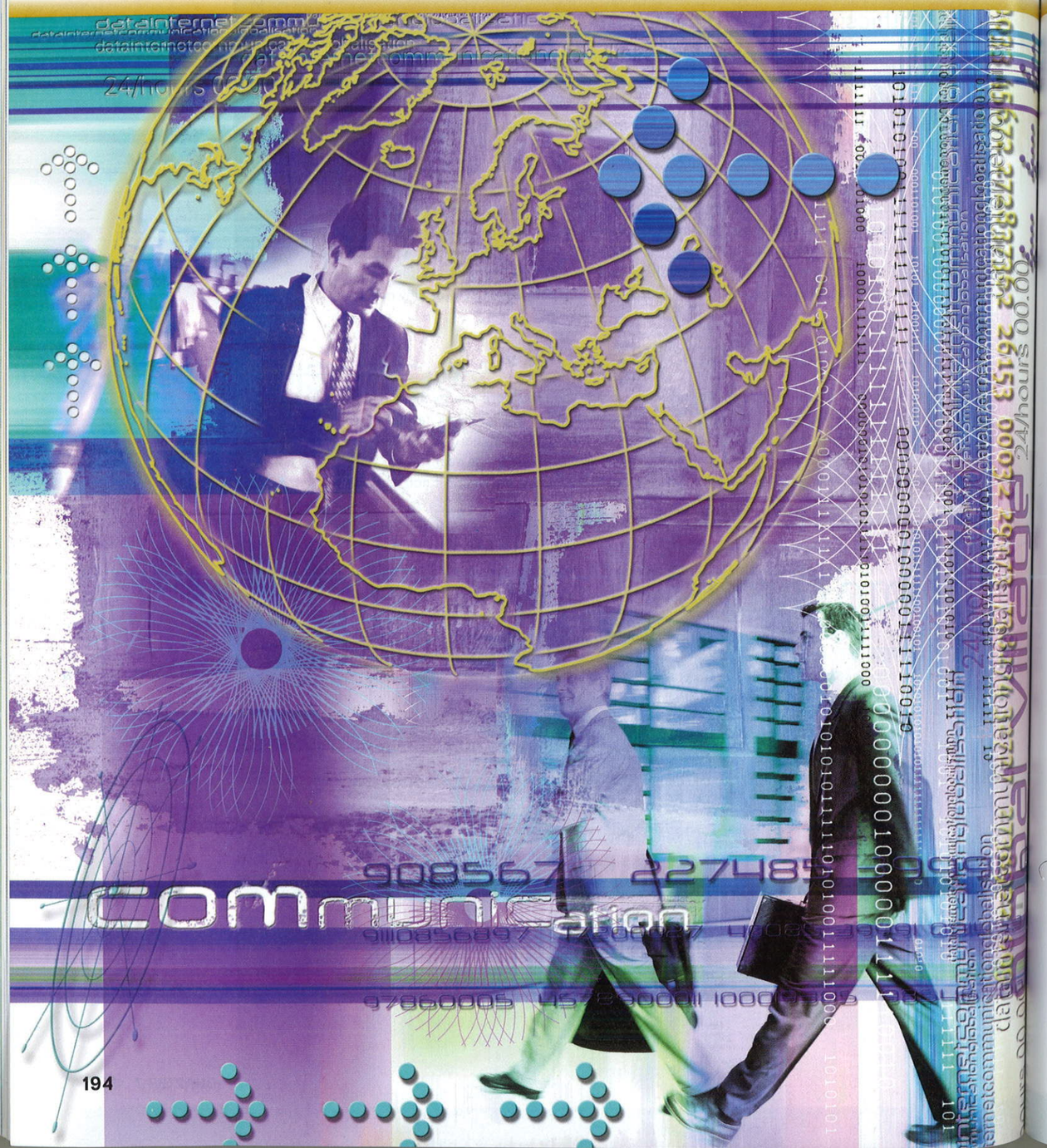
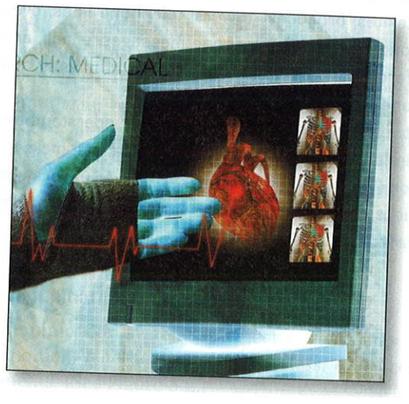
chapter 8

Communications and Networks



Why should I read this chapter?



Communication networks are the backbone of nearly every aspect of modern digital life. In the future, telepresence (the ability to fully experience the reality of a different place without actually being there) will be commonplace. For example, doctors will routinely perform surgery on patients located halfway around the world!

This chapter covers the things you need to know to be prepared for this ever-changing digital world, including:

- Wired networks—learn about coaxial and fiber-optic cables so you can make smart decisions about home Internet connections.
- Wireless networks—use your digital devices in smarter and safer ways by understanding Wi-Fi, satellites and Bluetooth.
- Mobile computing—become a digital road warrior using 4G data networks and GPS.

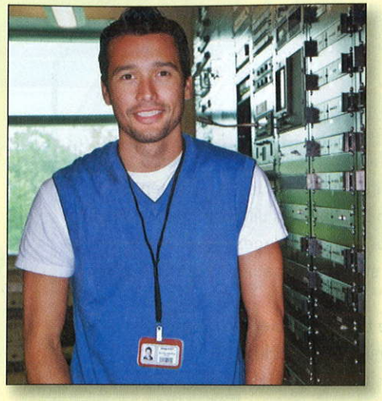
Learning Objectives

After you have read this chapter, you should be able to:

1. Explain connectivity, the wireless revolution, and communication systems.
2. Describe physical and wireless communication channels.
3. Differentiate between connection devices and services including dial-up, DSL, cable, satellite, and cellular.
4. Describe data transmission factors, including bandwidth and protocols.
5. Define networks and key network terminology including network interface cards and network operating systems.
6. Describe different types of networks, including local, home, wireless, personal, metropolitan, and wide area networks.
7. Describe network architectures, including topologies and strategies.
8. Explain the organization issues related to Internet technologies and network security.

Introduction

"Hi, I'm Michael, and I'm a network administrator. I'd like to talk with you about computer communications and networks. I'd also like to talk about technologies that support mobile computing including global positioning systems, Wi-Fi, and 3G and 4G networks."



We live in a truly connected society. We can communicate almost instantaneously with others worldwide; changing events from the smallest of countries and places are immediately broadcast to the world; our e-mail messages are delivered to handheld devices; cars access the Internet to receive driving instructions and solve mechanical problems. Even household appliances can connect to the Internet and be remotely controlled. The communications and information options we have at our fingertips have changed how we react and relate to the world around us.

As the power and flexibility of our communication systems have expanded, the sophistication of the networks that support these systems has become increasingly critical and complex. The network technologies that handle our cellular, business, and Internet communications come in many different forms. Satellites, broadcast towers, telephone lines, even buried cables and fiber optics carry our telephone messages, e-mail, and text messages. These different networks must be able to efficiently and effectively integrate with one another.

To efficiently and effectively use computers, you need to understand the concept of connectivity, wireless networking, and the elements that make up network and communications systems. Additionally, you need to understand the basics of communications channels, connection devices, data transmission, network types, network architectures, and organizational networks.

Communications

Computer communications is the process of sharing data, programs, and information between two or more computers. We have discussed numerous applications that depend on communication systems, including

- **E-mail**—provides a fast, efficient alternative to traditional mail by sending and receiving electronic documents.
- **Texting**—provides very efficient direct text communication between individuals using short electronic messages.
- **Videoconferencing**—provides a very-low-cost alternative to long-distance telephone calls using electronic voice and video delivery.
- **Electronic commerce**—buying and selling goods electronically.

In this chapter, we will focus on the communication systems that support these and many other applications. Connectivity, the wireless revolution, and communication systems are key concepts and technologies for the 21st century.

Connectivity

Connectivity is a concept related to using computer networks to link people and resources. For example, connectivity means that you can connect your personal computer to other computers and information sources almost anywhere. With this connection, you are linked to the world of larger computers and the Internet. This includes hundreds of thousands of web servers and their extensive information resources. Thus, being able to efficiently and effectively use computers becomes a matter of knowing not only about connectivity through networks to personal computers but also about larger computer systems and their information resources.

The Wireless Revolution

The single most dramatic change in connectivity and communications in the past decade has been the widespread use of mobile devices like smartphones and tablets with wireless Internet connectivity. Students, parents, teachers, businesspeople, and others routinely talk and communicate with these devices. It is estimated that over 1.5 billion smartphones are in use worldwide. This wireless technology allows individuals to stay connected with one another from almost anywhere at any time.

Figure 8-1 **Wireless revolution**

So what's the revolution? While wireless technology was originally used primarily for voice communications, today's mobile computers support e-mail, web access, social networking, and a variety of Internet applications. In addition, wireless technology allows a wide variety of nearby devices to communicate with one another without any physical connection. Wireless communications allows you to share a high-speed printer, share data files, and collaborate on working documents with a nearby co-worker without having your computers connected by cables or telephone. High-speed Internet wireless technology allows individuals to connect to the Internet and share information from almost anywhere in the world. (See Figure 8-1.) But is it a revolution? Most experts say yes and that the revolution is just beginning.

