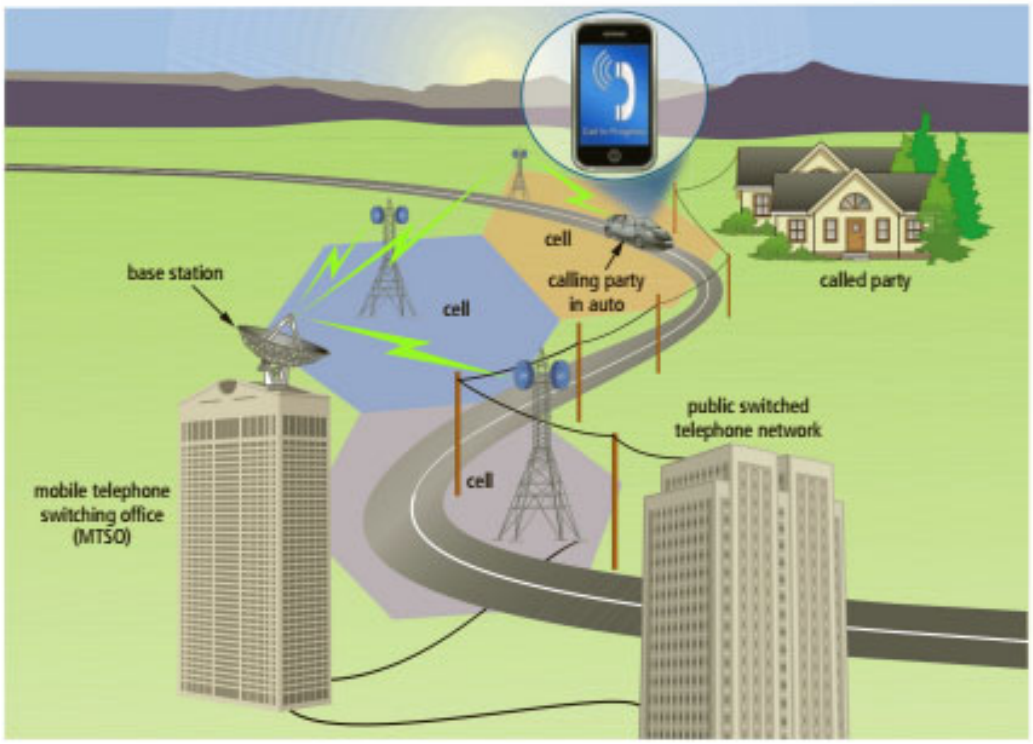


Figure 10-23 As a person with a mobile phone drives from one cell to another, the radio signals transfer from the base station (microwave station) in one cell to a base station in another cell.
Stuart Miles / Dreamstime.com

SECURE IT 10-4

Fake Cell Towers Are Tracking Devices

At least 17 cell towers located throughout the United States are intercepting mobile phone calls, according to technical security company ESD America. The company has identified these towers but does not know who owns them. It does know, however, that they do not belong to a mobile service provider or to the National Security Agency (NSA).

Every mobile device has a unique *International Mobile Subscriber Identity* (*IMSI*) that allows it to communicate with a cell tower. The interceptor technology on fake towers grasps, or catches, this IMSI signal; hence, it is known as an IMSI catcher. According to some reports, cyberthieves can purchase IMSI catchers for $1,800 or can build the devices themselves. The interceptors, also called stingrays, slow the protocol, so consumers may notice that the display on their smartphone shows that the 4G connection has dropped to 2G and that the performance has degraded. Higher-quality interceptors, however, will not change the phone's display when the phone has been attacked.

The Federal Communications Commission (FCC) is investigating these fake towers to determine who or what entity is intercepting the calls. It has established a task force to protect cellular networks and to address the threat of illicit IMSI catcher technology. It also is working with several industry organizations to develop new, secure cybersecurity standards. In addition, the FCC urges consumers to update their mobile devices' operating systems and apps because the latest software often addresses security vulnerabilities.

Consider This: Have you read any articles or publications disclosing the illicit and unauthorized use of IMSI catchers? Who or what organization do you think is using these interceptors?

Several categories of cellular radio transmissions exist, defining the development of cellular networks. Although the definitions of these categories may vary by mobile service providers, below are some general guidelines:

- *1G* (first generation of cellular transmissions)
  - Analog data transfer at speeds up to 14.4 Kbps
- *2G* (second generation of cellular transmissions)
  - Digital data transfer at speeds from 9.6 Kbps to 144 Kbps
  - Improved voice transmissions, added data communications, and added SMS (short message service) or text messaging services
  - Standards include *GSM* (Global System for Mobile Communications) and *GPRS* (General Packet Radio Service)
- *3G* (third generation of cellular transmissions)
  - Digital data transfer at speeds from 144 Kbps to 3.84 Mbps
  - Improved data transmissions, added MMS (multimedia message services)
  - Standards include *UMTS* (Universal Mobile Telecommunications System), CDMA (Code Division Multiple Access), EDGE (Enhanced Data GSM Environment), and EVDO (Evolution Data Optimized)
- *4G* (fourth generation of cellular transmissions)
  - Digital data transfer at speeds up to 100 Mbps
  - Improved video transmissions
  - Standards include Long Term Evolution (LTE), Ultra Mobile Broadband (*UMB*), and IEEE 802.16 (WiMAX)
- *5G* (fifth generation of cellular transmissions)
  - Future generation of cellular transmissions
  - Expected to improve bandwidth
  - Expected to provide artificial intelligence capabilities on wearable devices

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave transmission, often called *fixed wireless*, involves sending signals from one microwave station to another (Figure 10-24). A *microwave station* is an earth-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications. As with infrared, microwaves use line-of-sight transmission. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers, or mountains.

