CHAPTER 7
NETWORKS: COMMUNICATING AND SHARING RESOURCES

Computer networks link two or more computers so they can exchange data and share resources. Networks enable communications (electronically sending and receiving data) through the establishment of communications channels.

To connect to a network, you need to have a **network interface card (NIC)** and an operating system that supports networks.

A local area network (**LAN**) is within a small geographic area, such as a building or a group of buildings. LANs are typically owned and managed by a single person or organization.

A **wide area network** (**WAN**) is a geographically dispersed collection of LANs that links computers separated by a few miles or even thousands of miles. Unlike a LAN, a WAN is not owned by a single organization. Instead, it has a collective ownership or management, such as the Internet. The Internet is the largest WAN.

A **metropolitan area network** (**MAN**) is a network designed for a city or town. It is usually larger than a LAN but smaller than a WAN. Typically, a MAN is owned by a single government or organization.

A **campus area network** (**CAN**) includes several LANs that are housed in various locations on a college or business campus. It is usually smaller than a WAN.

A **personal area network** (**PAN**) is a network created among an individual's own personal devices, usually within a range of 32 feet. Such networks involve wireless technology.

A **home area network** (**HAN**) is a personal and specific use of network technology that provides connectivity between users and devices located in or near one residence. It enables users who reside at that location to quickly and conveniently share files and resources by using network connections between computers and peripheral devices.

In a **peer-to-peer network (P2P) network**, all the computers on the network are equals—that's where the term *peer-to-peer* comes from—and there's no file server. In **file sharing**, each computer user decides which, if any, files will be accessible to other users on the network. Users may also choose to share entire directories or even entire disks. They can also choose to share peripherals, such as printers and scanners.

P2P networks are easy to set up. People who aren't networking experts set up networks all the time, generally to share an expensive laser printer or provide Internet access to all the workstations on the LAN (Figure 7.9). Peer-to-peer networks tend to slow down with heavy use,

however, and keeping track of all the shared files and peripherals quickly becomes confusing. For this reason, peer-to-peer LANs are best used for simple networks connecting no more than 10 computers.

The typical corporate LAN is a **client/server network**, which includes one or more file servers, and networked workstations called **clients** (Figure 7.11). The file server on a client/server network is a high-capacity, high-speed computer with a large hard disk capacity. It contains the **network operating system (NOS)**, the software required to run the network. The server also contains network versions of programs and large data files. Clients—all the computers that can access the server—send requests to the server. The client/server model works with any size or physical layout of LAN and usually will not slow down with heavy use.

Many businesses today have extended their network structure to a **virtual private network** (**VPN**). A VPN operates as a private network over a public network, usually the Internet, making data accessible to authorized users in remote locations through the use of secure, encrypted connections, and special software.

The physical layout of a LAN is called its **network topology**. A topology isn't just the arrangement of computers in a particular space; a topology provides a solution to the problem of **contention**, which occurs when two workstations try to access the LAN at the same time. Contention sometimes results in **collisions**, the corruption of network data caused by two workstations transmitting simultaneously.

A **bus**, illustrated in Figure 7.14, is a network configuration in which the network cable is a single bus or backbone to which each workstation is connected. The two ends of the bus have special connectors called **terminators**.

A **star**, shown in Figure 7.15, is a network in which all other devices are connected to a central device, typically a computer. This configuration easily allows new users to be added to the network.

A **ring**, illustrated in Figure 7.16, is a network configuration in which all devices are connected in a closed loop or ring. In this network, data only travels in one direction around the ring.

Computer networks require physical media, but their most important component consists of the protocols that define how network devices can communicate with each other. A network requires many protocols to function smoothly. When a computer sends a message over the network, the application hands the message down the **protocol stack**, where a series of protocols prepares the message for transmission through the network. At the other end, the message goes up a similar stack. Figure 7.17 illustrates how messages move through the protocol stack.

By far the most widely used LAN protocol is **Ethernet**. The various versions of Ethernet are used by approximately 85 percent of all LANs. Although early versions of Ethernet (called

10base2 and 10base5) used coaxial cable in bus networks, the most popular versions today are Ethernet star networks that use switches and twisted-pair wire. Currently, three versions of Ethernet are in use: 10Base-T (10 Mbps), Fast Ethernet (100 Mbps, also called 100Base-T), and Gigabit Ethernet. The hardware to create a 10baseT Ethernet for five PCs can cost as little as $200. Refer to Figure 7.18 to review the various LAN protocols.