Communication Systems

Communication systems are electronic systems that transmit data from one location to another. Whether wired or wireless, every communication system has four basic elements. (See Figure 8-2.)

- **Sending and receiving devices.** These are often a computer or specialized communication device. They originate (send) as well as accept (receive) messages in the form of data, information, and/or instructions.
- **Connection devices.** These devices act as an interface between the sending and receiving devices and the communication channel. They convert outgoing messages into packets that can travel across the communication channel. They also reverse the process for incoming messages.

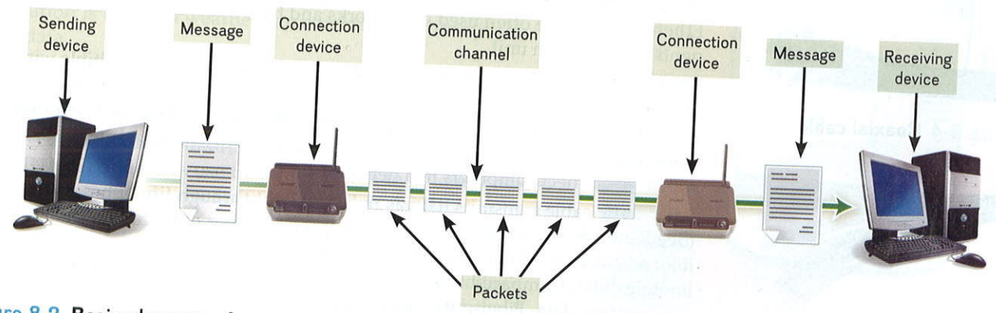


Figure 8-2 **Basic elements of a communication system**

ethics

As eavesdropping tools become more sophisticated, there is concern that law enforcement and government agencies will monitor everyone's Internet and cell phone activity. In the private sector, companies are increasingly using network tools and software to monitor the activity of their employees. Many websites also track your activity, and government officials have often requested these records during the course of an investigation. Some believe that it is unethical for government and businesses to engage in such monitoring and tracking. Do you agree?

- **Data transmission specifications.** These are rules and procedures that coordinate the sending and receiving devices by precisely defining how the message will be sent across the communication channel.
- **Communication channel.** This is the actual connecting or transmission medium that carries the message. This medium can be a physical wire or cable, or it can be wireless.

For example, if you wanted to send an e-mail to a friend, you could create and send the message using your computer, the *sending device.* Your modem, a *connection device,* would modify and format the message so that it could travel efficiently across *communication channels,* such as telephone lines. The specifics describing how the message is modified, reformatted, and sent would be described in the *data transmission specifications.* After your message traveled across the channel, the receiver's modem, a connection device, would reformat it so that it could be displayed on your friend's computer, the *receiving device.* (Note: This example presents the basic communication system elements involved in sending e-mail. It does not and is not intended to demonstrate all the specific steps and equipment involved in an e-mail delivery system.)

concept check

- Define computer communications and connectivity.
- What is the wireless revolution?
- Describe the four elements of every communication system.

Communication Channels

Communication channels are an essential element of every communication system. These channels actually carry the data from one computer to another. There are two categories of communication channels. One category connects sending and receiving devices by providing a physical connection, such as a wire or cable. The other category is wireless.

Figure 8-3 **Ethernet cable**

Figure 8-4 **Coaxial cable**

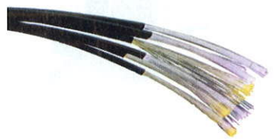


Figure 8-5 **Fiber-optic cable**

Physical Connections

Physical connections use a solid medium to connect sending and receiving devices. These connections include twisted-pair, coaxial, and fiber-optic cables.

- **Twisted-pair cable** consists of pairs of copper wire that are twisted together. Both standard **telephone lines** and **Ethernet cables** use twisted pair. (See Figure 8-3.) Ethernet cables are often used in networks and to connect a variety of components to the system unit.
- **Coaxial cable,** a high-frequency transmission cable, replaces the multiple wires of telephone lines with a single solid-copper core. (See Figure 8-4.) In terms of the number of telephone connections, a coaxial cable has over 80 times the transmission capacity of twisted pair. Coaxial cable is used to deliver television signals as well as to connect computers in a network.
- **Fiber-optic cable** transmits data as pulses of light through tiny tubes of glass. (See Figure 8-5.) The data transmission speeds of fiber-optic cables are incredible; recently speeds of 1 petabit per second were measured (a petabit is 1 million gigabits). Compared to coaxial cable, it is lighter, faster, and more reliable at transmitting data. Fiber-optic cable is rapidly replacing twisted-pair cable telephone lines.

Wireless Connections

Wireless connections do not use a solid substance to connect sending and receiving devices. Rather, they move data through the air.

Most wireless connections use radio waves to communicate. For example, smartphones and many other Internet-enabled devices use radio waves to place telephone calls and to connect to the Internet. Primary technologies used for wireless connections are Bluetooth, Wi-Fi, microwave, WiMax, cellular, and satellite connections.

Standard	Maximum speed
802.11g	54 Mbps
802.11n	600 Mbps
802.11ac	2.6 Gbps
802.11ax	10.5 Gbps

Figure 8-6 **Wi-Fi standards**

- **Bluetooth** is a short-range radio communication standard that transmits data over short distances of up to approximately 33 feet. Bluetooth is widely used for wireless headsets, printer connections, and handheld devices.
- **Wi-Fi (wireless fidelity)** uses high-frequency radio signals to transmit data. A number of standards for Wi-Fi exist, and each can send and receive data at a different speed. (See Figure 8-6.) Most home and business wireless networks use Wi-Fi.
- **Microwave** communication uses high-frequency radio waves. It is sometimes referred to as line-of-sight communication because microwaves can only travel in a straight line. Because the waves cannot bend with the curvature of the earth, they can be transmitted only over relatively short distances. Thus, microwave is a good medium for sending data between buildings in a city or on a large college campus. For longer distances, the waves must be relayed by means of microwave stations with microwave dishes or antennas. (See Figure 8-7.)
- **WiMax (Worldwide Interoperability for Microwave Access)** is a new standard that extends the range of Wi-Fi networks using microwave connections. WiMax is commonly used by universities and others to extend the capability of existing Wi-Fi networks.
- **Cellular** communication uses multiple antennae **(cell towers)** to send and receive data within relatively small geographic regions **(cells).** Most cell phones and mobile devices use cellular networks.
- **Satellite** communication uses satellites orbiting about 22,000 miles above the earth as microwave relay stations. Many of these are offered by Intelsat, the International Telecommunications Satellite Consortium, which is owned by 114 governments and forms a worldwide communication system. Satellites orbit at a precise point and speed above the earth. They can amplify and relay microwave signals from one transmitter on the ground to another. Satellites can be used to send and receive large volumes of data. **Uplink** is a term relating to sending data to a satellite. **Downlink** refers to receiving data from a satellite. The major drawback to satellite communication is that bad weather can sometimes interrupt the flow of data.

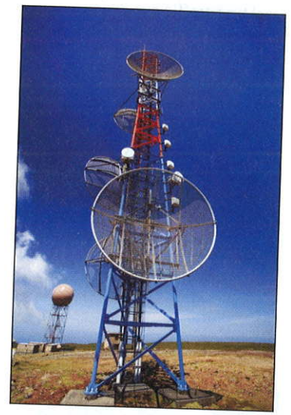


Figure 8-7 **Microwave dish**

One of the most interesting applications of satellite communications is for global positioning. A network of satellites owned and managed by the Department of Defense continuously sends location information to earth. **Global positioning system (GPS)** devices use that information to uniquely determine the geographic location of the device. Available in many automobiles to provide navigational support, these systems are often mounted into the dash with a monitor to display maps and speakers to provide spoken directions. Most of today's smartphones and tablets use GPS technology for handheld navigation. (See Figure 8-8.)

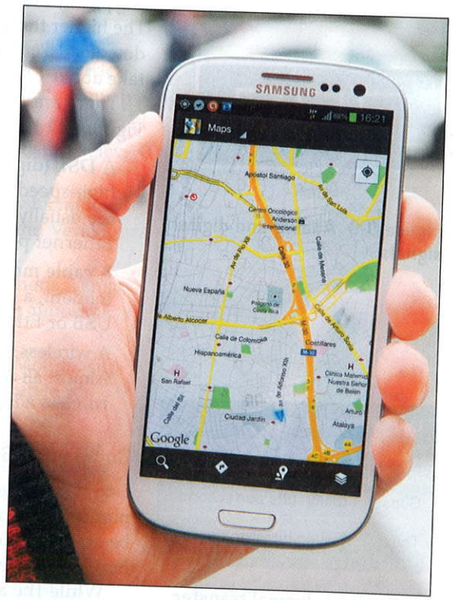


Figure 8-8 **GPS navigation**

environment

Did you know that GPS technology might help protect the environment? Many cars and mobile devices now have GPS capabilities, and these tools can help save fuel by providing drivers with the shortest route to a destination. Most devices now provide real-time traffic avoidance data, which will reduce the carbon emissions and pollution of cars stuck in traffic. By finding the best routes and avoiding congested areas, you can maximize your fuel efficiency and help protect the environment.