Microwave transmission typically is used in environments where installing physical transmission media is difficult or impossible and where line-of-sight transmission is available. For example, microwave transmission is used in wide-open areas, such as deserts or lakes, between buildings in a close geographic area, or to communicate with a satellite. Current users of microwave transmission include universities, hospitals, city governments, CATV providers, and phone companies. Homes and small businesses that do not have other high-speed Internet connections available in their area also opt for lower-cost fixed wireless plans.

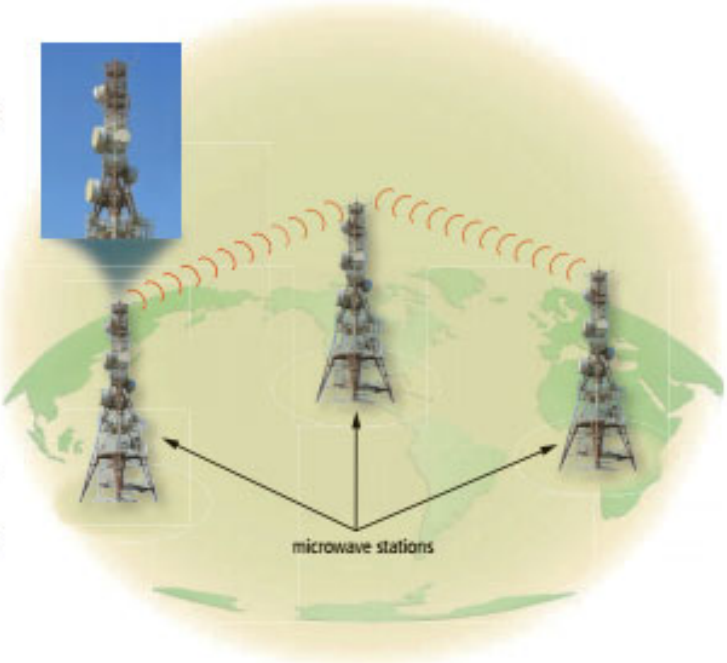


Figure 10-24 A microwave station is a ground-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications.

Alfonso de Tomas / Shutterstock.com

Figure 10-25 Communications satellites are placed about 22,300 miles above the Earth's equator.

Communications Satellite

A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies (strengthens) the signals, and broadcasts the signals back over a wide area to any number of earth-based stations (Figure 10-25). These earth-based stations often are microwave stations. Other devices, such as smartphones and GPS receivers, also can function as earth-based stations. Transmission from an earth-based station to a satellite is an *uplink*. Transmission from a satellite to an earth-based station is a *downlink*.

Applications such as air navigation, television and radio broadcasts, weather forecasting, videoconferencing, paging, GPS, and Internet connections use communications satellites. With the proper satellite dish and a satellite modem, consumers can access the Internet using satellite technology. With satellite Internet connections, however, uplink transmissions usually are slower than downlink transmissions. This difference in speeds usually is acceptable to most Internet satellite users because they download much more data than they upload. Although a satellite Internet connection is more expensive than cable Internet or DSL connections, sometimes it is the only high-speed Internet option in remote areas.

GPS As described previously, a **GPS** (*global positioning system*) is a navigation system that consists of one or more earth-based receivers that accept and analyze signals sent by satellites in order to determine the receiver's geographic location.

Many mobile devices, such as smartphones, have GPS capability built into the device or as an add-on feature. Some users carry a handheld GPS receiver; others mount a receiver to an object such as an automobile, a boat, an airplane, farm and construction equipment, or a computer or mobile device. A GPS receiver is a handheld, mountable, or embedded device that contains an antenna, a radio receiver, and a processor. Many include a screen display that shows an individual's location on a map. Figure 10-26 shows how a GPS works.

Figure 10-26 This simplified figure shows how a GPS works.

Tupungato / Shutterstock.com; kaczor58 / Shutterstock.com; iStockphoto.com / GeorgeManga; iStockphoto.com / Sebastien Cote / coteseb astien; iStockphoto.com / PhotoTalk; 3Dstock / Shutterstock.com; Lithiumphoto / Shutterstock.com; Evgeny Vasenev / Shutterstock.com; Courtesy of Garmin International; Courtesy of Garmin International; Mmaver / Shutterstock.com; iStockphoto.com / GeorgeManga

CONSIDER THIS

What are uses of GPS?

