LIVING ONLINE

LESSON 25

Network Fundamentals

Estimated Time: 1.5 hours

OBJECTIVES

Upon completion of this domain, you should be able to:

- Describe a network.
- Identify the benefits of a network.
- Evaluate the risks of network computing.
- Identify client/server networks.
- Identify network types.
- Understand network communications.
- Resolve network security issues.

DATA FILES

You do not need data files to complete this lesson.

WORDS TO KNOW

biometric security measure
cable modem
client
client/server network
communications channels
digital subscriber line (DSL)
extranet
firewall
hacker
hub
Internet
intranet
local area network (LAN)
modem
node
peer-to-peer (P2P) network
proxy server
Public Switched Telephone Network (PSTN)
router
server
server operating system
T-1 line
wide area network (WAN)
WiMAX
wireless Internet service provider (WISP)
wireless LAN (WLAN)

As companies grow and purchase more computers, they often find it advantageous to connect those computers through a network, a group of two or more computers linked together. This setup allows users to share software and hardware such as printers, scanners, and other devices. In addition to using a local network, organizations use more far-reaching networks to connect to employees, suppliers, and customers nationally and even internationally. The locations can be in the same city or in different locations all over the world.

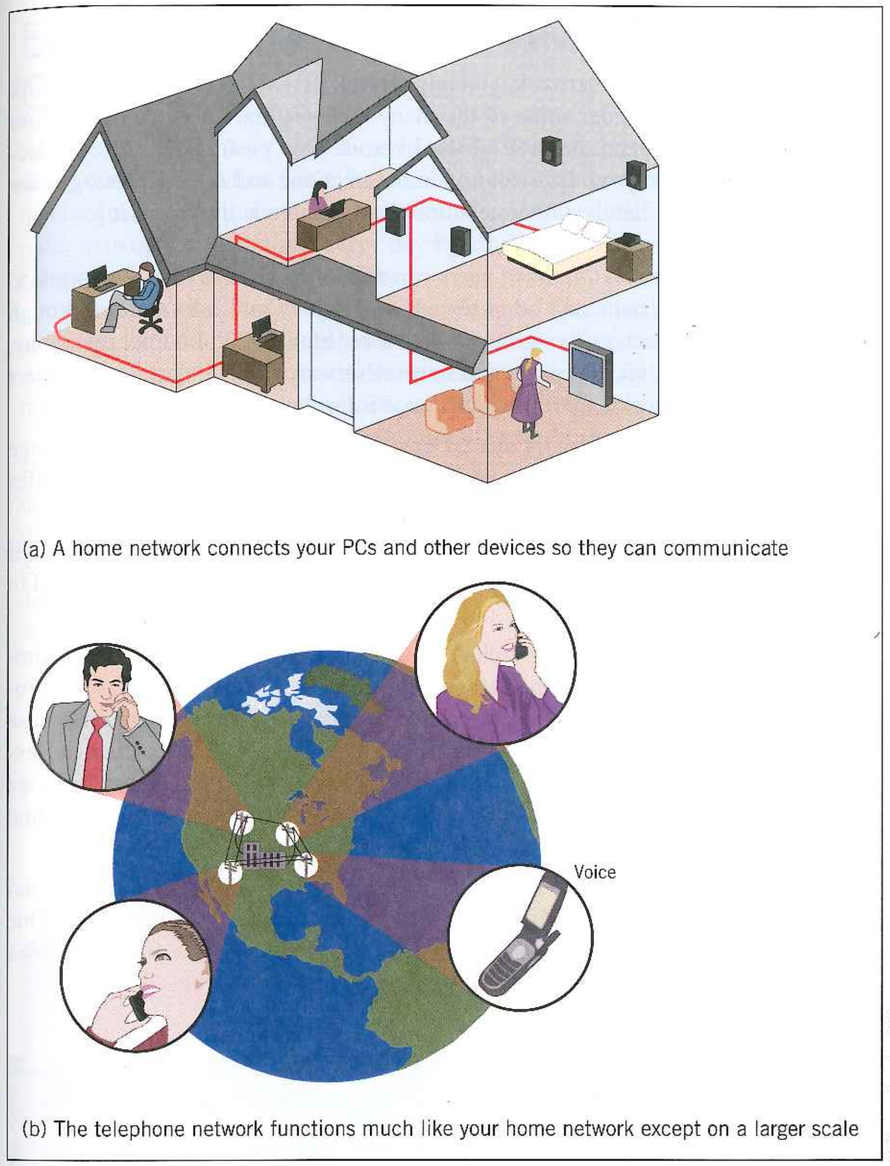
3-1.1.1

Introducing Networks

When most people think of networks, they envision something fairly complicated. However, at the lowest level, networks are not that complex. In fact, a network is simply a group of two or more computers linked together. As the size of a network increases and more devices are added, installing devices and managing the network becomes more technical. Even so, networking concepts and terminology basically remain the same regardless of size or type.

VOCABULARY
Public Switched Telephone Network (PSTN)

Different types of networks transfer different types of data. For instance, over a computer network, you can transfer text, images, video, and audio files. A telephone network is similar in makeup to a computer network, though it transfers voice data. The ***Public Switched Telephone Network (PSTN)*** supports telephone service and is the world's collection of interconnected commercial and government-owned voice-oriented systems. Digital, mobile, and standard telephones are supported through this network. **Figure 25–1a** and **Figure 25–1b** show the similarities between a home network and the telephone network.