Unlike radio waves, **infrared** uses infrared light waves to communicate over short distances. Like microwave transmissions, infrared is a line-of-sight communication. Because light waves can only travel in a straight line, sending and receiving devices must be in clear view of one another without any obstructions blocking that view. One of the most common infrared devices is the TV remote control.

concept check

- What are communication channels? List three physical connections.
- What is Bluetooth? Wi-Fi? Microwave communication? WiMax?
- What are cellular and satellite communications? GPS? Infrared?

Connection Devices

At one time nearly all computer communication used telephone lines. However, because the telephone was originally designed for voice transmission, telephones typically send and receive **analog signals,** which are continuous electronic waves. Computers, in contrast, send and receive **digital signals.** (See Figure 8-9.) These represent the presence or absence of an electronic pulse—the on/off binary signals we mentioned in Chapter 5. To convert the digital signals to analog signals and vice versa, you need a modem.

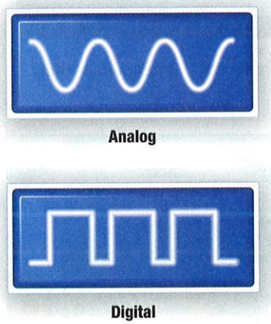


Figure 8-9 **Analog and digital signals**

Modems

The word **modem** is short for *modulator-demodulator.* **Modulation** is the name of the process of converting from digital to analog. **Demodulation** is the process of converting from analog to digital. The modem enables digital personal computers to communicate across different media, including telephone wires, cable lines, and radio waves.

The speed with which modems transmit data varies. This speed, called **transfer rate,** is typically measured in millions of bits **(megabits) per second (Mbps).** (See Figure 8-10.) The higher the speed, the faster you can send and receive information. For example, to download a complete full-length motion picture (700 MB) on a 1.5-Mbps modem would take about 1 hour. Using a 10.0-Mbps modem would take about 9 minutes.

There are three commonly used types of modems: DSL, cable, and wireless. (See Figure 8-11.)

- A **DSL (digital subscriber line)** modem uses standard phone lines to create a high-speed connection directly to your phone company's offices. These devices are usually external and connect to the system unit using either a USB or an Ethernet port.
- A **cable modem** uses the same coaxial cable as your television. Like a DSL modem, a cable modem creates high-speed connections using the system unit's USB or Ethernet port.
- A **wireless modem** is also known as a **WWAN (wireless wide area network) modem.** Almost all computers today have built-in wireless modems. For those that do not, wireless adapter cards are available that plug into USB or special card ports.

Unit	Speed
Mbps	Million bits per second
Gbps	Billion bits per second
Tbps	Trillion bits per second

Figure 8-10 **Typical transfer rates**

Connection Service

For years, large corporations have been leasing special high-speed lines from telephone companies. Originally, these were copper lines, known as **T1** lines, that could be combined to form higher-capacity options known as **T3** or **DS3** lines. These lines have largely been replaced by faster **optical carrier (OC)** lines.

While the special high-speed lines are too costly for most individuals, Internet service providers (as discussed in Chapter 2) do provide affordable connections.

DSL Cable Wireless

Figure 8-11 **Basic types of modems**

For years, individuals relied on **dial-up services** using existing telephones and telephone modems to connect to the Internet. This type of service has been replaced by higher-speed connection services including DSL, cable, satellite, and cellular services.

- **Digital subscriber line (DSL) service** is provided by telephone companies using existing telephone lines to provide high-speed connections. **ADSL (asymmetric digital subscriber line)** is one of the most widely used types of DSL. DSL is much faster than dial-up.
- **Cable service** is provided by cable television companies using their existing television cables. These connections are usually faster than DSL.
- **Fiber-optic service (FiOS)** is showing up in some areas, but it is a new technology and not widely available. Current providers of FiOS include Google and Verizon with speeds faster than cable or DSL connections.
- **Satellite connection services** use satellites to provide wireless connections. While slower than DSL and cable modem, satellite connections are available almost anywhere using a satellite-receiving disk.
- **Cellular service providers,** including Verizon, AT&T, Sprint, and T-Mobile, support voice and data transmission to wireless devices using cellular networks. These networks have gone through different generations. **First-generation mobile telecommunications (1G)** started in the 1980s using analog radio signals to provide analog voice transmission service. **Second-generation mobile telecommunications (2G)** started in the 1990s using digital radio signals. **Third-generation mobile telecommunications (3G)** started in the 2000s and provided services capable of effective connectivity to the Internet, marking the beginning of smartphones.

  Fourth-generation mobile telecommunications (4G) has begun to replace 3G networks in some areas with providers using **LTE (Long Term Evolution)**

connections to provide faster transmission speeds. While a user's experience with 4G will depend on several factors, including carrier, geography, and proximity to cell towers, 4G technologies can provide speeds up to 10 times faster than 3G.

To learn more about how you can use mobile communications, see Making IT Work for You: Mobile Internet on page 203.

concept check

- What is the function of a modem? Compare the three types of modems.
- What is a connection service? Compare the five high-speed connection services.
- Describe the four generations of mobile communications.

Data Transmission

Several factors affect how data is transmitted. These factors include bandwidth and protocols.

Bandwidth

Bandwidth is a measurement of the width or capacity of the communication channel. Effectively, it means how much information can move across the communication channel in a given amount of time. For example, to transmit text documents, a slow bandwidth would be acceptable. However, to effectively transmit video and audio, a wider bandwidth is required. There are four categories of bandwidth.

- **Voiceband,** also known as **low bandwidth,** is used for standard telephone communication. Personal computers with telephone modems and dial-up service use this bandwidth. While effective for transmitting text documents, it is too slow for many types of transmission, including high-quality audio and video.
- **Medium band** is used in special leased lines to connect midrange computers and mainframes as well as to transmit data over long distances. This bandwidth is capable of very-high-speed data transfer.
- **Broadband** is widely used for DSL, cable, and satellite connections to the Internet. Several users can simultaneously use a single broadband connection for high-speed data transfer.
- **Baseband** is widely used to connect individual computers that are located close to one another. Like broadband, it is able to support high-speed transmission. Unlike broadband, however, baseband can only carry a single signal at a time.

Protocols

For data transmission to be successful, sending and receiving devices must follow a set of communication rules for the exchange of information. These rules for exchanging data between computers are known as **protocols.**

As discussed in Chapter 2, **https,** or **hypertext transfer protocol secure,** is widely used to protect the transfer of sensitive information. Another widely used Internet protocol is **TCP/IP (transmission control protocol/Internet protocol).** The essential features of this protocol involve (1) identifying sending and receiving devices

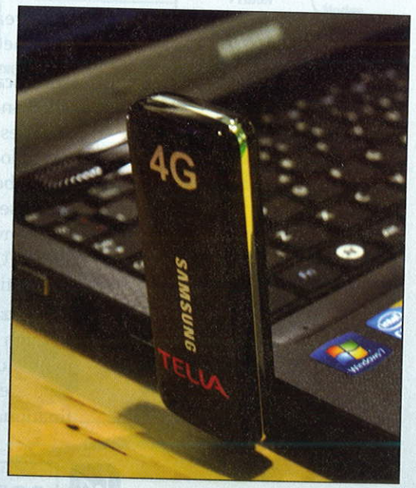
Making IT work for you

MOBILE INTERNET

Is your smartphone or tablet always connected to the Internet? Millions have this always-on connection to access their e-mail, favorite websites, cloud services, and apps from anywhere at any time. What can be confusing to many is the variety of connection devices, data plans, and penalties for exceeding usage limits.

Devices There are many devices that can help you get Internet access from wherever you are.

1. ***Smartphones.*** **Most modern smartphones are capable of accessing the Internet via Wi-Fi and 3G or 4G networks.**
2. ***Tablets.*** **Most tablets will provide Wi-Fi access, but to get 3G or 4G capabilities, you will generally have to purchase a higher-priced model.**
3. ***Laptops.*** **By inserting a USB modem, almost all laptops can access the Internet through a 3G or 4G network.**
4. ***Mobile hotspot device.*** **This is a stand-alone device that connects to a 3G or 4G network. It will then allow multiple devices near it to access the Internet via a Wi-Fi connection.**



Many smartphones can provide Wi-Fi sharing, or tethering, like a mobile hotspot device. However, you may have to pay an additional monthly fee.

Data Plans A data plan defines how much data you can download using your 3G or 4G connection. These plans can be very confusing, but for most individuals, the plan that gives you a few gigabytes per month is best. Although a few providers have unlimited data plans, they may slow down, or throttle, your connection speed significantly if they deem that your usage is excessive.