The first and most used application of GPS technology is to assist people with determining where they are located. The data obtained from a GPS, however, can be applied to a variety of other uses: creating a map, ascertaining the best route between two points, locating a lost person or stolen object, monitoring the movement of a person or object, determining altitude, and calculating speed.

Many vehicles use GPSs to provide drivers with directions or other information, such as alternate traffic routes, automatically call for help if the airbag is deployed, dispatch roadside assistance, unlock the driver's side door if keys are locked in the car, and track the vehicle if it is stolen. Newer GPS receivers and mobile apps that support GPS technology also provide information about nearby points of interest, such as gas stations, restaurants, and hotels. Hikers and remote campers may carry GPS receivers in case they need emergency help or directions.

Some GPS receivers work in conjunction with a cellular radio network. Parents, for example, can locate the whereabouts of a child who carries a mobile phone with GPS capability or other GPS-enabled device.

Summary

This module presented a variety of networks and communications technologies. It discussed various types of network architectures and standards and protocols. It explained communications software. Several types of communications lines and communications devices were presented. The module discussed how to create a home network. It also presented a variety of physical transmission media and wireless transmission media.

STUDENT ASSIGNMENTS

Study Guide

The Study Guide reinforces material you should know after reading this module.

Instructions: Answer the questions below using the format that helps you remember best or that is required by your instructor. Possible formats may include one or more of these options: write the answers; create a document that contains the answers; record answers as audio or video using a webcam, smartphone, or portable media player; post answers on a blog, wiki, or website; or highlight answers in the book/e-book.

1. List the device types and media you need for successful communications.
2. A(n) _____ is a collection of computers and devices connected together via communications devices and transmission media.
3. List reasons home and business users create a network. Identify how networks facilitate communications.
4. A(n) _____ is a third-party business that provides networking services, such as EDI.
5. Define the terms, intranet and extranet.
6. Differentiate among LANs, WLANs, MANs, WANs, and PANs.
7. Explain issues surrounding the use of BANs.
8. Name and describe two types of network architectures.
9. Define the terms, client and server.
10. Explain how P2P networks function, and describe the uses of P2P file sharing.
11. List functions of communications software. List and describe forms of immediate mobile communications.
12. Explain issues surrounding the use of telemedicine.
13. Define the terms, network standard and protocol. Explain whether they work together.
14. Define the term, Ethernet.
15. Explain what happens when two devices on an Ethernet attempt to send data at the same time.
16. Describe how a network transmits data using a token.
17. TCP/IP is the network standard for _____ communications. Describe how packet switching works.
18. Explain how network monitoring software and packet sniffers identify network security risks.
19. Explain whether you can use an IP address to determine a computer or device's location.
20. Describe how Wi-Fi enables users to connect to the Internet.
21. _____ is a network standard that defines how high-speed cellular transmissions use broadcast radio to transmit data for mobile communications.
22. List uses for Bluetooth devices. Name advantages and disadvantages of using Bluetooth.
23. Describe how to prevent Bluebugging.
24. Differentiate among UWB, IrDA, RFID, and NFC technologies.
25. Identify the role of a dedicated line. List types of digital dedicated lines.
26. Explain the advantages of cable Internet services and DSL.
27. List and differentiate among different T-carrier lines.
28. Define the term, communications device.
29. List and describe three widely used types of broadband modems.
30. Define the term, dial-up modem.
31. Define the terms, wireless modem and mobile hot spot.
32. List the steps to use your phone as a mobile hot spot.
33. Define the term, wireless access point. Explain how to strengthen your wireless signal.
34. Identify the role of a router. List types of routers that offer additional functionality.
35. To prevent unauthorized users from accessing files and computers, many routers are protected by a built-in _____ firewall.
36. Describe the function of a network card.
37. Identify the roles of hubs and switches on a network.
38. Explain how to determine if someone is accessing a wireless network without permission.
39. List questions to ask when planning a home network.
40. Identify hardware needed to set up a home network.
41. Define the terms, broadband, bandwidth, and latency.
42. Explain issues surrounding ISPs setting limits on Internet usage.
43. Name types of physical transmission media. Define the term, noise.
44. Identify advantages and disadvantages of fiber-optic cables.
45. List steps to add a wireless printer to a home/small office network.
46. Name types of wireless transmission media.
47. Explain how cyberthieves use fake cell towers to intercept communications.
48. Differentiate among 1G, 2G, 3G, 4G, and 5G cellular transmissions.
49. List uses of GPS.

STUDENT ASSIGNMENTS

Key Terms

You should be able to define the Primary Terms and be familiar with the Secondary Terms listed below.