(a) A home network connects your PCs and other devices so they can communicate

(b) The telephone network functions much like your home network except on a larger scale

© Cengage Learning 2013

FIGURE 25–1 Home and telephone networks

3-1.1.2

Identifying the Benefits of a Network

To identify the benefits of a network, you might think first about the biggest network of all—the Internet. Consider some of the many changes that have occurred in our society in the last few years because of the Internet. One profound change is electronic mail. A network provides instant communication, and e-mail messages are delivered almost immediately. Other network benefits include the following:

- *Information sharing*: Authorized users can access computers on the network to share information, data, and other resources. People share information through special group projects, news groups, databases, blogs, FTP, Internet telephony, instant messaging, social media, and so on. Users around the world can connect to each other to access, share, and exchange information. See **Figure 25–2**.
- *Collaborative environment*: A shared environment enables users to exchange files and collaborate on group projects by combining the power and capabilities of diverse equipment and software, thus increasing personal productivity.
- *Hardware sharing*: It is not necessary to purchase a printer or a scanner or other frequently used peripherals for each computer. Instead, one device connected to a network can serve the needs of many users.
- *Software sharing*: Instead of purchasing and installing software on every computer, it can be installed on the server. All of the users can then access the program from this one central location. Software sharing saves money because companies can purchase a site license for their users. This practice is less expensive than purchasing individual software packages, and updating software on the server is much easier and more efficient than updating it on individual computers.
- *Enhanced communications*: Electronic mail, text messages, social media, and other electronic communication have changed the way the world interacts. One advantage is the almost instantaneous delivery of e-mail. The cost for e-mail does not depend on the size of the message or the distance the message has to travel.

© Toria / Shutterstock.com

FIGURE 25–2 Information sharing

3-1.1.3

Evaluating the Risks of Networked Computing

As with any technology, you should consider the disadvantages of using a network along with the benefits. For instance, data insecurity and the vulnerability to unauthorized access are primary weaknesses of many networks. The security of a computer network is challenged every day by equipment malfunctions, system failures, computer hackers, and virus attacks.

Equipment malfunctions and system failures are caused by a number of factors, including natural disasters such as floods or storms, fires, and electrical disturbances such as brownouts or blackouts. Server malfunctions or failures mean users temporarily lose access to network resources, such as printers, drives, and information.

Computer hackers and viruses present a great risk to networked environments. ***Hackers*** are people who break into computer systems to steal services and information, such as credit card numbers, passwords, personal data, and even national security information. Hackers can also delete data. Other people threaten networks and data by creating viruses and other types of malicious software, which are particularly dangerous to networked computers because these programs usually are designed to sabotage shared files (see **Figure 25–3**).

VOCABULARY
hacker

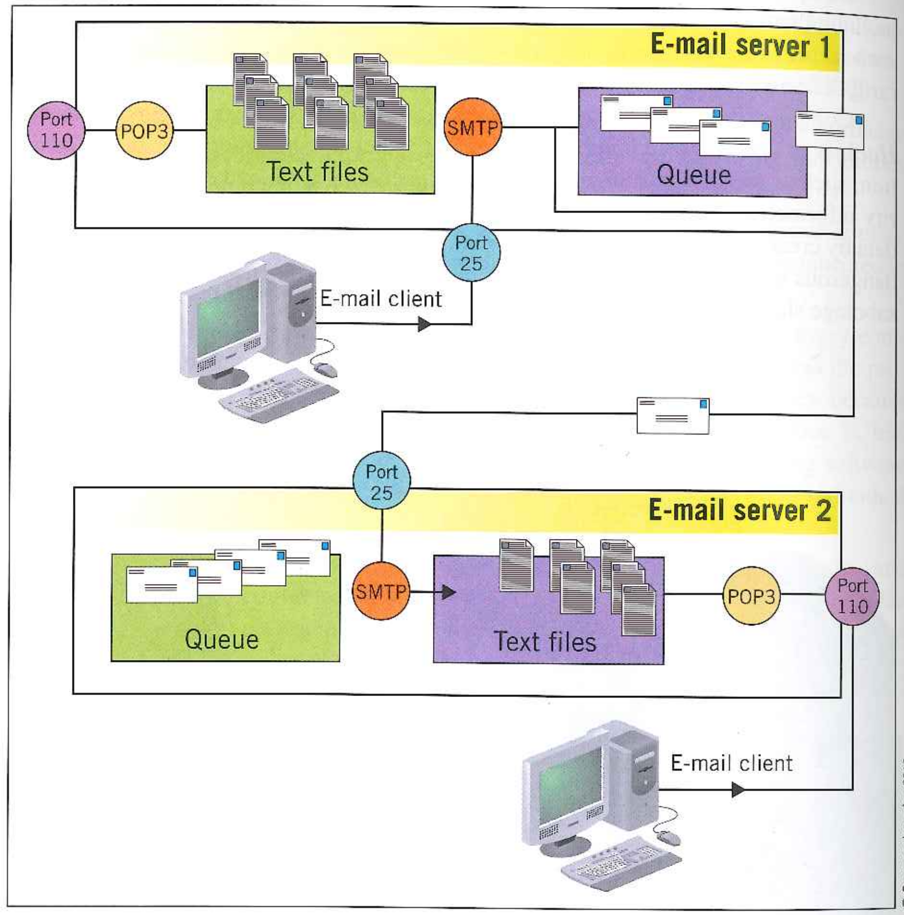
© Jozsef Szasz-Fabian / Shutterstock.com

FIGURE 25–3 Computer criminal

The following are some other disadvantages of networks:

- *Individual loss of autonomy*: Networks can play a part in taking away an individual's autonomy by controlling which software programs are accessible, and keeping a record of how the computer is used and what sites are accessed, for example.
- *Malicious code*: Compared to standalone computers, networks are more vulnerable to viruses, worms, Trojan horses, e-mail bombs, and spyware.
- *Network faults*: Network equipment problems can result in loss of data and resources.

