Chapter 7

Telecommunications, the Internet, and Wireless Technology

LEARNING OBJECTIVES

After reading this chapter, you will be able to answer the following questions:

1. What are the principal components of telecommunications networks and key networking technologies?
2. What are the different types of networks?
3. How do the Internet and Internet technology work and how do they support communication and e-business?
4. What are the principal technologies and standards for wireless networking, communication, and Internet access?
5. Why are radio frequency identification (RFID) and wireless sensor networks valuable for business?

CHAPTER OUTLINE

Interactive Sessions:

The Battle Over Net Neutrality

Monitoring Employees on Networks: Unethical or Good Business?

RFID AND WIRELESS TECHNOLOGY SPEED UP PRODUCTION AT CONTINENTAL TIRES

Continental AG, headquartered in Hanover, Germany, is a global auto and truck parts manufacturing company, with 164,000 employees in 46 countries. It is also the world's fourth largest tire manufacturer and one of the top five automotive suppliers in the world.

One of the factories for Continental's Tire Division is located in Sarreguemines, France. This facility produces 1,000 different kinds of tires and encompasses nearly 1.5 million square feet. The production process requires large wheeled carts loaded with sheets of rubber or other components to be transported from storage to workstations as tires are being built. Until recently, if a carrier was not in its expected location, a worker had to look for it manually. Manual tracking was time-consuming and inaccurate, and the plant often lost track of tire components altogether.

Missing materials created bottlenecks and production delays at a time when business was growing and the company needed to increase production capacity. Continental found a solution in a new real-time location system based on a Wi-Fi wireless network using radio frequency identification (RFID) tags, AeroScout MobileView software, mobile computers, and Global Data Sciences' material inventory tracking system software.

The Sarreguemines plant mounted AeroScout T2-EB Industrial RFID tags on the sides of 1,100 of its carriers. As the carriers move from one manufacturing or storage station to another, location information about the cart is transmitted to nearby nodes of a Cisco Wi-Fi wireless network. AeroScout's MobileView software picks up the location and represents the carrier as an icon on a map of the facility displayed on computer screens. Fifteen Honeywell Dolphin 6500 and Motorola Solutions MC9190 handheld computers are used to confirm that a carrier has been loaded with components or has arrived at a specific workstation.

Seven of the plant's tuggers, which are small trucks for hauling the carriers around the plant, are equipped with DLOG mobile vehicle-mounted computers. When a tugger driver is looking for a specific component, he or she can use the mobile device to access the MobileView system, pull up a map of the facility, and see an icon indicating where that component's carrier is located. The location tracking system provides a real-time snapshot of all the components used in the factory.

A bar code label is attached to each component and carrier, and the system starts tracking that component as soon as it is placed in a carrier. Plant workers use one of the Motorola or Honeywell handhelds and the MobileView software to scan the bar code labels on both the component and its carrier, which is associated with the ID number transmitted by an RFID tag mounted on the carrier. The scanned bar code data are stored in a material inventory tracking system. The MobileView software tracks the carrier's location as

© Caro / Alamy

it is being transported to a storage area, and also the location where it is placed in storage.

When components are needed for manufacturing, a tugger driver uses the DLOG mobile computer to identify the location of the carrier with those specific components, and then goes to that location. After the carrier has been retrieved and taken to a workstation, its bar code is scanned by an employee at that station using one of the handheld computers. This updates the system to show that the required components have been received.

By enabling tugger drivers to quickly locate components, the new system has increased productivity and ensures that materials are not overlooked or misplaced. Fewer materials are thrown away because they expired and were not used when they were needed. The system is able to send alerts of materials that have been sitting too long in one spot.

When AeroScout and the new material inventory tracking system were implemented in September 2011, Continental made sure all production employees, including truckers, tire builders, and management, received training in the new system functions. The company also provided workers with instruction cards with detailed descriptions of system functions that they could use for reference.

Thanks to the new system, the Sarreguemines tire factory has increased production from 33,000 to 38,000 tires per day. Wastage of tire components has been reduced by 20 percent.