Overage Charges If you exceed the monthly data limit, wireless providers will start charging overage fees. For example, one provider charges $10 for every extra gigabyte used. To minimize overage charges, consider the following:

1. ***Wi-Fi access points.*** **Whenever possible, use a Wi-Fi connection. These connections are not subject to your data plan limits. So if you are in a coffee shop that offers free Wi-Fi, use it!**
2. ***Streaming music/video.*** **Streaming too much of any media can quickly become a problem. The solution: Be selective when watching TV shows, movies, and YouTube videos, and try to store some of your music on your device.**
3. ***Downloading.*** **Limit your downloading of new apps and music to Wi-Fi connections only. Many programs and MP3 files can reach (or even exceed) a size of 10 MB.**
4. ***Monitor your data usage.*** **Most wireless companies provide a free app that helps you monitor your minutes, text messages, and data. Keep an eye on this.**

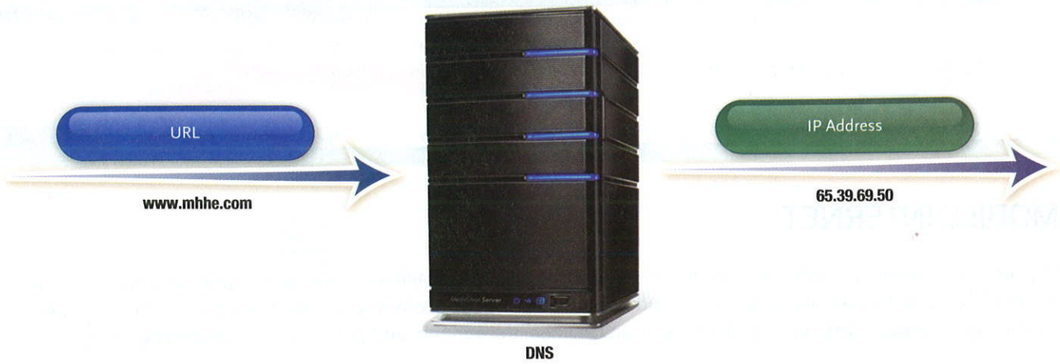


Figure 8-12 **DNS converts text-based addresses to numeric IP addresses**

and (2) breaking information into small parts, or packets, for transmission across the Internet.

- **Identification:** Every computer on the Internet has a unique numeric address called an **IP address (Internet protocol address).** Similar to the way a postal service uses addresses to deliver mail, the Internet uses IP addresses to deliver e-mail and to locate websites. Because these numeric addresses are difficult for people to remember and use, a system was developed to automatically convert text-based addresses to numeric IP addresses. This system uses a **domain name server (DNS)** that converts text-based addresses to IP addresses. For example, whenever you enter a URL, say www.mhhe.com, a DNS converts this to an IP address before a connection can be made. (See Figure 8-12.)
- **Packetization:** Information sent or transmitted across the Internet usually travels through numerous interconnected networks. Before the message is sent, it is reformatted or broken down into small parts called **packets.** Each packet is then sent separately over the Internet, possibly traveling different routes to one common destination. At the receiving end, the packets are reassembled into the correct order.

concept check

- What is bandwidth? Describe the four categories.
- What are protocols? What is the standard protocol for the Internet?
- Define TCP/IP, IP address, and packets.

Networks

A **computer network** is a communication system that connects two or more computers so that they can exchange information and share resources. Networks can be set up in different arrangements to suit users' needs. (See Figure 8-13.)

Terms

There are a number of specialized terms that describe computer networks. These terms include

- **Node**—any device that is connected to a network. It could be a computer, printer, or data storage device.

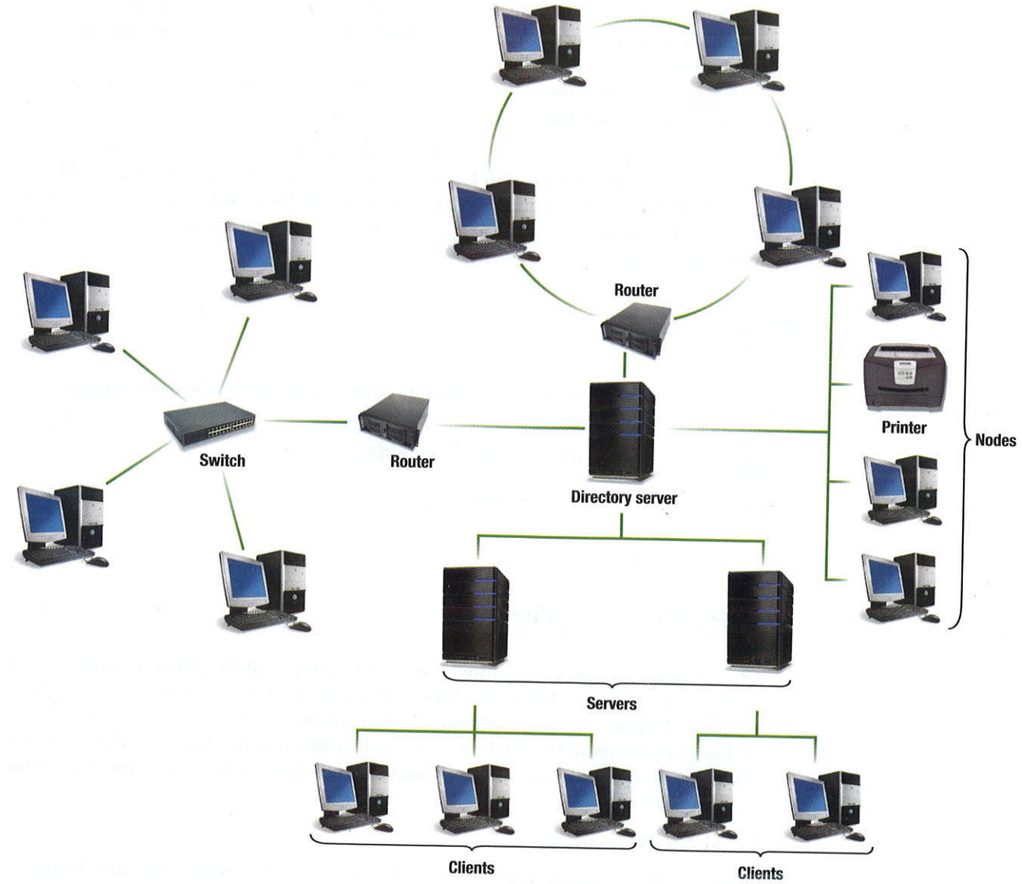


Figure 8-13 **Computer network**

- **Client**—a node that requests and uses resources available from other nodes. Typically, a client is a user's personal computer.
- **Server**—a node that shares resources with other nodes. Dedicated servers specialize in performing specific tasks. Depending on the specific task, they may be called an application server, communication server, database server, file server, printer server, or web server.
- **Directory server**—a specialized server that manages resources, such as user accounts, for an entire network.
- **Host**—any computer system connected to a network that provides access to its resources.
- **Router**—a node that forwards or routes data packets from one network to their destination in another network.
- **Switch**—central node that coordinates the flow of data by sending messages directly between sender and receiver nodes. A **hub** previously filled this purpose by sending a received message to all connected nodes, rather than just the intended node.
- **Network interface cards (NIC)**—as discussed in Chapter 5, these are expansion cards located within the system unit that connect the computer to a network. Sometimes referred to as a LAN adapter.

- **Network operating systems (NOS)**—control and coordinate the activities of all computers and other devices on a network. These activities include electronic communication and the sharing of information and resources.
- **Network administrator**—a computer specialist responsible for efficient network operations and implementation of new networks.

A network may consist only of personal computers, or it may integrate personal computers or other devices with larger computers. Networks can be controlled by all nodes working together equally or by specialized nodes coordinating and supplying all resources. Networks may be simple or complex, self-contained or dispersed over a large geographic area.

concept check

What is a computer network? What are nodes, clients, servers, directory servers, hosts, routers, and switches?

What is the function of an NIC and an NOS?

What is a network administrator?

Network Types

Clearly, different types of channels—wired or wireless—allow different kinds of networks to be formed. Telephone lines, for instance, may connect communications equipment within the same building or within a home. Networks also may be citywide and even international, using both cable and wireless connections. Local area, metropolitan area, and wide area networks are distinguished by the size of the geographic area they serve.

Local Area Networks

Networks with nodes that are in close physical proximity—within the same building, for instance—are called **local area networks (LANs).** Typically, LANs span distances less than a mile and are owned and operated by individual organizations. LANs are widely used by colleges, universities, and other types of organizations to link personal computers and to share printers and other resources. For a simple LAN, see Figure 8-14.

The LAN represented in Figure 8-14 is a typical arrangement and provides two benefits: economy and flexibility. People can share costly equipment. For instance, the four personal computers share the high-speed laser printer and the file server, which are expensive pieces of hardware. Other equipment or nodes also may be added to the LAN—for instance, more personal computers, a mainframe computer, or optical disc storage devices. Additionally, the **network gateway** is a device that allows one LAN to be linked to other LANs or to larger networks. For example, the LAN of one office group may be connected to the LAN of another office group.

There are a variety of different standards or ways in which nodes can be connected to one another and ways in which their communications are controlled in a LAN. The most common standard is known as **Ethernet.** LANs using this standard are sometimes referred to as Ethernet LANs.