- *Setup and management costs*: Setting up a network requires an investment in hardware and software; ongoing maintenance and management of the network requires the care and attention of at least one IT professional.
- *Lack of privacy*: For example, e-mail is not necessarily private. Messages travel through a number of systems and networks and provide opportunities for others to intercept or read the messages (see **Figure 25–4**). Junk e-mail also can become a problem. On the other hand, a standalone system is not vulnerable to many of these risks because it does not share connections with other computers.



© Cengage Learning 2013

FIGURE 25–4 E-mail system

ETHICS IN TECHNOLOGY

Hackers

Computer security violations are one of the biggest problems experienced on computer networks. People who break into computer systems are called hackers. The reasons they break in are many and varied. Common types of violations follow:

- *Theft of services*: Many password-protected services charge a fee for usage. A hacker finds a way to bypass the password and uses the service without paying for it.
- *Theft of information*: A hacker might break into a system to steal credit card numbers, test data, or even national security data.
- *Unfair competition or vengeance*: Hackers might access an organization's system to destroy files as a form of revenge for real or imagined grievances. They also might steal information to sell to opposing groups or to use to compete with the organization.
- *Thrill*: Some hackers break into sites for the challenge. The thrill is in breaking the code or feeling superior to the security system.

Identifying Client/Server Networks

3-1.1.4

VOCABULARY
client/server network
client
server
server operating system
local area networks (LAN)
wide area networks (WAN)

The term ***client/server network*** describes a network design model. Most common network functions such as database access, e-mail exchange, and Internet access are based on this model. In most instances, the ***client*** is a software program such as Internet Explorer. The ***server*** is hardware (a computer) and can be one of many types of servers, such as a mail server, a database server, an FTP server, an application server, a Web server, and so on. When you access the Internet using a browser, the browser is the client you use to access any available server in the world. This access enables the server and client to share files and other resources such as printers and external storage devices. In general, a server provides a service, such as Web access, to one or many clients.

For network administrators, selecting a server can be a simple or a complicated task, depending on the network size, the amount of storage needed, the number of users, and so on. Similar to a desktop computer, a network server requires an operating system.

Server operating systems are high-end programs designed to provide network control and include special functions for connecting computers and other devices into a network. Three of the more popular server operating systems are Microsoft Windows, Mac OS X, and UNIX/Linux. The selection of an operating system is determined by how the server will be accessed, security issues, whether the server will host a database, whether forms will be processed, whether programs such as Microsoft Expression Web or Adobe Dreamweaver will be used, and other individual factors. Client access to the server can be through desktop or notebook computers, handheld devices, game systems, and other similar electronic devices.

Identifying Network Types

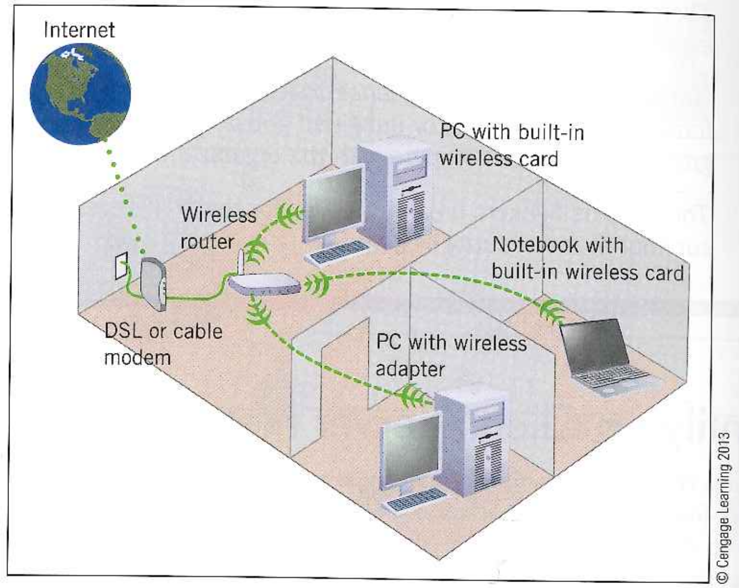
3-1.1.5

Networks can be categorized by size as ***local area networks (LANs)*** or ***wide area networks (WANs)***. They can also be classified by type, which includes client/server, peer-to-peer, intranet, extranet, and the Internet.

Local Area Networks

VOCABULARY
node
wireless LAN (WLAN)
router
communications channels

Most LANs connect personal computers, workstations, and other devices such as printers and scanners in a limited geographical area, such as an office building, school, or home. Each device on the network is called a ***node***, and each node generally shares resources such as a printer, programs, and other hardware. A ***wireless LAN (WLAN)*** is a variation of the LAN that uses few if any physical wires to connect devices. To communicate on a WLAN, the computer and other devices that access the network must each contain a wireless device such as a network card, flash card, PC card, USB network adapter, or other type of built-in wireless capability or a wireless network card (see **Figure 25–5**).


Internet
PC with built-in wireless card
Wireless router
Notebook with built-in wireless card
DSL or cable modem
PC with wireless adapter

© Cengage Learning 2013

FIGURE 25–5 Wireless LAN

Wide Area Networks (WAN)