Primary Terms (shown in **bold-black** characters in the module)

802.11 (10-12)
ATM (10-18)
bandwidth (10-26)
Bluetooth (10-13)
broadband (10-26)
broadcast radio (10-29)
cable modem (10-18)
cellular radio (10-30)
client/server network (10-7)
clients (10-7)
coaxial cable (10-28)
communications device (10-18)
communications satellite (10-32)
communications software (10-8)
dedicated line (10-16)
DSL (10-17)
DSL modem (10-19)
Ethernet (10-10)
fiber-optic cable (10-28)
FTTP (Fiber to the Premises) (10-17)
GPS (10-32)
home network (10-24)
IrDA (10-15)
latency (10-26)
local area network (LAN) (10-4)
LTE (10-12)
microwaves (10-31)
network (10-3)
NFC (10-16)
noise (10-27)
personal area network (PAN) (10-6)
receiving device (10-3)
RFID (10-15)
sending device (10-2)
server (10-7)
T-carrier line (10-18)
TCP/IP (10-11)
token ring (10-10)
transmission media (10-3)
twisted-pair cable (10-27)
UWB (ultra-wideband) (10-14)
wide area network (WAN) (10-6)
Wi-Fi (10-12)
wireless LAN (WLAN) (10-5)

Secondary Terms (shown in *italic* characters in the module)

1G (10-31)
2G (10-31)
3G (10-31)
4G (10-31)
5G (10-31)
ADSL (asymmetric digital subscriber line) (10-17)
Bluebugging (10-14)
body area network (BAN) (10-6)
broadband modem (10-18)
broadband router (10-21)
broadband wireless router (10-22)
cable Internet service (10-16)
capping (10-27)
coax (10-28)
communications channel (10-3)
dial-up modem (10-19)
digital modem (10-18)
Digital Subscriber Line (10-17)
downlink (10-32)
downstream rate (10-12)
EDI (electronic data interchange) (10-4)
electronic funds transfer (EFT) (10-4)
extranet (10-4)
file sharing network (10-8)
fixed wireless (10-31)
fractional T1 (10-18)
FTTB (Fiber to the Building) (10-17)
FTTH (Fiber to the Home) (10-17)
Gbps (10-10)
global positioning system (10-32)
GPRS (10-31)
GSM (10-31)
hardware firewall (10-22)
hub (10-23)
International Mobile Subscriber Identity (IMSI) (10-30)
intranet (10-4)
IP hijacking (10-24)
ISDN modem (10-19)
line-of-sight transmission (10-15)
Mbps (10-10)
metropolitan area network (MAN) (10-6)
microwave station (10-31)
mobile broadband wireless router (10-22)
mobile hot spot (10-19)
near field communications (10-16)
net neutrality (10-27)
network architecture (10-7)
network card (10-22)
network interface card (NIC) (10-22)
network monitoring software (10-12)
network standard (10-10)
node (10-4)
optical fiber (10-28)
packet sniffer software (10-12)
packet switching (10-11)
packets (10-11)
peer (10-7)
peer-to-peer (P2P) network (10-7)
protocol (10-10)
radio frequency identification (10-15)
router (10-21)
switch (10-23)
T1 line (10-18)
T3 line (10-18)
Tbps (10-29)
telemedicine (10-9)
throttling (10-27)
token (10-10)
twisted-pair wire (10-27)
UMB (10-31)
UMTS (10-31)
uplink (10-32)
upstream rate (10-13)
value-added network (VAN) (10-4)
wireless access point (10-20)
wireless Ethernet (10-12)
wireless modem (10-19)
wireless router (10-21)

© iStockphoto.com / rodmalpicture

Checkpoint

The Checkpoint exercises test your knowledge of the module concepts.

True/False

Mark T for True and F for False. If False, rewrite the statement so that it is True.

_____ 1. All types of computers and mobile devices serve as sending and receiving devices in a communications system.

_____ 2. Files on an intranet also are accessible from the Internet.

_____ 3. Disadvantages of BANs include data validity and security.

_____ 4. A peer-to-peer (P2P) network typically connects fewer than 10 computers.

_____ 5. Voice and video calling require large amounts of bandwidth.

_____ 6. UWB requires line-of-sight transmission, so its technology is not as widespread as IrDA.

_____ 7. For successful communications with NFC devices, the devices or objects must touch or be placed within an inch or two of each other.

_____ 8. DSL transmits on existing standard copper phone wiring.

_____ 9. Large corporations, phone networks, the Internet, and other networks with large amounts of traffic use DSL.

_____ 10. A broadband modem is a communications device that converts digital signals to analog signals and analog signals to digital signals, so that data can travel along an analog phone line.

_____ 11. Although some routers may be able to connect more than 200 wired and/or wireless computers and mobile devices, the performance of the router may decline as you add connections.

_____ 12. With satellite Internet connections, uplink transmissions usually are slower than downlink transmissions.

Matching

Match the terms with their definitions.

_____ 1. bandwidth

_____ 2. client

_____ 3. Ethernet

_____ 4. latency

_____ 5. LTE

_____ 6. packet sniffer software

_____ 7. protocol

_____ 8. network standard

_____ 9. TCP/IP

_____ 10. value-added network (VAN)

a. standard that outlines characteristics of how two devices communicate on a network

b. guidelines that specify the way computers access the medium to which they are connected, the type(s) of medium used, the speeds used on different types of networks, and the type(s) of physical cable and/or the wireless technology used

c. third-party business that provides networking services, such as EDI services, secure data and information transfer, storage, or email

d. program that monitors and logs packet traffic for later analysis

e. network protocol that defines how messages are routed from one end of a network to the other, ensuring the data arrives correctly

f. the amount of data, instructions, and information that can travel over transmission media

g. network standard that specifies no computer or device on the network should control when data can be transmitted

h. computers or mobile devices on the network that rely on the server for its resources

i. the time it takes a signal to travel from one location to another on a network

j. network standard that defines how high-speed cellular transmissions use broadcast radio to transmit data for mobile communications

Problem Solving

The Problem Solving exercises extend your knowledge of module concepts by seeking solutions to practical problems with technology that you may encounter at home, school, or work. The Collaboration exercise should be completed with a team.