Home Networks

While LANs have been widely used within organizations for years, they are now being commonly used by individuals in their homes and apartments. These LANs, called

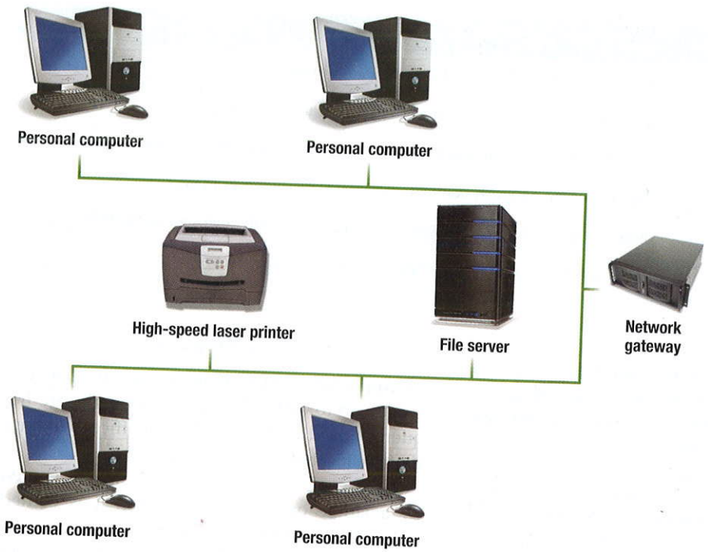


Figure 8-14 Local area network

home networks, allow different computers to share resources, including a common Internet connection. Computers can be connected in a variety of ways, including electrical wiring, telephone wiring, and special cables. One of the simplest ways, however, is without cables, or wireless.

Figure 8-15 Wireless adapter

Wireless LAN

A wireless local area network is typically referred to as a **wireless LAN (WLAN).** It uses radio frequencies to connect computers and other devices. All communications pass through the network's centrally located **wireless access point** or **base station.** This access point interprets incoming radio frequencies and routes communications to the appropriate devices.

Wireless access points that provide Internet access are widely available in public places such as coffee shops, libraries, bookstores, colleges, and universities. These access points are known as **hotspots** and typically use Wi-Fi technology. Many of these services are free and easy to find using free locator sites such as www.hotspot-locations.com. Most mobile computing devices have an internal wireless network card to connect to hotspots. If your mobile device does not have an internal wireless network card, you can use an external wireless adapter (see Figure 8-15) that plugs into your computer's USB port or PC card slot.

Personal Area Network

A **personal area network (PAN)** is a type of wireless network that works within a very small area—your immediate surroundings. PANs connect cell phones to headsets, keyboards to cell phones, and so on. These networks make it possible for wireless devices to interact with each other. The most popular PAN technology is Bluetooth, with a maximum range of around 33 feet. Virtually all wireless peripheral devices available today use Bluetooth, including the controllers on popular game systems like the PlayStation and Wii.

Type	Description
LAN	Local area network; located within close proximity
Home	Local area network for home and apartment use; typically wireless
WLAN	Wireless local area network; all communication passes through access point
PAN	Personal area network; connects digital devices, such as PDAs
MAN	Metropolitan area network; typically spans cities with coverage up to 100 miles
WAN	Wide area network for countrywide or worldwide coverage

Figure 8-16 Types of networks

tips **Do you use your laptop to connect to wireless networks at school or in public places such as coffee shops, airports, or hotels? If so, it is important to use caution to protect your computer and your privacy. Here are a few suggestions:**

1. **Use a firewall.** A personal firewall is essential when connecting your computer directly to public networks. Some firewalls, such as the one built into Windows 8 and Windows 10, will ask whether a new network should be treated as home, work, or a public network.
2. **Avoid fake hotspots.** Thieves are known to set up rogue (or fake) hotspots in popular areas where users expect free Wi-Fi, such as coffee shops and airports. Since many operating systems automatically connect to the access point with the strongest signal, you could be connecting to the one set up by the thief. Always confirm that you are connecting to the access point of that establishment. Ask an employee if you are unsure.
3. **Turn off file sharing.** Turning off file-sharing features in your operating system will ensure that no one can access or modify your files.
4. **Check if connection is encrypted.** If the hotspot you are using is protected with a password, then it is likely encrypted. If it is not, then be very careful with websites you visit and the information you provide.

Metropolitan Area Networks

Metropolitan area networks (MAN) span distances up to 100 miles. These networks are frequently used as links between office buildings that are located throughout a city.

Unlike a LAN, a MAN is typically not owned by a single organization. Rather, it is owned either by a group of organizations or by a single network service provider that provides network services for a fee.

Wide Area Networks

Wide area networks (WANs) are countrywide and worldwide networks. These networks provide access to regional service (MAN) providers and typically span distances greater than 100 miles. They use microwave relays and satellites to reach users over long distances—for example, from Los Angeles to Paris. Of course, the widest of all WANs is the Internet, which spans the entire globe.

The primary difference between a PAN, LAN, MAN, and WAN is the geographic range. Each may have various combinations of hardware, such as personal computers, midrange computers, mainframes, and various peripheral devices.

For a summary of network types, see Figure 8-16.

concept check

- What is a LAN? Network gateway? Ethernet? Home network?
- What is a wireless network? Wireless access point? Hotspot?
- What is a PAN? MAN? WAN?

Network Architecture

Network architecture describes how a network is arranged and how resources are coordinated and shared. It encompasses a variety of different network specifics, including network topologies and strategies. Network topology describes the physical arrangement of the network. Network strategies define how information and resources are shared.

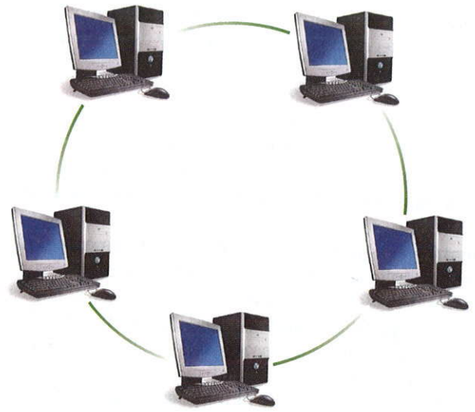


Figure 8-17 Ring network

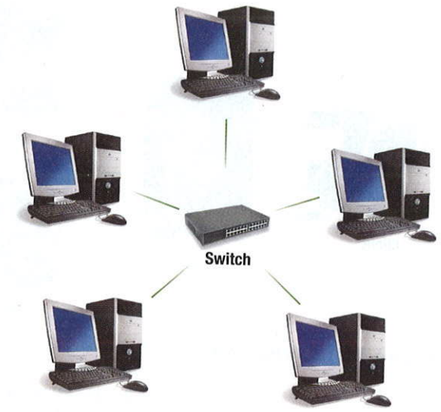


Figure 8-18 Star network

Topologies

A network can be arranged or configured in several different ways. This arrangement is called the network's **topology.** The most common topologies are

- **Bus network**—each device is connected to a common cable called a **bus** or **backbone,** and all communications travel along this bus.
- **Ring network**—each device is connected to two other devices, forming a ring. (See Figure 8-17.) When a message is sent, it is passed around the ring until it reaches the intended destination.
- **Star network**—each device is connected directly to a central network switch. (See Figure 8-18.) Whenever a node sends a message, it is routed to the switch, which then passes the message along to the intended recipient. The star network is the most widely used network topology today. It is applied to a broad range of applications from small networks in the home to very large networks in major corporations.
- **Tree network**—each device is connected to a central node, either directly or through one or more other devices. The central node is connected to two or more subordinate nodes that in turn are connected to other subordinate nodes, and so forth, forming a treelike structure. (See Figure 8-19.) This network, also known as a **hierarchical network,** is often used to share corporatewide data.
- **Mesh network**—this topology is the newest type and does not use a specific physical layout (such as a star or a tree). Rather, the mesh network requires that each node have more than one connection to the other nodes. (See Figure 8-20.) The resulting pattern forms the appearance of a mesh. If a path between two nodes is somehow disrupted, data can be

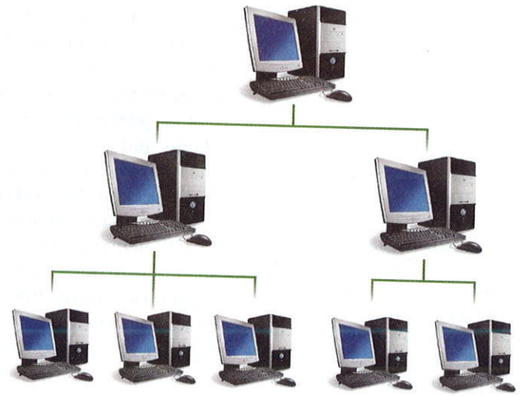


Figure 8-19 Tree network

Figure 8-20 Mesh network

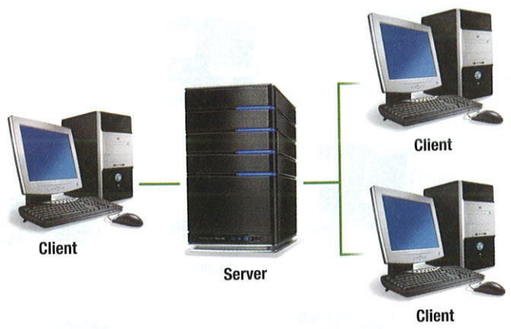


Figure 8-21 Client/server network

automatically rerouted around the failure using another path. Wireless technologies are frequently used to build mesh networks.