There are wireless networks as well. They use the IEEE 802.11 standards and transmit on the 2.4-GHz or 5-GHz radio frequency band. There are currently three popular IEEE 802.11 standards. The 802.11g standard is the most common, with 802.11n and 802.11r being the newest standards. Refer to Figures 7.19 and 7.20 to review the various wireless network standards and the networks they are best suited to serve.

Take the following security precautions when using WiFi:

- Use a firewall and update all antivirus and antispyware software.
- Change the router's default network name and password.
- Turn off SSID broadcasting to avoid detection by hackers.
- Make sure your router's software is the updated version.
- Turn on WPA to enable encryption.
- Turn on MAC (Media Access Control) address filtering so only authorized devices can obtain access.

The special components that distinguish a WAN from a LAN are point of presence and backbones. A **point of presence** (**POP**) is a WAN network connection point that enables users to access the WAN by a local analog telephone call (using a modem) or a direct digital hookup that enables a continuous direct connection. **Backbones** are the high-capacity transmission lines that carry WAN traffic.

Internet data can travel over any type of WAN because of Internet protocols. Collectively, Internet protocols are called **TCP/IP** (**Transmission Control Protocol/Internet Protocol**).

X.25 is the oldest packet-switching protocol; it is used by automated teller machines and credit card authorization devices.

New protocols designed for digital lines and faster data transfer rates include Switched Multimegabit Data Service (SMDS) and Asynchronous Transfer Mode (ATM).

Visit the Cisco Systems Web site (www.cisco.com). Cisco is a worldwide leader in networking equipment for the Internet.

Objective: *Contrast circuit-switching and packet-switching networks and explain their respective strengths and weaknesses.*

CHAPTER 7
NETWORKS: COMMUNICATING AND SHARING RESOURCES

In **circuit switching**, the network creates a physical end-to-end circuit between the sending and receiving computers. Circuit switching works best when it is essential to avoid delivery delays. In a circuit-switching network, high-speed electronic switches handle the job of establishing and maintaining the connection.

In **packet switching**, an outgoing message is divided into data units of a fixed size, called **packets**. Each packet is numbered and addressed to the destination computer. The sending computer pushes the packets onto the network, where routers examine the packets. **Routers** are devices that examine each packet they detect. After reading the packet's address, the router consults a table of possible pathways to the packet's destination. If more than one path exists, the router sends the packet along the path that is most free of congestion. There's no guarantee that the packets will arrive in the same order that they were sent, but that's not a problem. Protocols on the receiving end put the packets in the correct order and decode the messages they contain. If any packets are missing, the receiving computer sends a message requesting retransmission.

Circuit switching creates a permanent end-to-end circuit that is optimal for voice and real-time data. Packet switching does not require a permanent switched circuit and can funnel more data through a medium with a given data transfer capacity. However, packet switching introduces slight delays that make the technology less than optimal for voice or real-time data.

Objective: *Identify the options, components, configuration, and maintenance of a home area network (HAN).*

Home networks can accommodate both wired and wireless communications.

Wired home networks typically use Cat-5 or Cat-6 Ethernet cable or a home's electrical wiring. The simplest form of Ethernet network links different computers with a connecting switch or router. With an Ethernet network, each networked computer must have an Ethernet network adapter, also called a network interface card (NIC).

Wireless home networks rely on WiFi radio signals. **WiFi** is the wireless standard used for home networking.

For home WiFi networks, each computer on the network broadcasts its information to another using radio signals. WiFi networks use communications devices called network access points, also referred to as **wireless access points**, to send and receive data between computers that have wireless adapters. In a home network, in addition to enabling communication between networked devices and other networks, wireless routers also act as network access points. Network access points enable you to move a notebook with a wireless adapter from room to room or to place computers in different locations throughout a house.

A P2P relationship exists among all the computers in a wireless network. All peripherals in a wireless network must be within the router's range, which is usually 100 to 300 feet, depending on the building's construction and thickness of the walls, floors, and ceilings.