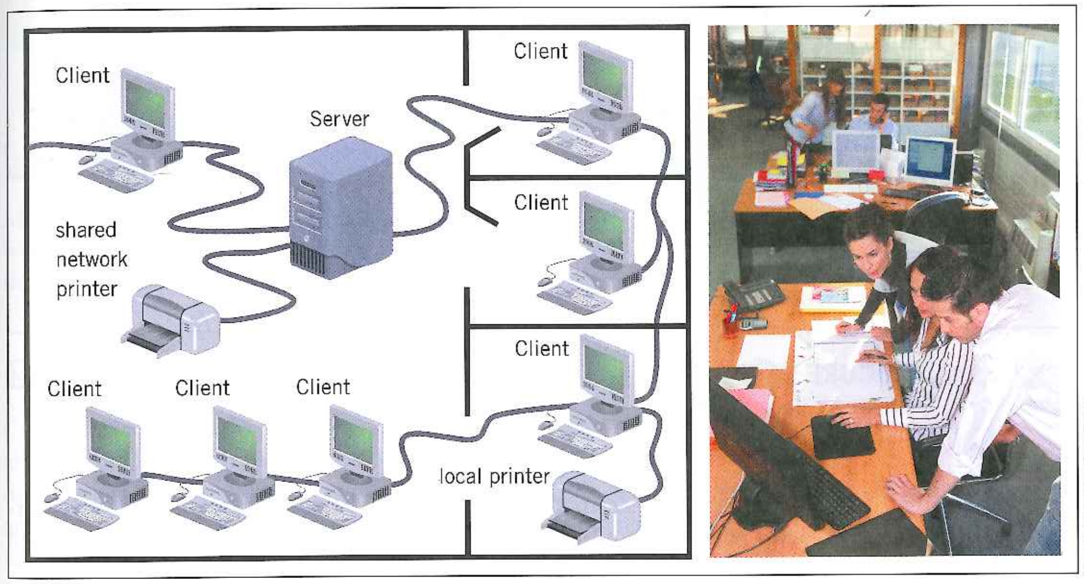
A WAN covers a large geographical area and can contain communication links across metropolitan, regional, or national boundaries. The communications area might be as large as a state, country, or even the world. The largest WAN is the Internet. Most WANs consist of two or more LANs and are connected by ***routers***, which direct traffic on the Internet or on multiple connected networks. ***Communications channels*** can include telephone systems, fiber optics, satellites, microwaves, or any combination of these.

Other Types of Networks

The design of a network, including how it is set up physically, is called its architecture. The two broad categories of network architecture are client/server and peer-to-peer.

VOCABULARY
hub

- *Client/server network*: In this type of architecture, one or more computers on the network acts as a server. The server manages network resources. Depending on the size of the network, several servers might be connected. For example, a print server manages the printing and a database server manages a large database. In most instances, a server is a high-speed computer with considerable storage space. The network operating system software and network versions of software applications are stored on the server. All of the other computers on the network are called clients. They share the server resources and other peripherals such as hubs, firewalls, and routers. A ***hub*** is a small, simple, inexpensive device that joins multiple computers together. Users access the server by entering a user name and password. See **Figure 25–6**. Some networks use a switch, which performs the same tasks as a hub and is much faster.



© auremar / Shutterstock.com

FIGURE 25–6 Client/server local area network

VOCABULARY

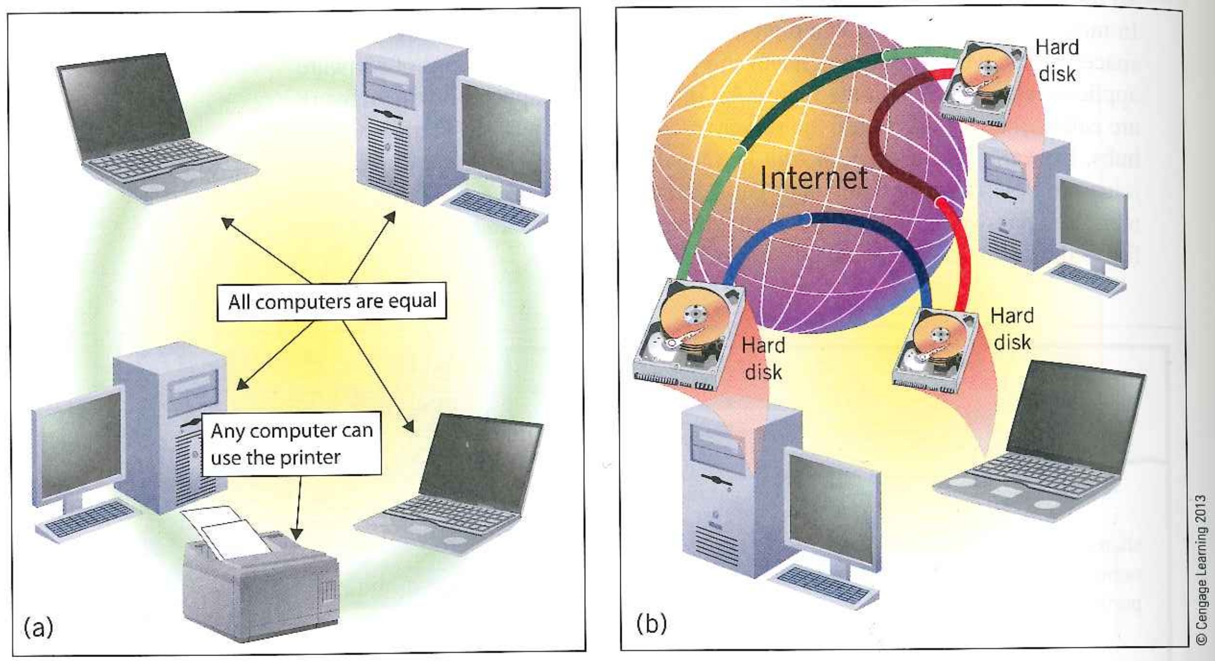
peer-to-peer (P2P) network

intranet

extranet

Internet

- *Peer-to-peer network*: In a ***peer-to-peer (P2P) network***, all the computers are equal. No computer is designated as the server. People on the network each determine what files on their computer they share with others on the network. This type of network is much easier to set up and manage. Many small offices use P2P networks. Some types of P2P networks allow you to download different parts of files simultaneously from several computers at the same time. Using this format, you can potentially get much faster downloads and get larger files more quickly. See **Figure 25–7**.