Strategies

Every network has a **strategy,** or way of coordinating the sharing of information and resources. Two of the most common network strategies are client/server and peer-to-peer.

Client/server networks use central servers to coordinate and supply services to other nodes on the network. The server provides access to resources such as web pages, databases, application software, and hardware. (See Figure 8-21.) This strategy is based on specialization. Server nodes coordinate and supply specialized services, and client nodes request the services. Commonly used server operating systems are Windows Server, Mac OS X Server, Linux, and Solaris.

Client/server networks are widely used on the Internet. For example, each time you open a web browser, your computer (the client) sends out a request for a specific web page. This request is routed over the Internet to a server. This server locates and sends the requested material back to your computer.

One advantage of the client/server network strategy is the ability to handle very large networks efficiently. Another advantage is the availability of powerful network management software to monitor and control network activities. The major disadvantages are the cost of installation and maintenance.

In a **peer-to-peer (P2P) network,** nodes have equal authority and can act as both clients and servers. The most common way to share games, movies, and music over the Internet is to use a P2P network. For example, special file-sharing software such as BitTorrent can be used to obtain files located on another personal computer and also can provide files to other personal computers.

P2P networks are rapidly growing in popularity as people continue to share information with others around the world. The primary advantage is that they are easy and inexpensive (often free) to set up and use. One disadvantage of P2P networks is the lack of security controls or other common management functions. For this reason, few businesses use this type of network to communicate sensitive information.

concept check

- What is a network topology?
- Compare bus, ring, star, tree, and mesh topologies.
- What is a network strategy?
- Compare client/server and peer-to-peer strategies.

Organizational Networks

Computer networks in organizations have evolved over time. Most large organizations have a complex and wide range of different network configurations, operating systems, and strategies. These organizations face the challenge of making these networks work together effectively and securely.

Internet Technologies

Many organizations today employ Internet technologies to support effective communication within and between organizations using intranets and extranets.

- An **intranet** is a *private* network within an organization that resembles the Internet. Like the *public* Internet, intranets use browsers, websites, and web pages. Typical applications include electronic telephone directories, e-mail addresses, employee benefit information, internal job openings, and much more. Employees find surfing their organizational intranets to be as easy and as intuitive as surfing the Internet.
- An **extranet** is a *private* network that connects *more than one* organization. Many organizations use Internet technologies to allow suppliers and others limited access to their networks. The purpose is to increase efficiency and reduce costs. For example, an automobile manufacturer has hundreds of suppliers for the parts that go into making a car. By having access to the car production schedules, suppliers can schedule and deliver parts as they are needed at the assembly plants. In this way, operational efficiency is maintained by both the manufacturer and the suppliers.

Network Security

Large organizations face the challenge of ensuring that only authorized users have access to network resources, sometimes from multiple geographic locations or across the Internet. Securing large computer networks requires specialized technology. Three technologies commonly used to ensure network security are firewalls, intrusion detection systems, and virtual private networks.

- A **firewall** consists of hardware and software that control access to a company's intranet and other internal networks. Most use software or a special computer called a **proxy server.** All communications between the company's internal networks and the outside world pass through this server. By evaluating the source and the content of each communication, the proxy server decides whether it is safe to let a particular message or file pass into or out of the organization's network. (See Figure 8-22.)
- **Intrusion detection systems (IDS)** work with firewalls to protect an organization's network. These systems use sophisticated statistical techniques to analyze all incoming and outgoing network traffic. Using advanced pattern matching and heuristics, an IDS can recognize signs of a network attack and disable access before an intruder can do damage.
- **Virtual private networks (VPN)** create a secure private connection between a remote user and an organization's internal network. Special VPN protocols create the equivalent of a dedicated line between a user's home or laptop computer and a company server. The connection is heavily encrypted, and, from the perspective of the user, it appears that the workstation is actually located on the corporate network.

Like organizations, end users have security challenges and concerns. We need to be concerned about the privacy of our personal information. In the next chapter, we will discuss personal firewalls and other ways to protect personal privacy and security.

concept check

- What are Internet technologies? Compare intranets and extranets.
- What is a firewall? What is a proxy server?
- What are intrusion detection systems?
- What are virtual private networks?

privacy

Did you know that right now, people are attempting to access private networks that hold your private records and correspondence? Some individuals and governments are continually attempting to gain unauthorized access to networks and to obtain information stored on computers on those networks. Sometimes the objective is simply to create mischief; other times, to steal information or to test the security of a network. While some would say that any type of unauthorized intrusion is an unacceptable violation of privacy, others would say that under certain circumstances (such as homeland security), these intrusions can be essential.

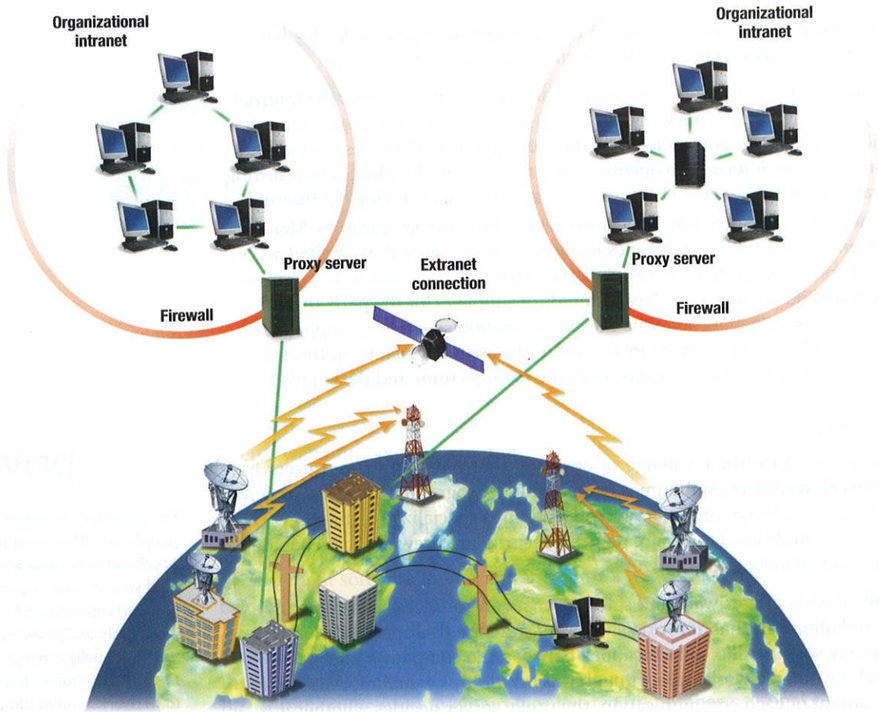
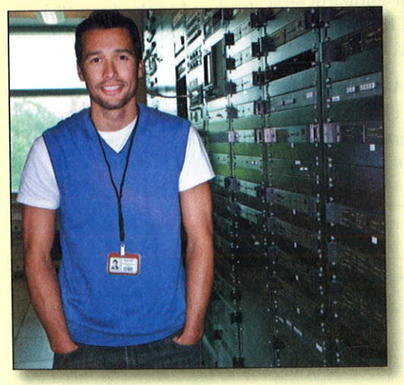


Figure 8-22 **Intranets, extranets, firewalls, and proxy servers**

Careers in IT

"Now that you have learned about computer communications and networks, let me tell you about my career as a network administrator."



Network administrators manage a company's LAN and WAN networks. They may be responsible for design, implementation, and maintenance of networks. Duties usually include maintenance of both hardware and software related to a company's intranet and Internet networks. Network administrators are typically responsible for diagnosing and repairing problems with these networks. Some network administrators' duties include planning and implementation of network security as well.

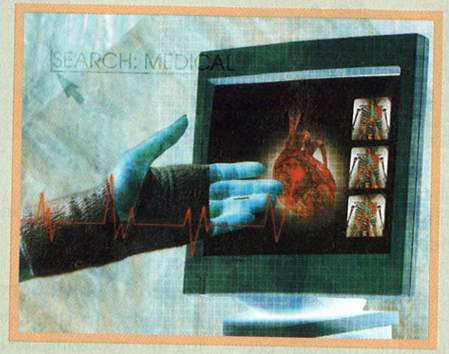
Employers typically look for candidates with a bachelor's or an associate's degree in computer science, computer technology, or information systems as well as practical networking experience. Experience with network security and maintenance is preferred. Also technical certification may be helpful in obtaining this position. Because network administrators are involved directly with people in many departments, good communication skills are essential.

Network administrators can expect to earn an annual salary of $47,000 to $64,000. Opportunities for advancement typically include upper-management positions. This position is expected to be among the fastest-growing jobs in the near future.