Instructions: You often can solve problems with technology in multiple ways. Determine a solution to the problems in these exercises by using one or more resources available to you (such as a computer or mobile device, articles on the web or in print, blogs, podcasts, videos, television, user guides, other individuals, electronics or computer stores, etc.). Describe your solution, along with the resource(s) used, in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

Personal

1. **Problems Exchanging Files** You are attempting to use Bluetooth to send files from your phone to your computer. When you try sending the files from your phone, it does not display your computer as a device to which it can send the file. What might be the problem?
2. **Cannot Connect to Hot Spot** You are sitting in a fast food restaurant that offers free Wi-Fi. When you search for available hot spots using your computer, the restaurant's hot spot does not appear in the computer's list of wireless networks. What are your next steps?
3. **Paired Bluetooth Devices** You and your brother each have your Bluetooth-enabled smartphones paired with your car so that you can talk through the car's microphone and listen through its speakers. When you and your brother are both in the car at the same time, his phone rings but it is not connected to the car's audio. Why might this be the case?
4. **Slow Internet Connection** Your Internet speed has suffered a sharp decline in performance recently. You have not added any computers or mobile devices to your house that might be accessing the network, and you are puzzled by the sudden performance problems. What might be the problem?
5. **Wireless Network Coverage** You installed a new wireless network in your house. You notice that you sometimes have trouble connecting to the network from certain locations in the house, but other times you can connect from the same location without issue. What might be causing the problem?

Professional

6. **Cannot Access Network** You brought your personal laptop to your place of employment so that you can take care of some personal obligations while you are on lunch break. You successfully connect to your company's wireless network but are unable to access the Internet. What might be the problem?
7. **Cannot Sign In** Your corporate network requires you to sign in with a user name and password as soon as your computer or mobile device connects. After entering your user name and password, the computer still does not connect to the network. What might be the problem?
8. **Too Many Networks** While attempting to connect to the wireless network at your job, you notice that five different wireless networks are available. How can you determine the network to which you should connect?
9. **No Network Connection** You have unpacked, installed, and turned on a new computer at your desk. When the operating system starts and you run the browser to display a webpage, you receive an error message stating that you are not connected to the Internet. You check the network card on the back of the computer and although the cable is plugged in, the lights next to the port are not flashing. What are your next steps?
10. **Connecting Corporate Email** You are visiting your company's remote office for the day and realize that you do not have the necessary information to connect to their wireless network. Your boss has asked you to check your email throughout the day, so it is important that you connect to the Internet. What are your next steps?

Collaboration

11. **Technology in Agriculture** Your employer owns hundreds of acres of orange groves and realizes labor and utility costs can be decreased by installing automated systems to manage the property. As a digitally literate employee of the organization, your supervisor asks you to research automated systems that can help decrease expenses. Form a team of three people to research automated agricultural solutions. One team member should research automated irrigation systems that water the trees only as needed. Another team member should research solutions that can keep the trees healthy and free from pests, and the third team member should create a list of reasons why these automated systems can decrease costs, bolster efficiency, and increase profit. Compile your findings and submit them to your instructor.

STUDENT ASSIGNMENTS

How To: Your Turn

The How To: Your Turn exercises present general guidelines for fundamental skills when using a computer or mobile device and then require that you determine how to apply these general guidelines to a specific program or situation.

Instructions: You often can complete tasks using technology in multiple ways. Figure out how to perform the tasks described in these exercises by using one or more resources available to you (such as a computer or mobile device, articles on the web or in print, online or program help, user guides, blogs, podcasts, videos, other individuals, trial and error, etc.). Summarize your 'how to' steps, along with the resource(s) used, in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1 Evaluate Internet Access Plans

If you are planning to connect to the Internet from your computer or mobile device, you will need to subscribe to an Internet access plan. Cable companies, phone companies, and mobile service providers all offer Internet access plans, so it is important to evaluate the plans in your area to determine which one is best for you. The following steps guide you through the process of evaluating Internet access plans.