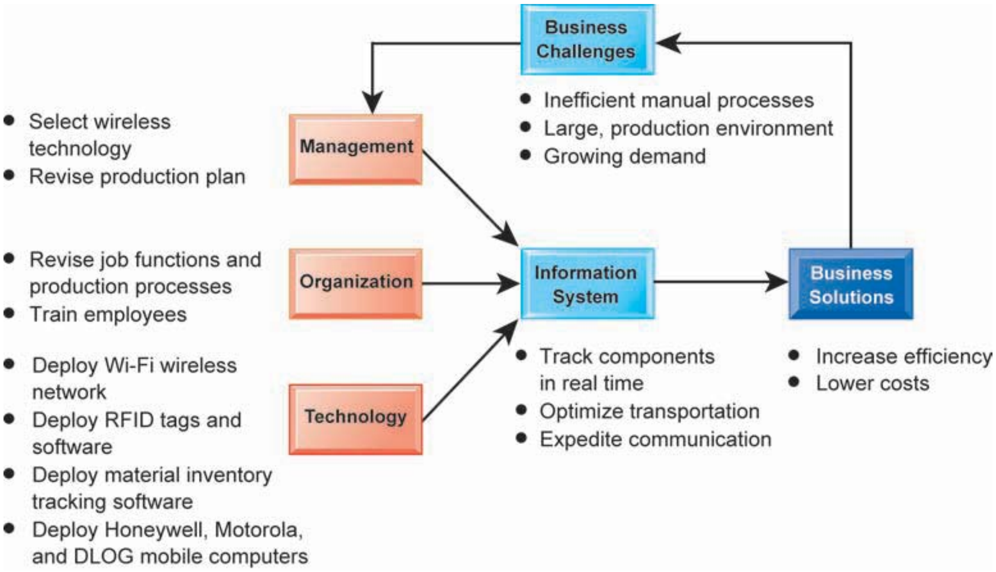
Sources: Claire Swedberg, "Continental Tire Plant Increases Productivity, Reduces Waste," *RFID Journal*, April 25, 2012 and www.conti-online.com, accessed May 2, 2012.

Continental Tires's experience illustrates some of the powerful capabilities and opportunities provided by contemporary networking technology. The company uses wireless networking, radio frequency identification (RFID) technology, mobile computers, and materials inventory management software to automate tracking of components as they move through the production process.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. Continental Tires' production environment extends over a very large area, and requires intensive oversight and coordination to make sure that components are available when and where they are needed in the production process. Tracking components manually was very slow and cumbersome, increasing the possibility that components would be overlooked or lost.

Management decided that wireless technology and RFID tagging provided a solution and arranged for the deployment of a wireless RFID network throughout the entire Sarreguemines production facility. The network made it much easier to track components and to optimize tugger truck movements. Continental Tires had to redesign its production and other work processes and train employees in the new system to take advantage of the new technology.

Here are some questions to think about: How did Continental's real-time location system transform operations? Why was training so important?



7.1 Telecommunications and Networking in Today's Business World

If you run or work in a business, you can't do without networks. You need to communicate rapidly with your customers, suppliers, and employees. Until about 1990, businesses used the postal system or telephone system with voice or fax for communication. Today, however, you and your employees use computers, e-mail and messaging, the Internet, cell phones, and mobile computers connected to wireless networks for this purpose. Networking and the Internet are now nearly synonymous with doing business.

NETWORKING AND COMMUNICATION TRENDS

Firms in the past used two fundamentally different types of networks: telephone networks and computer networks. Telephone networks historically handled voice communication, and computer networks handled data traffic. Telephone networks were built by telephone companies throughout the twentieth century using voice transmission technologies (hardware and software), and these companies almost always operated as regulated monopolies throughout the world. Computer networks were originally built by computer companies seeking to transmit data between computers in different locations.

Thanks to continuing telecommunications deregulation and information technology innovation, telephone and computer networks are converging into a single digital network using shared Internet-based standards and equipment. Telecommunications providers today, such as AT&T and Verizon, offer data transmission, Internet access, cellular telephone service, and television programming as well as voice service. Cable companies, such as Cablevision and Comcast, offer voice service and Internet access. Computer networks have expanded to include Internet telephone and video services. Increasingly, all of these voice, video, and data communications are based on Internet technology.

Both voice and data communication networks have also become more powerful (faster), more portable (smaller and mobile), and less expensive. For instance, the typical Internet connection speed in 2000 was 56 kilobits per second, but today more than 68 percent of the 239 million U.S. Internet users have high-speed **broadband** connections provided by telephone and cable TV companies running at 1 to 15 million bits per second. The cost for this service has fallen exponentially, from 25 cents per kilobit in 2000 to a tiny fraction of a cent today.