A LOOK TO THE FUTURE

Telepresence Lets You Be There without Actually Being There

How would you like to speak with distant friends or family as though they were in the same room at the touch of a button? Can you imagine receiving a physical examination from a doctor thousands of miles away? All this and more could be possible in the future thanks to the emerging technology known as telepresence. Telepresence can be considered the natural evolution of the phone call, from the analog telephone to the digital video chats of today. In the future, telepresence robots will allow video, audio, and manipulation of real-world objects. Technology has been making better telepresence, and will continue to evolve to improve our lives as we look to the future.



Telepresence seeks to create the illusion that you are actually at a remote location, seeing, hearing, and, someday maybe, even feeling as though you were really there. Today's early implementations, such as Cisco TelePresence, mainly focus on an extension of videoconferencing, allowing people in different locations to conduct meetings as though they are sitting across a table from one another. This illusion is created with very high-definition video, acoustically tuned audio systems, and high-speed networks. However, telepresence could someday go beyond the simple voice and videoconferencing available today, and the applications seem endless.

Robots are quickly becoming a key part of many telepresence applications. In addition to audio and video feeds from another location, robots will bring you the ability to manipulate objects at the remote location. Such robots are already being used in the medical field. In one system, a surgeon uses special controls and screens in one room to control robotic arms that operate on the patient in another room. This type of system could be used to allow expert surgeons to perform several procedures on various patients located throughout the world in just one day!

In addition to manipulating objects, users may one day wear special gloves and other sensors that permit them to feel the objects being touched by the robot. This technology might be used to allow people to work in hazardous areas or perform search and rescue operations from a safe, remote location. A more casual application may see individuals using telepresence as a substitute for traditional vacations. Imagine touring remote cities or touching objects from a shipwreck on a deep-sea diving expedition without the expense, hassle, or risk of travel.

Various research institutions are currently experiencing breakthroughs in the areas of holography, which is technology that creates 3D images, called holograms, that might pave the way to advanced telepresence. In the coming decade, you might be able to interact virtually with others via a projected, 3D hologram of yourself. How would you use telepresence? What benefits do you see from this technology? How might telepresence affect traveling? Do you see any disadvantages?

VISUAL SUMMARY | Communications and Networks

COMMUNICATIONS

Communications is the process of sharing data, programs, and information between two or more computers. Applications include e-mail, texting, videoconferencing, and electronic commerce.

Connectivity

Connectivity is a concept related to using computer networks to link people and resources. You can link or connect to large computers and the Internet, providing access to extensive information resources.

The Wireless Revolution

Mobile devices like smartphones and tablets have brought dramatic changes in connectivity and communications. These wireless devices are becoming widely used for computer communication.

Communication Systems

Communication systems transmit data from one location to another. There are four basic elements:

- Sending and receiving devices originate or accept messages.
- Connection devices act as an interface between sending and receiving devices and the communication channel.
- Data transmission specifications are rules and procedures for sending and receiving data.
- Communication channel is the actual connecting or transmission medium for messages.

COMMUNICATION CHANNELS

Communication channels carry data from one computer to another.

Physical Connections

Physical connections use a solid medium to connect sending and receiving devices. Connections include **twisted-pair cable (telephone lines** and **Ethernet cables), coaxial cable,** and **fiber-optic cable.**

Wireless Connections

Wireless connections do not use a solid substance to connect devices. Most use radio waves.

- **Bluetooth**—transmits data over short distances; widely used for a variety of wireless devices.
- **Wi-Fi (wireless fidelity)**—uses high-frequency radio signals; most home and business wireless networks use Wi-Fi.
- **Microwave**—line-of-sight communication; used to send data between buildings; longer distances require microwave stations.
- **WiMax (Worldwide Interoperability for Microwave Access)**—extends the range of Wi-Fi networks using microwave connections.
- **Cellular**—uses **cell towers** to send and receive data within relatively small geographic regions or **cells.**
- **Satellite**—uses microwave relay stations; **GPS (global positioning system)** tracks geographic locations.
- **Infrared**—uses light waves over a short distance; line-of-sight communication.

To efficiently and effectively use computers, you need to understand the concepts of connectivity, the wireless revolution, and communication systems. Additionally, you need to know the essential parts of communication technology, including channels, connection devices, data transmission, networks, network architectures, and network types.

CONNECTION DEVICES

Many communication systems use standard telephone lines and **analog signals.** Computers use **digital signals.**

Modems

Modems modulate and **demodulate. Transfer rate** is measured in **megabits per second.** Three types are **DSL, cable,** and **wireless (wireless wide area network, WWAN).**

Connection Service

T1, T3 (DS3), and **OC (optical carrier)** lines provide support for very-high-speed, all-digital transmission for large corporations. More affordable technologies include **dial-up, DSL (digital subscriber line), ADSL** (widely used), **cable, fiber-optic service (FiOS), satellite,** and **cellular services. 4G (fourth-generation mobile telecommunications)** can provide 10 times faster speeds than **3G** using **LTE (Long Term Evolution)** connections.

DATA TRANSMISSION

Bandwidth measures a communication channel's width or capacity. Four bandwidths are **voiceband (low bandwidth), medium band, broadband** (high-capacity transmissions), and **baseband. Protocols** are rules for exchanging data. Widely used Internet protocols include **https** and **TCP/IP. IP addresses (Internet protocol addresses)** are unique numeric Internet addresses. **DNS (domain name server)** converts text-based addresses to and from numeric IP addresses. **Packets** are small parts of messages.

NETWORKS

Computer networks connect two or more computers. Some specialized network terms include

- **Node**—any device connected to a network.
- **Client**—node requesting resources.
- **Server**—node providing resources.
- **Directory server**—specialized node that manages resources.
- **Host**—any computer system that provides access to its resources over a network.
- **Router**—a node that forwards data packets from one network to another network.
- **Switch**—node that coordinates direct flow of data between other nodes. **Hub** is an older device that directed flow to all nodes.
- **NIC (network interface card)**—LAN adapter card for connecting to a network.
- **NOS (network operating system)**—controls and coordinates network operations.
- **Network administrator**—network specialist responsible for network operations.

NETWORK TYPES

Networks can be citywide or even international, using both wired and wireless connections.

- **Local area networks (LANs)** connect nearby devices. **Network gateways** connect networks to one another. **Ethernet** is a LAN standard. These LANs are called Ethernet LANs.
- **Home networks** are LANs used in homes.
- **Wireless LANs (WLANs)** use a **wireless access point (base station)** as a hub. Hotspots provide Internet access in public places.
- **Personal area networks (PANs)** are wireless networks for PDAs, cell phones, and other wireless devices.
- **Metropolitan area networks (MANs)** link office buildings within a city, spanning up to 100 miles.
- **Wide area networks (WANs)** are the largest type. They span states and countries or form worldwide networks. The Internet is the largest wide area network in the world.

NETWORK ARCHITECTURE

Network architecture describes how networks are arranged and resources are shared.

Topologies

A network's **topology** describes the physical arrangement of a network.

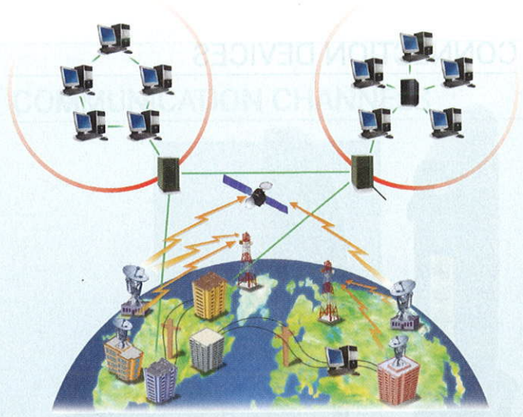
- **Bus network**—each device is connected to a common cable called a **bus** or **backbone.**
- **Ring network**—each device is connected to two other devices, forming a ring.
- **Star network**—each device is connected directly to a central network switch; most common type today.
- **Tree (hierarchical) network**—a central node is connected to subordinate nodes forming a treelike structure.
- **Mesh network**—newest; each node has two or more connecting nodes.

Strategies

Every network has a **strategy,** or way of sharing information and resources. Common network strategies include client/server and peer-to-peer.

- **Client/server (hierarchical) network**—central computers coordinate and supply services to other nodes; based on specialization of nodes; widely used on the Internet; able to handle very large networks efficiently; powerful network management software available.
- **Peer-to-peer network**—nodes have equal authority and act as both clients and servers; widely used to share games, movies, and music over the Internet; easy to set up and use; lacks security controls.

ORGANIZATIONAL NETWORKS



Internet Technologies

Internet technologies support effective communication using intranets and extranets.

- **Intranet**—private network within an organization; uses browsers, websites, and web pages. Typical applications include electronic telephone directories, e-mail addresses, employee benefit information, internal job openings, and much more.
- **Extranet**—like intranet except connects *more than one* organization; typically allows suppliers and others limited access to their networks.

Network Security

Three technologies commonly used to ensure network security are firewalls, intrusion detection systems, and virtual private networks.

- **Firewall**—controls access; all communications pass through **proxy server.**
- **Intrusion detection systems (IDS)**—work with firewalls; use sophisticated statistical techniques to recognize and disable network attacks.
- **Virtual private network (VPN)**—creates secure private connection between remote user and organization's internal network.