Computer networks for homes and small businesses can be built using either wired or wireless technology. Wired Ethernet has been the traditional choice in homes. Wired LANs generally also require central devices such as hubs, switches, or routers to accommodate more computers. In a wired network, a wire runs from the back of each computer to the router; the router serves as a communications point to connect the signal to the appropriate cable that goes to the intended destination.

To create a wireless network, you need a wireless router, which acts as the hub of the service. Each node to be connected to the wireless network needs a wireless adapter that connects to and communicates with the wireless router. Every device that connects to the wireless network needs a wireless adapter. Finally, connect your DSL or cable modem to your wireless router.

The good news is not much maintenance is needed with today's home networking solutions. You may need to blow off dust and lint that accumulates on your router, wireless adapter, or modem. You also may need to use your operating system's network utilities to refresh your network's settings.

When something goes wrong, you should try to think of what might have caused the problem. Sometimes the solution is as simple as restarting your computer and/or unplugging the power source from your router and other peripherals and then plugging them back in. You also may need to restart each computer that is connected to your system.

Internet Exercise: Voice over IP (VoIP) Service

Many individuals and businesses are using Voice over IP (VoIP) phone services to save money on phone bills, in comparison with using land lines and cell phones. Companies such as Skype and Vonage supply VoIP services, which allow people to use their Internet connection to place and receive calls.

Search the Web to determine what the rates are for these services. How do they compare with regular landline service rates? How does one get connected and use these services? Are there any disadvantages to this type of service? If so, what are they?

Which provider might be the best choice for you? Why? Submit your findings to your instructor.

Suggested Web sites:
www.voipreview.org
www.whichvoip.com

Suggested keywords:

residential, Skype, Vonage, VoIP services, VoIP providers

WEB RESOURCES

www.thelist.com: This site provides listings of various ISPs.

www.cisco.com: The Web site for Cisco Systems, a company that provides networking equipment for the Internet worldwide, provides solutions, products, and training opportunities for those interested in networking.

www.ethermanage.com/ethernet/ethernet.html: Charles Spurgeon's Ethernet Web page covers all the Ethernet technologies in use today and includes a practical guide for do-it-yourselfers.

www.howstuffworks.com/wireless-network1.htm: This Web site provides information on Wi Fi wireless networks.

www.wifinetnews.com: The Web site of Wi-Fi Net News offers daily updates on what's new in wireless networking.

www.about.com: This Web site is devoted to providing online guides on anything imaginable.

www.whatismyipaddress.com: This Web site determines your computer's IP address and provides information on IP protocols and tools.

http://en.wikipedia.org/wiki/Computer_network: This encyclopedia Web page provides an online overview of computer networking.

www.linktionary.com/g/gigabit_ethernet.html: This Web page provides definitions and hyperlinks for networking-related topics.

http://compnetworking.about.com/od/homenetworking/a/homeadvisor.htm: This Web site launches the Home Network Interactive Advisor, which makes network recommendations that meet users' needs.

www.freedomlist.com/info.php?mid=2: This Web page offers information related to ISPs.

http://compnetworking.about.com/cs/basicnetworking/f/whatsnetworking.htm: This Web site provides additional information on LANs, WANs, and networks in general.

www.skype.com: This is the Web site for Skype, a company that provides Voice over Internet Protocol (VoIP) phone service.

CHAPTER 7
NETWORKS: COMMUNICATING AND SHARING RESOURCES

KEY TERMS

backbone—A high-speed, high-capacity medium that transfers data over hundreds or thousands of miles in a wide area network (WAN) such as the Internet. A variety of physical media are used for backbone services, including microwave relay, satellites, and dedicated telephone lines.

bus topology—The physical layout of a local area network in which the network cable is a single conduit that forms a bus, or line; every node, whether it is a computer or peripheral device, is attached to that bus. At the ends of the bus, connectors called terminators signify the end of the circuit.

campus area network (CAN)—A network that includes several LANs that are housed in various locations on a college or business campus.

circuit switching—One of two fundamental architectures for a wide area network (WAN)—the other is packet switching—in which high-speed electronic switches create a direct connection between two communicating devices. The telephone system is a circuit-switching network.