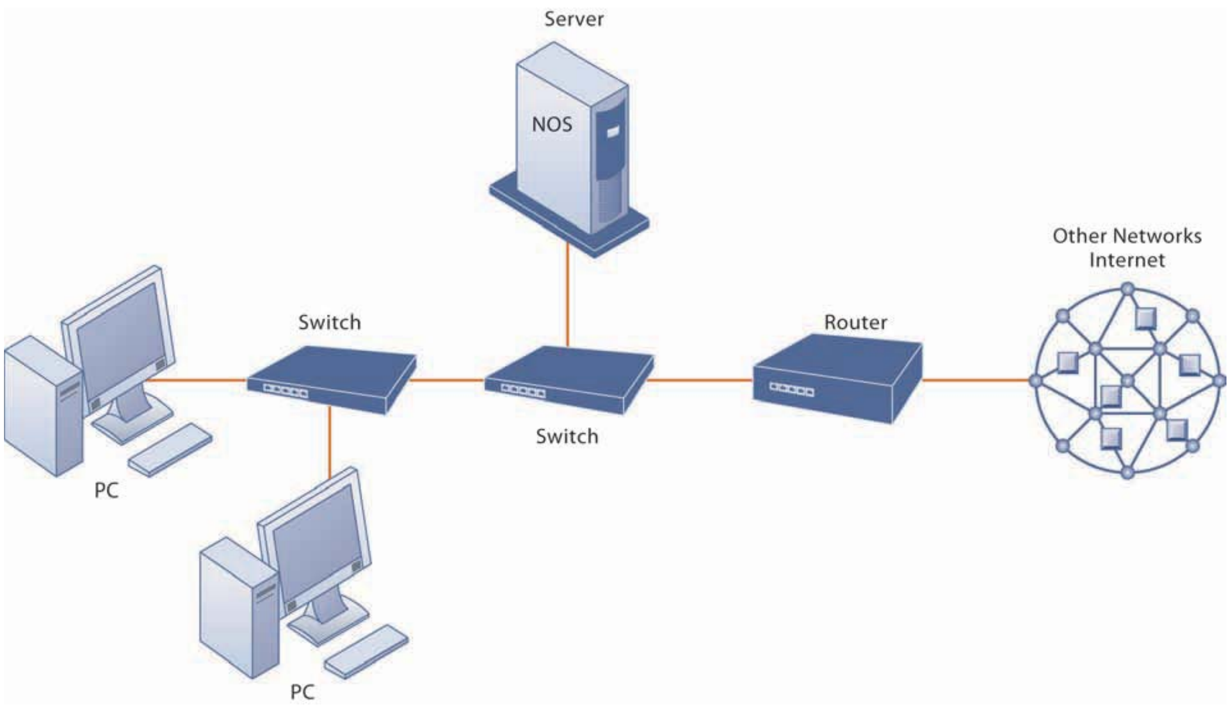
Increasingly, voice and data communication, as well as Internet access, are taking place over broadband wireless platforms, such as cell phones, mobile handheld devices, and PCs in wireless networks. In a few years, more than half the Internet users in the United States will use smartphones and mobile netbooks to access the Internet. In 2012, 122 million Americans (50% of all Internet users) accessed the Internet through mobile devices, and this number is expected to grow to 135 million by 2015 (eMarketer, 2012).

WHAT IS A COMPUTER NETWORK?

If you had to connect the computers for two or more employees together in the same office, you would need a computer network. Exactly what is a network? In its simplest form, a network consists of two or more connected computers. Figure 7.1 illustrates the major hardware, software, and transmission components used in a simple network: a client computer and a dedicated server computer, network interfaces, a connection medium, network operating system software, and either a hub or a switch.

Each computer on the network contains a network interface device to link the computer to the network. The connection medium for linking network components can be a telephone wire, coaxial cable, or radio signal in the case of cell phone and wireless local area networks (Wi-Fi networks).

FIGURE 7.1 COMPONENTS OF A SIMPLE COMPUTER NETWORK



Illustrated here is a very simple computer network, consisting of computers, a network operating system (NOS) residing on a dedicated server computer, cable (wiring) connecting the devices, switches, and a router.

The **network operating system (NOS)** routes and manages communications on the network and coordinates network resources. It can reside on every computer in the network, or it can reside primarily on a dedicated server computer for all the applications on the network. A server computer is a computer on a network that performs important network functions for client computers, such as serving up Web pages, storing data, and storing the network operating system (and hence controlling the network). Server software such as Microsoft Windows Server, Linux, and Novell Open Enterprise Server are the most widely used network operating systems.