© Cengage Learning 2013

FIGURE 25–7 (a) Peer-to-peer network using a printer resource (b) Internet peer-to-peer network

ABOVE AND BEYOND

In discussions about networks, you might hear someone mention bridges, which are also a type of communications device. A bridge is a special computer that connects one LAN to another LAN. For the most part, however, bridges are rarely used in modern networks.

Networks are also classified by the type of technology they use to share information. Most networks use the Internet Protocol (IP) technology to share data and resources. The following types of networks use IP technology:

- *Intranet*: An ***intranet*** is designed for the exclusive use of people within an organization. Many businesses have implemented intranets. Documents such as handbooks and employee manuals, newsletters, employment forms, and other relevant company documents are the types of files stored on an intranet server.
- *Extranet*: An ***extranet*** is similar to an intranet, but it allows specific users outside of the organization to access internal information systems. Like the Internet, intranets and extranets use and support Web technologies, such as hyperlinks and Web pages coded in hypertext markup language (HTML).
- *Internet*: The ***Internet*** is a worldwide system composed of thousands of smaller networks. This global network allows computers worldwide to connect and exchange information. The Web and electronic mail are two of the more popular components of the Internet.

In Step-by-Step 25.1, you research home wireless networks.

Step-by-Step 25.1

1. Click the **Start** button on the taskbar, and then click **Help and Support**.
2. Search for Help topics on networking.
3. Select the **Setting up a wireless network** topic.
4. Read the topic and then use your word-processing program to answer the following questions:
   - What equipment do you need to set up a wireless network?
   - Where should you position a wireless router?
   - What two tasks should you perform to secure the wireless network?
   - How do you add a computer to the network?
   - How can you share files on a Windows 7 network?
5. Save your file as **networking** and submit it to your instructor.

Understanding Network Communications

IC³ 3-1.1.6

Most networks consist of a network server and computer clients. In addition, networks use two other categories of hardware: communications devices and devices that connect the network cabling and amplify the signal.

Communication Hardware

Communication hardware devices help to transmit and receive data. When we think about communication hardware, the first thing that generally comes to mind is the desktop computer and router. However, other types of computers and devices send and receive data. Some examples are mainframe computers, minicomputers, and large computers such as supercomputers; handheld and laptop computers; and even fax machines and digital cameras. All of these devices require some type of transmitting hardware device. Examples of communication hardware follow:

VOCABULARY

modem

- *Modem*: The word ***modem*** is an acronym for *mo*dulate-*dem*odulate, which means to convert analog signals to digital and vice versa. This device enables a computer to transmit data over telephone lines. Computer information is stored digitally (in binary code of 0s and 1s), whereas information sent over telephone lines or other media generally is transmitted in the form of analog waves. Both the sending and receiving users must have a modem. The speed at which modems can transmit data has increased dramatically in the past few decades. The first modems introduced in the 1960s could send data at a rate of about 300 bits per second (bps). By the early 1990s, the speed of data transmission via modem had increased to 9600 bps, with the standard modem speed of 56 Kbps (kilobits per second) reached by the middle of the decade. Special modems can transmit data as fast as 8 Mbps (megabits per second) over telephone lines.

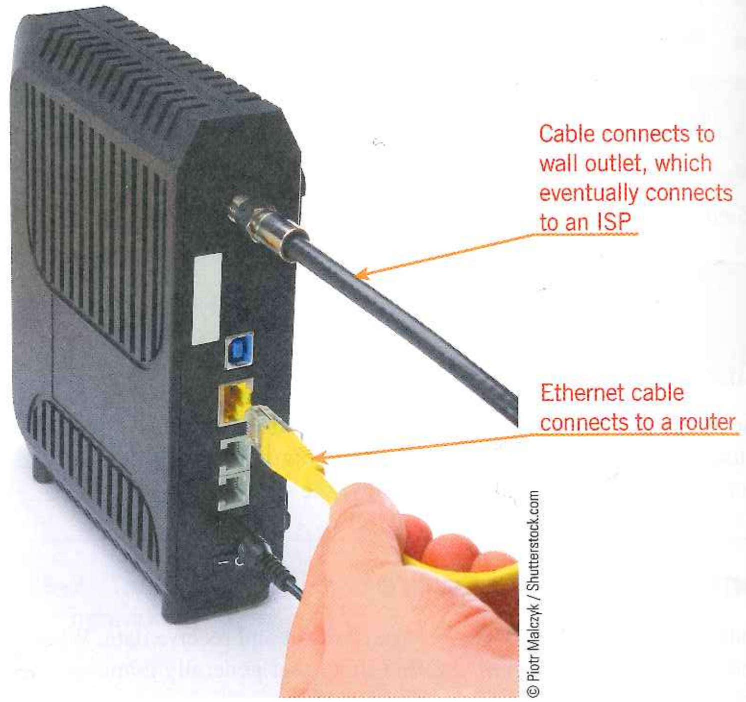
VOCABULARY

cable modem

digital subscriber line (DSL)

T-1 line

- *Cable modem*: A ***cable modem*** uses coaxial cable to send and receive data. This is the same type of cable used for cable TV. The bandwidth, which determines the amount of data that can be sent at one time, is much greater with a cable modem than with the older technology of a dial-up modem. For this reason, cable modems are used to deliver broadband Internet access, which is a high data rate connection to the Internet. Cable modems allow as many as 1,000 users to transmit data on one 6-MHz (megahertz) channel and can transmit data at speeds of 30 to 40 Mbps. A cable modem can be connected directly to your computer, enabling you to connect to the Internet, or it can be connected to a router so that your computer has wireless access to the Internet. See **Figure 25–8**.