a. Create a budget. Internet access plans are available for a monthly fee, so determine how much money you are able to spend for Internet access on a monthly basis.
b. Locate and list the Internet access plans available in your area. To determine Internet access plans that are available, check the local cable or phone company's website and search for available plans. You may have to enter your ZIP code to determine whether certain plans are available in your area. Alternatively, visit a local electronics store and inquire about wireless Internet access plans available in your area.
c. Compare Internet access speeds. Each Internet access plan may offer a different speed, so determine which speed is sufficient for you. If you mainly browse webpages and send or receive email messages, you may not need a plan that offers the fastest transfer rates. If you plan to download files, play online games, and watch movies on the Internet, you should consider a plan with faster transfer rates. You also should consider a plan with faster transfer rates if you will have multiple devices accessing the Internet simultaneously in your household. If an ISP offers multiple plans with a variety of transfer rates, it often will let you switch back and forth between plans without penalty so that you can find the one with the transfer rate that is best for you.
d. Check for package deals. If you already have service with an existing CATV or phone provider, they may be able to add Internet access to your current services at a reduced rate. Bundling multiple services can make each service (such as Internet access) less expensive, but you should be careful not to sign up for services you do not need.
e. Think about how much data you intend to transfer each month. Some Internet access plans limit the amount of data you can upload or download each month. While it can be difficult to determine how much data you will upload or download, you first should purchase a plan that might allow you to transfer more than you think you will need. Monitor your data usage each month and consider downgrading to a plan that provides the amount of data transfer that better represents your use.
f. Determine where you require Internet access. Some ISPs will allow you to use their hot spots for free in locations such as shopping malls, coffeehouses, and airports. Consider the additional locations from where you can access the Internet for free, and determine whether it makes the Internet access plan more desirable.
g. Consider whether a wireless Internet access plan is appropriate. While these plans can cost more and transfer rates often are not as fast, they do provide the flexibility of allowing you to connect to the Internet from almost anywhere. If you often travel and regularly need to access the Internet while away from home, a wireless Internet access plan might be right for you.

Exercises

1. What Internet access plans are available in your area?
2. Prepare a table comparing the Internet access plans in your area. Based on your current Internet usage, which plan appears to be the best? Why?
3. How can you determine approximately how much data you will transfer each month?

2 Locate Hot Spots

If you are using a mobile computer or device and need to access the Internet, you will need to locate a hot spot. Hot spots are available in a variety of locations, such as coffeehouses, shopping malls, public libraries, airports, and educational institutions. Once you locate a hot spot, be sure to use it safely. Read Secure IT 2-1 in Module 2 for more information about using public Wi-Fi hot spots safely. If you plan to connect to a wireless hot spot, make sure you are authorized to connect.

For example, you should not connect to people's or businesses' hot spots without their knowledge or consent. If you are unsure of whether you are authorized to connect to a hot spot, contact someone representing the residence or business providing the hot spot. The following are guidelines that can assist you in locating a hot spot:

- Enable (turn on) your mobile computer or device's Wi-Fi and see whether it automatically detects any wireless networks. If one or more wireless networks are detected, connect to the one with the SSID that accurately describes your location. For example, if you are at a coffeehouse, the SSID of the wireless network might be the coffeehouse's name. If you unsure of the wireless network to which you should connect, contact an employee at the location and inquire. If the wireless network is protected with a password, the employee may be able to provide the password.
- You can check the location's website or app in advance to determine whether it has free Wi-Fi. For example, if you are flying out of your local airport, the airport's website might indicate whether Wi-Fi is available.
- Businesses offering free Wi-Fi sometimes have a decal on a front door or window indicating the location has Wi-Fi. If necessary, contact an employee to determine how to connect to the wireless network.
- Search for and navigate to a website that lists Wi-Fi hot spots in a particular area. These websites sometimes do not provide the most up-to-date information, so do not rely completely on the information you locate.

DaiMou / Shutterstock.com

Exercises

1. What public hot spots are available near where you live?
2. Have you connected to a public hot spot before? If so, when?
3. What security risks may be associated with connecting to a public hot spot?

3 Test Your Internet Speed

Internet connection speeds will vary depending on the type of Internet connection you currently are using. If you believe your Internet speed is not what was promised by your Internet access provider, you can test your Internet speed to see how it is performing. The following steps guide you through the process of testing your Internet speed:

a. Turn off any computers or mobile devices that might be accessing the Internet, except for the computer on which you want to test your broadband speed.
b. If your broadband Internet service is provided through your phone company, do not talk on the phone during the test. If your CATV company provides your broadband Internet service, turn off all devices accessing the cable television. If you have cable boxes or converters, disconnect them from their power source so that they cannot communicate using the Internet connection while you are testing your broadband speed.
c. Run the browser.
d. Search for and navigate to a website that can test your Internet speed.
e. Click the button to start the test. The test may take up to one minute to complete before displaying results.
f. Internet speeds sometimes can vary with the time of day or day of the week. Repeat the previous steps to test your Internet speed at various times throughout the day, as well as on weekdays and weekends.
g. If you have any concerns regarding your Internet speed, contact your Internet access provider.

Exercises

1. What is the speed of the Internet connection on the computer or mobile device you currently are using?
2. Test your Internet speed while other computers and mobile devices also are using the Internet connection. How do the results vary from when your other devices are turned off?
3. Do you see differences in the Internet speed when you test it during the day versus at night? If so, what might explain these differences in speed?

speedtest.net

STUDENT ASSIGNMENTS

Internet Research

The Internet Research exercises broaden your understanding of module concepts by requiring that you search for information on the web.