client—In a client/server network, any type of computer: a PC, Mac, desktop, notebook, or even handheld device that is connected to a network and contains the software that enables it to send requests to the server.

client/server network—A computer network in which some computers are dedicated to function as servers, making information available to clients that make requests.

collision—In local area networks (LANs), a garbled transmission that results when two or more workstations transmit to the same network cable at exactly the same time. Networks have means of detecting and preventing collisions.

communications device—Any hardware device that is capable of moving data into or out of the computer, including modems, routers, switches, wireless access points, network interface cards, and other computers.

congestion—In a packet-switching network, a performance interruption that occurs when a segment of the network experiences an overload—too much traffic flooding the same network path.

contention—In a computer network, a problem that arises when two or more computers try to access the network at the same time. Contention can result in collisions, which can destroy data or require frequent and costly retransmissions.

contention management—In a computer network, the use of one of several techniques for managing contention and preventing collisions.

Ethernet—A set of standards that defines local area networks (LANs) capable of operating at data transfer rates of 10 Mbps to 6 Gbps. About 90 percent of all LANs use one of several Ethernet standards.

file server—In client/server computing, a computer that has been set aside (dedicated) to make program and data files available to users on a network who have been granted access.

gigaPoP (gigabits per second points of presence)—A point of presence (POP) that provides access to a backbone service capable of data transfer rates exceeding 1 Gbps (1 billion bits per second).

home network (**home area network** or **HAN**)—A personal and specific use of network technology that provides connectivity between users and devices located in or near one residence.

hot spot—A public wireless access location.

hub—A simple broadcast device used as the central wiring mechanism in a star topology network layout. It does not manage traffic and usually results in frequent collisions.

hybrid network—A network that is a combination of both wired and wireless technology.

Internet address (IP address)—The unique 32-bit address assigned to a computer that is connected to the Internet. It is represented in four parts, which are separated by periods (such as 128.254.108.7).

Internet Protocol (IP)—One of the two core Internet standards (the other is the Transmission Control Protocol, TCP), IP defines the standard that describes how an Internet-connected computer should break data down into packets for transmission across the network and how those packets should be addressed so that they arrive at their destination. IP is the connectionless part of the TCP/IP protocols.

intranet—A password-protected network controlled by a company and accessed only by employees.

latency—In a packet-switching network, a signal delay that is introduced when many routers examine packets en route to their destination.

local area network (LAN)—A computer network that connects computers in a limited geographic area, such as a building or group of clustered buildings.

logical address—An identifier assigned to a network node by the software in use.

metropolitan area network (MAN)—A network designed for a city or town and is usually larger than a LAN but smaller than a WAN.

modulation protocol—In modems, the communications standard that governs how the modem translates between the computer's digital signals and the analog tones used to convey computer data over the Internet so that the message is received and understood by the destination modem.

network—A group of two or more computer systems linked together to enable communications by exchanging data and sharing resources.

network administrator—A **c**omputer professional who installs, maintains, and supports computer networks, interacts with users, handles security, and troubleshoots problems. Also called a network engineer.

network architecture—The overall design of a computer network that specifies its functionality at every level by means of protocols.

network interface card (NIC)—An expansion board that fits into a computer's expansion slots, or an adapter built into the motherboard, that provides the electronic components to make the connection between a computer and a network.

network layers—Separate divisions within a network architecture with specific functions and protocols to allow engineers to make changes within a layer without having to redesign the entire network.

network operating system (NOS)—An operating system needed to enable data transfer and application use over a local area network (LAN).

network topology—The physical layout of a local area network (LAN), such as a bus, star, or ring topology, that determines what happens when, for example, two clients try to access the LAN or transmit data simultaneously.

node—Any device connected to a network. A node can be any computer, peripheral device (such as a printer or scanner), or communication device (such as a modem).

packet—In a packet-switching network, a unit of data of a fixed size—not exceeding the network's maximum transmission unit (MTU) size—that has been prepared for network transmission. Each packet contains a header that indicates its origin and its destination.