Cable connects to wall outlet, which eventually connects to an ISP
Ethernet cable connects to a router

© Piotr Malczyk / Shutterstock.com

FIGURE 25–8 Cable modem

- *Digital subscriber line*: A ***digital subscriber line (DSL)*** is an Internet connection technology that provides for the transfer of information to a computer at a high-speed bandwidth over ordinary copper telephone lines. A DSL can carry both data and voice. The data part of the line is a dedicated connection to the Internet. High bit-rate DSL (HDSL) was the first DSL technology to use twisted-pair cables. Very-high bit-rate DSL (VDSL) can support HDTV, telephone services, and Internet access over a single connection. Like cable modems, DSL modems are widely used to provide broadband Internet access.
- *T-1 line*: A ***T-1 line*** is a type of fiber-optic telephone line that can transmit up to 1.544 megabits per second or can be used to transmit 25 digitized voice channels. T-1 lines can be used for data transfer on a network or to provide phone service for a commercial building.

VOCABULARY

wireless Internet service provider (WISP)

WiMAX

- *Wireless*: ***Wireless Internet service providers (WISPs)*** provide connection speeds more than 30 times faster than dial-up connections—from 384 Kbps to 2.0 Mbps. ***WiMAX*** (Worldwide Interoperability for Microwave Access) is a wireless technology that can deliver maximum speeds of up to 1 Gbps to your cell phone, home computer, or car. WiMAX is an alternative to cable and DSL, especially for users in areas that cable and DSL service providers do not serve. It is also used to connect mobile computer users to the Internet across cities and countries. You can use a WiMAX USB modem to connect to a WiMAX network. See **Figure 25–9**.

© cheyennezj / Shutterstock.com

FIGURE 25–9 USB modem for connecting to a WiMAX network

As indicated earlier, connecting to the Internet requires special devices—typically a cable or DSL modem linked to a computer using an Ethernet cable, a type of cable designed to connect devices on a network. To connect devices such as personal computers, cell phones, and game systems wirelessly to the Internet, the following components are needed:

- A notebook computer or other type of device such as a computer game system, an iPhone or other smart phone, or similar device
- An internal wireless adapter or a USB port for connecting an external adapter; the adapter must be compatible with the wireless provider's protocols
- A high-speed, wireless Internet access plan from a provider
- "Sniffer" software, used to locate hot spots; usually built into the device

Communication standards enable all of these different devices to communicate with each other.

ABOVE AND BEYOND

Broadband is high-speed Internet access; most Internet users in the United States have broadband access.

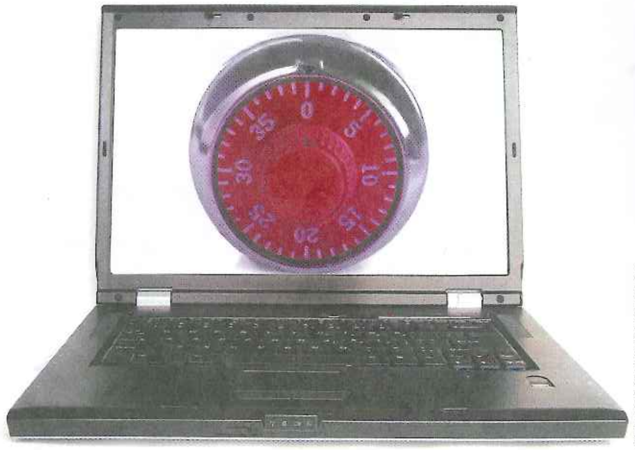
3-1.1.7

Resolving Network Security Issues

Establishing and maintaining computer security is necessary to keep hardware, software, and data safe from harm or destruction. Some risks to computers are natural causes, some are accidents, and others are intentional. It is not always evident that some type of computer crime or intrusion has occurred. Therefore, safeguards for each type of risk should be put into place. It is the responsibility of a company or an individual to protect its data.

The best way to protect data is to effectively control access to it. Generally, this protection is the responsibility of the network administrators and security personnel. If unauthorized persons gain access to data, they may obtain valuable information or trade secrets. Perhaps worse, they might change data outright so that no one can use it.

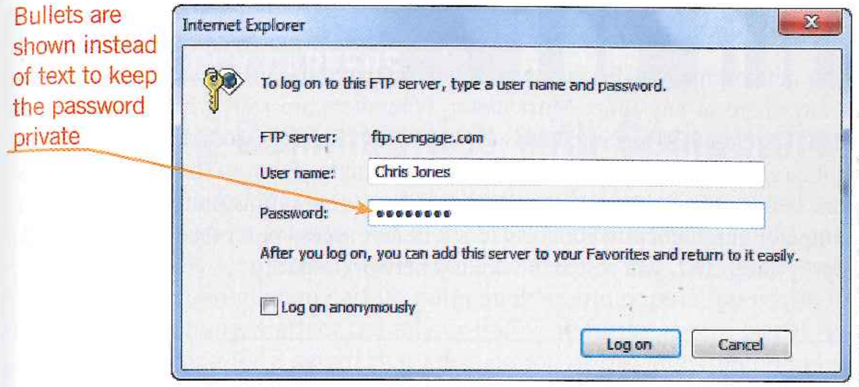
The most common form of restricting access to data is the use of passwords, which are similar to combinations you need to remove a lock, as shown in **Figure 25–10**. Users may need a password to log on to a computer system or to specific parts of it. Companies often establish password-protected locations on hard drives and networks so that designated people have access to certain areas but not to others.



© zimmytws / Shutterstock.com

FIGURE 25–10 Password-protected computer

To maintain secure passwords, you should change them frequently so that people who no longer need access are locked out. Tips for creating secure passwords include using a mixture of upper- and lowercase letters, using numbers as well as letters, and adding special characters such as & or % to the password. The challenge is to create passwords that are easy for you to remember but difficult for anyone else to decipher, because you should never write down a password or share it with anyone else (see **Figure 25–11**). The challenge is to create passwords that are easy for you to remember, but difficult for anyone else to decipher. You should never share or write down a password. More password protection is broken by people who gain access through a shared password or lost "cheat sheet" than by anyone guessing your "secret code."