CAREERS in IT

Network administrators manage a company's LAN and WAN networks. Bachelor's or associate's degree in computer science, computer technology, or information systems and practical networking experience required. Salary range is $47,000 to $64,000.

KEY TERMS

1G (first-generation mobile telecommunications) (201)
2G (second-generation mobile telecommunications) (201)
3G (third-generation mobile telecommunications) (201)
4G (fourth-generation mobile telecommunications) (201)
analog signal (200)
asymmetric digital subscriber line (ADSL) (201)
backbone (209)
bandwidth (202)
base station (207)
baseband (202)
Bluetooth (199)
broadband (202)
bus (209)
bus network (209)
cable modem (200)
cable service (201)
cellular (199)
cellular service provider (201)
cell (199)
cell tower (199)
client (205)
client/server network (210)
coaxial cable (198)
communication channel (198)
communication system (197)
computer network (204)
connectivity (196)
demodulation (200)
dial-up service (201)
digital signal (200)
digital subscriber line (DSL) (200)
digital subscriber line (DSL) service (201)
directory server (205)
domain name server (DNS) (204)
downlink (199)
DS3 (200)
Ethernet (206)
Ethernet cable (198)
extranet (211)
fiber-optic cable (198)
fiber-optic service (FiOS) (201)
firewall (211)
global positioning system (GPS) (199)
hierarchical network (209)
home network (207)
host (205)
hotspot (207)
https (hypertext transfer protocol secure) (202)
hub (205)
infrared (200)
intranet (211)
intrusion detection system (IDS) (211)
IP address (Internet protocol address) (204)
local area network (LAN) (206)
low bandwidth (202)
LTE (Long Term Evolution) (201)
medium band (202)
megabits per second (Mbps) (200)
mesh network (209)
metropolitan area network (MAN) (208)
microwave (199)
modem (200)
modulation (200)
network administrator (206, 212)
network architecture (208)
network gateway (206)
network interface card (NIC) (205)
network operating system (NOS) (206)
node (204)
optical carrier (OC) (200)
packet (204)
peer-to-peer (P2P) network (210)
personal area network (PAN) (207)
protocol (202)
proxy server (211)
ring network (209)
router (205)
satellite (199)
satellite connection service (201)
server (205)
star network (209)
strategy (210)
switch (205)
T1 (200)
T3 (200)
telephone line (198)
topology (209)
transfer rate (200)
transmission control protocol/Internet protocol (TCP/IP) (202)
tree network (209)
twisted-pair cable (198)
uplink (199)
virtual private network (VPN) (211)
voiceband (202)
wide area network (WAN) (208)
Wi-Fi (wireless fidelity) (199)
WiMax (Worldwide Interoperability for Microwave Access) (199)
wireless access point (207)
wireless LAN (WLAN) (207)
wireless modem (200)
wireless wide area network (WWAN) modem (200)

MULTIPLE CHOICE

Circle the letter of the correct answer.

1. The concept related to using computer networks to link people and resources.
   a. connectivity
   b. GPS
   c. TCP/IP
   d. Wi-Fi

2. A high-frequency transmission cable that delivers television signals as well as connects computers in a network.
   a. coaxial
   b. hi def
   c. 3D
   d. twisted pair

3. A short-range radio communication standard that transmits data over short distances of up to approximately 33 feet.
   a. Bluetooth
   b. broadband
   c. DSL
   d. TCP/IP

4. The speed with which a modem transmits data is called its:
   a. digital velocity
   b. dynamic rate
   c. modular rating
   d. transfer rate

5. The bandwidth typically used for DSL, cable, and satellite connections to the Internet.
   a. baseband
   b. broadband
   c. medium band
   d. voiceband

6. Every computer on the Internet has a unique numeric address called a(n):
   a. IP address
   b. DNS
   c. broadcast
   d. packet

7. Sometimes referred to as a LAN adapter, these expansion cards connect a computer to a network.
   a. PCMCIA
   b. NIC
   c. server
   d. VPN

8. A device that allows one LAN to be linked to other LANs or to larger networks.
   a. IDS
   b. network gateway
   c. PAN
   d. switch

9. Typically using Wi-Fi technology, these wireless access points are available from public places such as coffee shops, libraries, bookstores, colleges, and universities.
   a. hotspots
   b. extranets
   c. PANs
   d. LANs

10. Bus, ring, star, tree, and mesh are five types of network:
    a. topologies
    b. protocols
    c. strategies
    d. devices

MATCHING

Match each numbered item with the most closely related lettered item. Write your answers in the spaces provided.

a. analog
b. bus
c. intrusion detection systems
d. microwave
e. network administrator
f. node
g. peer-to-peer
h. protocols
i. TCP/IP
j. tree

___ 1. Type of network topology in which each device is connected to a common cable called a backbone.
___ 2. A widely used Internet protocol.
___ 3. Uses high-frequency radio waves.
___ 4. Signals that are continuous electronic waves.
___ 5. Rules for exchanging data between computers.
___ 6. Any device that is connected to a network.
___ 7. A computer specialist responsible for efficient network operations and implementation of new networks.
___ 8. This network, also known as a hierarchical network, is often used to share corporatewide data.
___ 9. In this network, nodes have equal authority and can act as both clients and servers.
___ 10. Work with firewalls to protect an organization's network.

OPEN-ENDED

On a separate sheet of paper, respond to each question or statement.

1. Define communications including connectivity, the wireless revolution, and communication systems.
2. Discuss communication channels including physical connections and wireless connections.
3. Discuss connection devices including modems (DSL, cable, and wireless modems) and connection services (DSL, ADSL, cable, satellite, and cellular connection services).
4. Discuss data transmission including bandwidths (voiceband, medium band, broadband, and baseband) as well as protocols (IP addresses, domain name servers, and packetization).
5. Discuss networks by identifying and defining specialized terms that describe computer networks.
6. Discuss network types including local area, home, wireless, personal, metropolitan, and wide area networks.
7. Define network architecture including topologies (bus, ring, star, tree, and mesh) and strategies (client/server and peer-to-peer).
8. Discuss organization networks including Internet technologies (intranets and extranets) and network security (firewalls, proxy servers, intrusion detection systems, and virtual private networks).

DISCUSSION

Respond to each of the following questions.

1 Making IT Work for You: MOBILE INTERNET

Is your smartphone or tablet always connected to the Internet? Review the Making IT Work for You: Mobile Internet on page 203, and then respond to the following: (a) What mobile Internet devices do you currently use? If you do not own any, which device do you feel would be most beneficial to you? (b) Do you currently have a 3G or 4G data plan for your mobile device? If so, provide details on your plan and why you chose it. Otherwise, describe what your ideal data plan would include. (c) Have you, a friend, or a family member ever gone over the data limit and/or been throttled? What sorts of activities are typically responsible for excessive data usage? (d) Go to the websites of at least two wireless companies, and compare their data plans. How are they similar? How are they different?

2 Privacy: UNAUTHORIZED NETWORK INTRUSION

Unauthorized network access is common today. Review the Privacy box on page 211, and then respond to the following: (a) Some argue that some networks must be penetrated and that the loss in privacy is outweighed by other concerns. Others suggest that we have already sacrificed too much privacy. What do you think? Defend your position. (b) Are there any circumstances when unauthorized network access can be justified? Be specific. (c) Is it acceptable for the U.S. government to support unauthorized network access to obtain information about other countries including terrorist activities? (d) Is it acceptable for other countries to attempt to gain unauthorized access to U.S. government networks? Why or why not?

3 Ethics: ELECTRONIC MONITORING

Many companies, websites, and law enforcement and various government agencies engage in monitoring or tracking Internet activity. Review the Ethics box on page 198, and respond to the following: (a) Is it unethical for an organization or corporation to use programs to monitor communications on its network? Why or why not? (b) Is it unethical for a government agency (such as the FBI) to monitor communications on the Internet or gather your records from the websites you visit? Why or why not? (c) Do you feel that new laws are needed to handle these issues? How would you balance the needs of companies and the government with the needs of individuals? Explain your answers.

4 Environment: GPS

Did you know that GPS technology might help protect the environment? Review the Environment box on page 200, and then respond to the following: (a) Identify ways in which GPS could benefit the environment. You need not limit your response to applications in motor vehicles. (b) Have you used a GPS device or mobile navigation app? If so, describe what you used it for. If not, do you think that you will in the near future? (c) Do you think that GPS should be standard equipment for every new car? Why or why not? (d) Do you think that it should be required by law? Why or why not?

PHOTO CREDITS

CHAPTER 8

Opener: © Digital Vision/Punchstock RF; p. 195, 213: © Brand X Pictures/Punchstock RF; p. 196, 212: © Jetta Productions/The Image Bank/Getty Images; 8-1, p. 214 (left): © Alberto Pomares/Getty Images RF; 8-4, 8-5, 8-11 (all), p. 215 (both): © Willis Technology; 8-7, p. 214 (right): © Stuart Gregory/Photodisc/Getty Images RF; 8-8: © Alex Segre/Alamy; p. 203 (top): Holger Motzkau 2010, Wikipedia/Wikimedia Commons; p. 203 (bottom): © 2015 Verizon Wireless; 8-15: © Ilya Starikov/Alamy RF.