Instructions: Use a search engine or another search tool to locate the information requested or answers to questions presented in the exercises. Describe your findings, along with the search term(s) you used and your web source(s), in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1 Making Use of the Web

Blogs, Wikis, and Collaboration

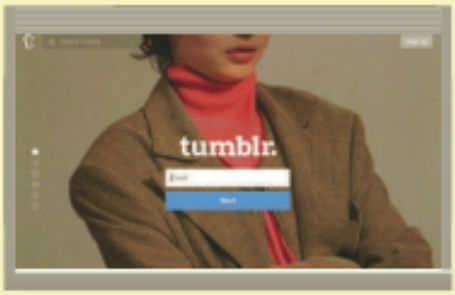
Writers can publish their views and share their interests using blogs, as you learned in Module 2. The blogosphere began as an easy way for individuals to express their opinions on the web. Today, this communications vehicle has become a powerful tool for individuals, groups, and corporations to promote their ideas and to advertise their products. Individuals easily may set up a blog free or for a fee, and they do not need to have knowledge of web design or programming.

Wikis are collaborative websites. As discussed in Module 2, users can develop, modify, and delete content on these public or private websites. This information can include articles, documents, photos, and videos. Other collaboration websites, such as Google Docs, allow users to share documents and to work together in real time. All files are stored online, so participants can access these documents everywhere at any time.

Research This: (a) Visit two blogging services, such as Tumblr, WordPress, or Blogger. What steps are required to start a blog? Do these services have monthly or annual fees? Do storage limitations exist? What options are available to customize the design? Can products or services be sold or advertised? If you were to set up a blog, which topics would you cover? Could you assign your own domain name to your blog?

(b) Visit two reference wikis. Which subjects are featured? Which organizations host the websites? How are the wikis funded? Are they public or private? Who may edit the content? What procedure is used to add, modify, or delete information?

(c) Visit two collaboration websites. What features are available for sharing content, such as managing projects, scheduling, blogging, discussing forum topics, publishing information, delivering announcements, or uploading photos and videos? Are chat windows and whiteboards offered? What is the charge for using these services? Do they offer a mobile app? Do members receive notifications when content is updated?



Source: Tumblr, Inc.

2 Social Media

Online Dating Websites

Using social media can be an excellent opportunity to unite with people who share similar interests. In some cases, local groups form for members to improve themselves and their communities. Dog owners, runners, photographers, entrepreneurs, parents, and travelers are among the thousands of groups with members who met online. In addition, more than 41 million people in the United States have subscribed to at least one of the 2,500 online dating services. Online dating can offer a safe opportunity to meet a variety of people if some practical advice is followed. Reputable dating services keep information confidential and have many members. Some have niche dating demographics, such as age, professions, religion, cultural interests, or geographical regions, and members can search for matches with desired criteria.

Research This: Search at least two online dating websites for information about these services. How many members do they have? What is the cost to join? What are the monthly membership fees? What claims do their privacy statements make about not disclosing personal information? What policies are in place to report members who have acted inappropriately?

3 Search Skills

Map Search

Search engines provide capabilities to search for maps, directions, and local attractions. Type search text in a search engine and then click the Maps link on a search engine's home page to see a map of locations for your search text. For example, type the search text, verizon wireless chicago, in the search box to find locations of Verizon Wireless stores in Chicago. Type the search text, cisco boston, to view the location of the Boston Cisco office on a map. To obtain directions, type the address to or from which to obtain directions, and specify walking, driving, or by public transportation. On mobile devices with GPS capability, you can specify to use your current location as a starting or

ending location. You also can search near a location. For example, type the search text, pizza near 125 high street boston, to display the names of pizza restaurants near that location. Some mapping search tools allow you to zoom, pan, and navigate a map in aerial view or street view, showing the location when looking from above or on the street.

Source: Google, Inc.

Research This: Create search text using the techniques described above or in previous Search Skills exercises, and type it in a search engine to create maps that provide this information: (1) aerial and street view of your home, (2) directions to a local store that sells wireless networking equipment, (3) locations of your mobile service provider's retail stores in your current city, and (4) distance between Microsoft's headquarters in Redmond, Washington and Apple's headquarters in Cupertino, California. Take screenshots to capture and document your results.

4 Security

Online Dating Fraud

The Social Media exercise in this section discusses online dating websites. According to some of these dating services, 20 percent of people currently in committed relationships met online. While using these dating websites may result in a positive experience, the Better Business Bureau and other consumer-oriented organizations receive thousands of complaints each year about these services. Online dating fraud is rising, so security experts caution online dating members to follow safe practices, including the following:

- Compose a profile carefully, and be certain it reflects the image you want to portray. Do not post your full name, phone number, or home or work location.
- Use the service's messaging system before sending email or text messages or having a phone conversation.
- When arranging a first date, meet in a safe location, such as a restaurant during a busy time of the day. Share your plans with a friend, and keep a mobile phone handy.
- Trust your instincts. If you feel uncomfortable or threatened, leave the location and call a friend.