Bullets are shown instead of text to keep the password private

Internet Explorer

To log on to this FTP server, type a user name and password.

FTP server: ftp.cengage.com

User name: Chris Jones

Password: ●●●●●●●●

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

Used with permission from Microsoft Corporation

FIGURE 25–11 Passwords protect data against unauthorized use

All users should maintain password security to keep out unauthorized users, hackers, and other computer criminals. Never reveal a password to anyone without authorization. Inform the appropriate people if you discover that an unauthorized user knows or can access passwords. Avoid using the same or similar passwords for other applications or Internet accounts.

Other security measures include the following:

- Electronic identification cards are used to gain access to certain areas within a building or department.
- ***Firewalls***, which consist of special hardware and software, protect an internal network from external networks. A firewall gives users inside an organization the ability to access computers outside of their organization but keeps unauthorized users from accessing the organization's computers.
- Antivirus software is used to protect data on your computer. It always should be running on a computer to protect data and programs from corruption or destruction.
- A ***proxy server*** acts like a switchboard through a firewall. The server is an intermediary between a user and the Internet, ensuring security, administrative control, and caching service. A cache (pronounced *cash*) is a place to store something temporarily.

VOCABULARY

firewall

proxy server

biometric security measure

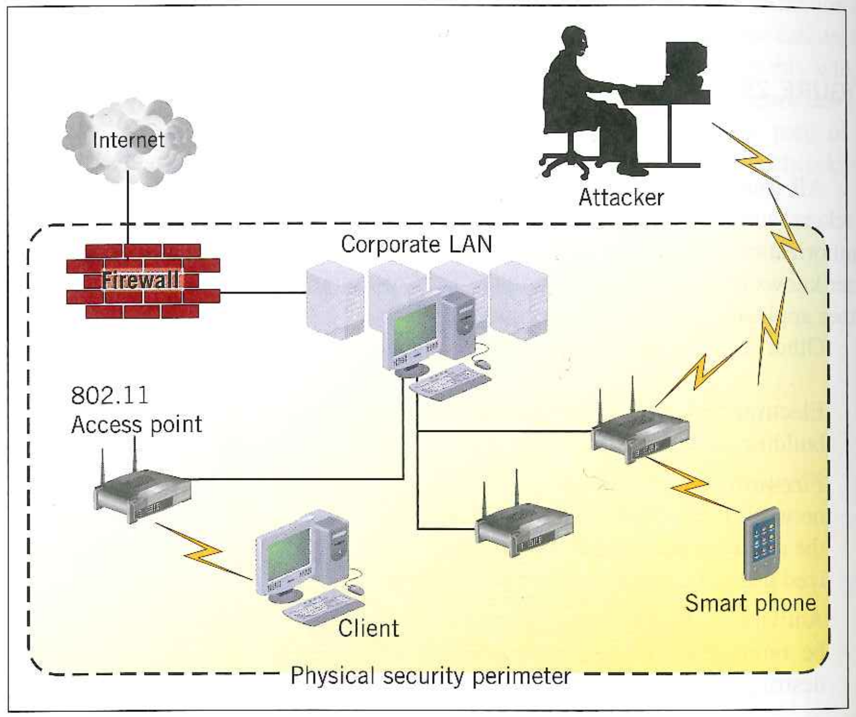
Planning for Security

Companies must plan for security before it is needed rather than handle breaches in security as they occur. For example, any company that deals with sensitive information or needs to protect its data should consider the following guidelines:

- Institute a selective hiring process that includes careful screening of potential employees. Do not keep employees on staff that refuse to follow security rules. This measure can prevent internal theft or sabotage.
- Regularly back up data and store it off site.
- Employ ***biometric security measures***, which examine a fingerprint, a voice pattern, or the iris or retina of the eye. These must match the entry that was originally stored in the system for an employee to gain access to a secure area. This method of security is usually applied when high-level security is required.

Wireless Security

Wireless networking (Wi-Fi) is now so common that you can access the Internet just about anywhere at any time. Most laptop computers are sold with wireless cards installed. Wireless networking, however, has many security issues, and hackers have found it easy to access wireless networks. For example, one way to access a wireless network is through accidental association, when the user turns on the computer and the computer automatically connects to a wireless access point (see **Figure 25–12**). In Step-by-Step 25.2, you research wireless network security.



© Cengage Learning 2013

FIGURE 25–12 Securing wireless networks

Step-by-Step 25.2

1. Click the **Start** button on the taskbar, and then click **Help and Support**.
2. Search for Help topics on wireless networks, and then click a link such as the **Why can't I connect to a network?** link.
3. Read the information and then use your word-processing program to summarize what you learned.
4. Define the terms *Internet Connectivity Evaluation tool* and *Windows Compatibility Center*.
5. Submit your word-processing document to your instructor.

TECHNOLOGY CAREERS

Building Communities with Computers

Computer modeling is a term that describes the use of computers to create a mathematical model of a real-life system or process and then test it under different conditions. If you have played the computer game SimCity, you already have some experience with computer modeling. When you play the game, create a city, and then change certain data, such as the population or the location of a utility system, you can see how those changes affect the city overall. The future is still bright for computer gaming and simulation. If you are looking for a career that stays on top of the latest technical innovations, consider one in computer simulation.