packet switching—One of two fundamental architectures for a wide area network (WAN), the other is a circuit-switching network. In a packet-switching network, such as

the Internet, no effort is made to establish a single electrical circuit between two computing devices. For this reason, packet-switching networks are often called connectionless. Instead, the sending computer divides a message into packets, each of which contains the address of the destination computer and dumps them onto the network. They are intercepted by devices called routers, which send the packets in the appropriate direction. The receiving computer assembles the packets, puts them in order, and delivers the received message to the appropriate application. Packet-switching networks are highly reliable and efficient, but they are not suited to the delivery of real-time voice and video.

peer-to-peer (P2P) network—A computer network design in which all the computers on the network are equals or peers. There is no file server. File sharing is decided by each computer user. A user may choose to share a few files, an entire directory, or even an entire disk. Users also can choose to share peripherals, such as printers and scanners. P2P is best used when connecting 10 computers or fewer.

personal area network (PAN)—A network created among an individual's own personal devices, usually within a range of 32 feet.

physical address—An identifier embedded in the hardware of a network node.

point of presence (POP)—A wired or wireless access connection point in a wide area network. ISPs that provide connectivity to the largest WAN, the Internet, are likely to have POPs in many cities and towns, but rural areas may not be so lucky.

protocol— In data communications and networking, the standard or set of rules that enable network-connected devices to communicate with each other.

protocol stack—In a computer network, a means of conceptualizing network architecture as vertical layers connected by protocols. Data is moved down the stack from its initial level, or transmitting node, to the lowest, physical hardware level that sends it over the network. When the data arrives at its destination, it moves back up the stack through the layers in reverse order, eventually arriving at the receiving node.

protocol suite—In a computer network, the collection of network protocols, or rules, that define the network's functionality.

ring topology—The physical layout of a local network in which all nodes are attached in a circle, without a central host computer. This topology, which is no longer used frequently, employs a unit of data called a *token* that travels around the ring. A node can transmit only when it possesses the token, thus avoiding collisions.

router—A complex device, or in some cases software, used to connect two or more networks. Routers have the capability to determine the best path to route data and locate alternative pathways so that the data reaches its destination.

server—A computer or device with software that manages network resources. Common servers manage files, e-mail, printers, and databases.

star topology—The physical layout of a local network in which a central wiring device, which can be a hub switch or computer, manages the network. A new user is added by simply running a cable to the hub or switch and plugging the new user into a vacant connector.

switch—A device that filters and forwards data between computers, printers, and other network nodes, enabling them to talk to each other. A switch is used only to move data between nodes within a single network.

TCP/IP—TCP/IP is an abbreviation for Transmission Control Protocol (TCP)/Internet Protocol (IP), the two most important Internet protocols. See **Transmission Control Protocol** and **Internet Protocol**.

terminator—Special connectors that signify the end of a circuit in bus topology.

token—A special unit of data that travels around the ring in a ring topology layout of a network. A node can transmit only when it possesses the token, thus preventing collisions.

Transmission Control Protocol (TCP)—One of two basic Internet protocols (the other is Internet Protocol, IP). TCP is the protocol (standard) that permits two Internet-connected computers to establish a reliable connection.

USB dongle—A device that is inserted into a USB port and adds additional features to the base system, such as enabling network connectivity, increasing RAM memory, and permitting Bluetooth communication.

USB wireless network adapter—Communication device that plugs into a USB port and usually provides an intuitive graphical user interface (GUI) for easy configuration.

virtual private network (VPN)—A network that operates as a private network over the Internet, making data accessible to authorized users in remote locations through the use of secure, encrypted connections, and special software.

wide area network (WAN)—A data network that uses long-distance transmission media to link computers separated by a few miles or even thousands of miles. The Internet is the

largest WAN—it connects millions of LANs all over the globe using a variety of physical media, such as microwave relay, satellites, and phone lines.

WiFi—A wireless LAN standard that offers Ethernet speeds through the use of radio waves instead of wires.

wireless access point (**AP** or **WAP**)—A node on a network that acts as a receiver and transmitter of wireless radio signals between other nodes on a network. A WAP can also act as a join or bridge connecting wireless clients to a wired network.

wireless LAN—A local area network that connects its nodes though the use of radio signals spread over a seemingly random series of frequencies for greater security.

X.25—A packet-switching network protocol optimized for use on noisy analog telephone lines.