Research This: Visit at least two websites providing advice for online dating members. What guidance is provided in addition to the four safe practices listed above? What behaviors may signal potentially dangerous situations? Where can members verify other members' reputations? How can members report fraud and inappropriate behavior?

5 Cloud Services

Streaming Media from the Cloud (SaaS)

Streaming media allows users to play music or videos from the cloud without having to wait for the entire file to download. Streaming media is an example of software as a service (SaaS), a service of cloud computing that allows access to software apps using a browser, without the need to install software on a computer or device. Streaming media has become popular because of the decreasing cost of cloud storage; the increasing download speeds for business, home, and mobile users; and the growing number of devices available to play downloaded content.

When streaming, a provider sends the media to the user's device over the Internet in a compressed format. The user runs a media player app to uncompress the data as it arrives and then play the resulting audio data as sound; or, the user can display the resulting video data on mobile devices, computers, Smart TVs, and other devices that have an appropriate player.

Content providers, such as Netflix, Hulu, and Amazon, allow users to subscribe to their services for a monthly fee and watch videos on demand, or instantly, by streaming them to Internet-connected devices.

Individuals and businesses use streaming services to broadcast video of their events live, on the Internet in high definition. Many will use this service to broadcast presentations, product demonstrations, performances, and other events online.

Research This: (1) What file formats are used to compress audio and video files for streaming? (2) Compare the offerings of Netflix, Hulu, and Amazon for providing video on demand. Do you use any of these services? Which would you choose? Why? (3) Find a television or radio broadcast that is streamed live on the Internet and simultaneously broadcast "on air." Watch or listen to part of the live stream and then do the same for the broadcast on television or radio. How do the experiences and quality compare? What other events often are streamed live online?

STUDENT ASSIGNMENTS

Critical Thinking

The Critical Thinking exercises challenge your assessment and decision-making skills by presenting real-world situations associated with module concepts. The Collaboration exercise should be completed with a team.

Instructions: Evaluate the situations below, using personal experiences and one or more resources available to you (such as articles on the web or in print, blogs, podcasts, videos, television, user guides, other individuals, electronics or computer stores, etc.). Perform the tasks requested in each exercise and share your deliverables in the format requested by your instructor (brief report, presentation, discussion, blog post, video, or other means).

1. Transmission Media

You work as an intern in the IT department for a local newspaper. The newspaper's management team recently approved a budget for redesigning the interior of its century-old building as part of an urban rehabilitation project. Because the employees at the newspaper more often use mobile devices and laptops than desktops, the newspaper plans to set up a wireless LAN.

Do This: Prepare information that summarizes the issues surrounding wireless network setup. Include the following information: What hardware is required for a wireless network? Could the thick walls in the building present a problem? If so, how can the issue be resolved? Does a wireless network present any health hazards? What security concerns exist for a wireless network? What advantages does a wireless network have over a wired network for the newspaper's needs?

iStockphoto.com / wsfurlan

2. Wireless Networking Standards

Several networking standards exist for wireless networks, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, and 802.11af. You want to install a wireless network in your house and want to ensure that you choose the standard that best meets your needs.

Do This: Use the web to research the various wireless networking standards and answer the following questions: Which was the first developed standard? Are any of the standards more susceptible to interference from other wireless devices in your home, such as alarm systems and mobile phones? Which standard is the fastest? Is the fastest standard always the best, or do other factors on your wireless network or on the Internet affect performance? Is equipment to support one standard more expensive than the equipment that supports the other standards? Which would you recommend? Why? Address the answers to those questions, as well as any other information you find pertinent. Compile your findings.

3. Case Study

Family-Owned Coffee Shop You are the new manager for a family-owned coffee shop. The shop's office equipment consists of a few laptops and tablets, a printer, and several smartphones. The owners have asked you to investigate how the shop might use Bluetooth technology.

Do This: Review the uses of Bluetooth technology listed in Tech Feature 10-2 in this module. Which uses might apply to the shop? Can you think of other ways the shop might use Bluetooth technology? What are the advantages of using Bluetooth technology? Use the web to find industry experts' recommendations for Bluetooth use in a small business. What other wireless technologies might the shop use? Examine issues related to bandwidth, speed, and reliability. What security concerns exist? What measures should the shop take to prevent Bluebugging? Would you recommend the shop use Bluetooth? Why or why not? Should the shop replace its LAN with Bluetooth? Why or why not? Compile your findings.

Collaboration

4. Network Security

You are a network administrator for a small security firm. The company's main office includes 20 workers, most of whom use laptops. This year, the company plans to upgrade the network. The company asks your team to create a list of common network security issues, to make recommendations for hardware and software, and to create guidelines to secure the network.

Do This: Form a three-member team. As a team, list different networking security risks discussed in this module. Each member should choose a different risk to research. Members should determine the following: Describe the risk. Find an example of an industry article or blog post describing an experience with the risk. What damage was done? What steps did the network administrator take to recover from the damage, and/or prevent future attacks? What hardware or software can be used to safeguard against the risk? What guidelines for network users should be in place to help avoid the risk? As a team, compile your findings and share your recommendation with the class.