SUMMARY

In this lesson, you learned:

- A network is a group of two or more computers linked together.
- A telephone network is similar in makeup to a computer network. The Public Switched Telephone Network (PSTN) supports telephone service, and it is the world's largest collection of interconnected commercial and government-owned voice-oriented systems.
- You can use a network for information sharing, hardware sharing, software sharing, and as a collaborative environment.
- Networks are categorized according to size as local area networks (LANs) and wide area networks (WANs).
- LANs connect personal computers, workstations, and other devices such as printers and scanners in a limited geographical area, such as an office building, a school, or a home.
- A WAN is made up of several connected local area networks.
- In a client/server network, one or more computers on the network acts as a server. The server manages network resources. In a peer-to-peer (P2P) network, all of the computers are equal. No computer is designated as the server. People on the network each determine what files on their computer they share with others on the network.
- Data insecurity is a risk with many networks. Some risks to computers are natural causes, some are accidents, and others are intentional.
- The best way to protect data is to effectively control the access to it. Generally, this protection is the responsibility of the network administrators and security personnel. If unauthorized persons gain access to data, they may obtain valuable information or trade secrets. Hackers are people who break into computer systems to steal services and information.
- Transmission media can be either physical or wireless.
- A modem is a type of communications device. A hub is a device that controls the incoming and forwarding of data. A router directs traffic on the Internet or on multiple connected networks.

LESSON REVIEW

TRUE / FALSE

Circle T if the statement is true or F if the statement is false.

T F **1.** The biggest network is the Internet.

T F **2.** E-mail always is private.

T F **3.** A WAN covers a large geographical area.

T F **4.** The best way to protect data is to effectively control access to it.

T F **5.** Networks are classified according to speed.

MULTIPLE CHOICE

Select the best response for the following statements:

1. A telephone network is similar in makeup to a __________ network.

   A. computer network C. tiny area network
   B. local area network D. metropolitan area network

2. A __________ server acts as an intermediary between a user and the Internet.

   A. high-level C. connected-level
   B. proxy D. biometric

3. The two broad categories of network architecture are __________ and peer to peer.

   A. intranet/extranet C. client/server
   B. DSL D. proxy/server

4. A(n) __________ can carry both data and voice.

   A. SLD C. WAN
   B. bridge D. DSL

5. A __________ is a variation of the LAN that uses no physical wires.

   A. WLAN C. P2P
   B. PSTN D. WiMAX

FILL IN THE BLANK

Complete the following sentences by writing the correct word or words in the blanks provided:

1. __________, which consist of special hardware and software, protect internal networks from external networks.
2. A(n) __________ converts analog signals to digital and vice versa.
3. A(n) __________ __________ is a type of fiber-optic telephone line.
4. The __________ is a worldwide system composed of thousands of smaller networks.
5. In a client/server network, the __________ manages network resources.

PROJECTS

PROJECT 25–1

3-1.1.1
3-1.1.3
3-1.1.7

As indicated in this lesson, the best way to protect data is to control access to the data.

1. Obtain a copy of the student use policy from your school. If one is not available, then locate a student use policy online from a school similar to yours.
2. After reading the policy carefully, rewrite it to include any additional guidelines and rules you believe should be included.
3. Explain why you selected these additional guidelines and rules and how they would benefit your educational environment.
4. Submit the document to your instructor as requested.

PROJECT 25–3

3-1.1.2
3-1.1.3

In recent times, schools have been criticized concerning the use of computers, especially in education at the primary and high school levels. Respond to the following questions:

1. Do you believe that computers should be used in elementary and high schools? Explain why or why not.
2. Should students have access to the Internet? Why or why not?
3. List at least two other options supporting computer access and two other options against computer access.

PROJECT 25–2

3-1.1.5
3-1.1.6

You want to set up a network in your home with the following elements:

- DSL, cable, or satellite Internet connection
- Desktop PC and two laptop computers that share the same Internet connection
- A printer and wireless router
- No additional charges from your Internet service provider

1. Use the Internet to research how to set up the home network according to this description.
2. Describe the network in a one- or two-page document.
3. Submit the document to your instructor as requested.

TEAMWORK PROJECT

3-1.1.1
3-1.1.4

You work at a local retail store that sells building supplies. Your supervisor at work is interested in learning about computers and various networking options as well as other technology solutions. In particular, she would like to know the best solutions for the store's environment. Assume that the hardware store has 14 employees and is part of a national chain. Develop a plan that you think would best serve the needs of your store for employee payroll, a directory and location of all store items, and a weekly review that would provide a list of what was sold and what needed to be replaced. Submit your final document to your instructor.

CRITICAL THINKING

3-1.1.3
3-1.1.7

Use the Internet and other resources to identify early security measures that were used to protect computers and computer data. Describe how these measures counteracted the intrusions made. Then, visit the Web sites of some companies that make computer security devices such as *www.computersecurity.com/individual.htm*. Compare these early security measures to today's current needs and practices. Write a report of your findings.

ONLINE DISCOVERY

Smart phones and notebook computers each use Wi-Fi to connect to the Internet. Use the Web to research the similarities and differences between Wi-Fi networks that smart phones use and those that notebook computers use. Organize your findings into a one-page document and submit it to your instructor.

IC3 3-1.1.5 3-1.1.6

JOB SKILLS

Netiquette—a word made from combining network and etiquette—refers to conventions to follow when using networks, including network services such as e-mail, blogs, and forums. Because so much workplace communication occurs on a network, knowing the rules of netiquette helps you set and maintain a professional reputation at work. Use the Internet to research the current rules of netiquette, and then list at least five rules in a document. Submit the document to your instructor.

Estimated Time:
1.5 hours

LESSON 26

Communication Services

OBJECTIVES

Upon completion of this domain, you should be able to:

- Categorize electronic communication.
- Identify users of electronic communication.
- Identify components of electronic communication.
- Manage e-mail with Microsoft Outlook.
- Send and receive e-mail.
- Save a message.

DATA FILES

You do not need data files to complete this lesson.

WORDS TO KNOW

Address Book
archiving
attachment
Contact Group
e-mail address
electronic mail (e-mail)
instant messaging
packet
save a message
signature
spam
text messaging
user agent
Windows Live Mail