Most networks also contain a switch or a hub acting as a connection point between the computers. **Hubs** are very simple devices that connect network components, sending a packet of data to all other connected devices. A **switch** has more intelligence than a hub and can filter and forward data to a specified destination on the network.

What if you want to communicate with another network, such as the Internet? You would need a router. A **router** is a communications processor used to route packets of data through different networks, ensuring that the data sent gets to the correct address.

Network switches and routers have proprietary software built into their hardware for directing the movement of data on the network. This can create network bottlenecks and makes the process of configuring a network more complicated and time-consuming. **Software-defined networking (SDN)** is a new networking approach in which many of these control functions are managed by one central program, which can run on inexpensive commodity servers that are separate from the network devices themselves. This is especially helpful in a cloud computing environment with many different pieces of hardware because it allows a network administrator to manage traffic loads in a flexible and more efficient manner.

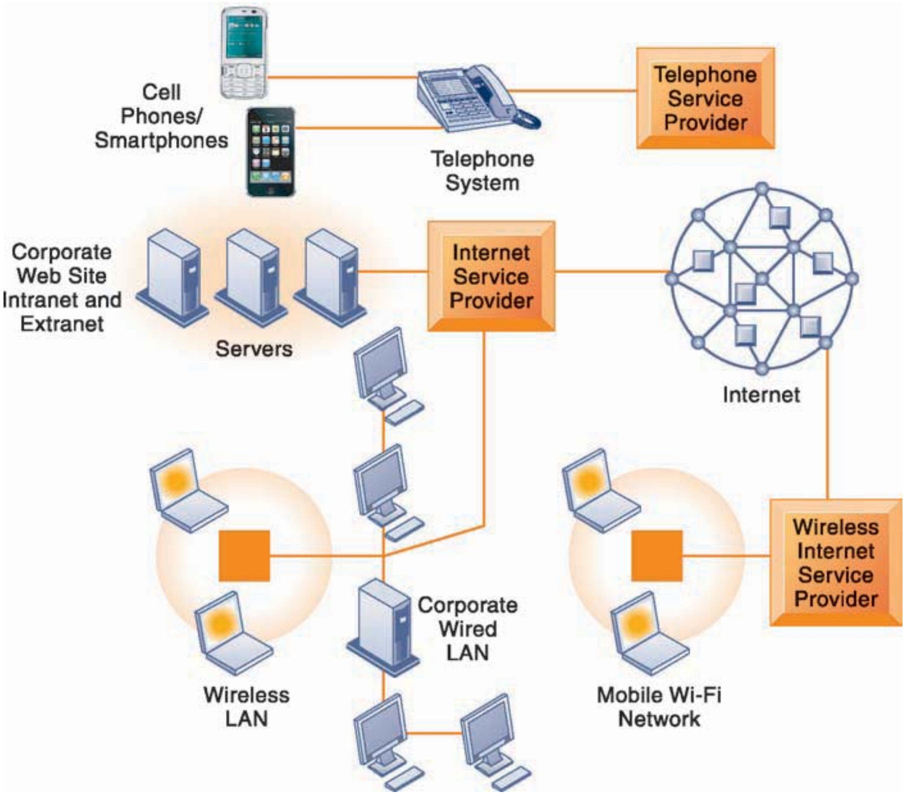
Networks in Large Companies

The network we've just described might be suitable for a small business. But what about large companies with many different locations and thousands of employees? As a firm grows, and collects hundreds of small local area networks, these networks can be tied together into a corporate-wide networking infrastructure. The network infrastructure for a large corporation consists of a large number of these small local area networks linked to other local area networks and to firmwide corporate networks. A number of powerful servers support a corporate Web site, a corporate intranet, and perhaps an extranet. Some of these servers link to other large computers supporting back-end systems.

Figure 7.2 provides an illustration of these more complex, larger scale corporate-wide networks. Here you can see that the corporate network infrastructure supports a mobile sales force using cell phones and smartphones, mobile employees linking to the company Web site, internal company networks using mobile wireless local area networks (Wi-Fi networks), and a videoconferencing system to support managers across the world. In addition to these computer networks, the firm's infrastructure usually includes a separate telephone network that handles most voice data. Many firms are dispensing with their traditional telephone networks and using Internet telephones that run on their existing data networks (described later).

As you can see from this figure, a large corporate network infrastructure uses a wide variety of technologies—everything from ordinary telephone service and corporate data networks to Internet service, wireless Internet, and cell phones. One of the major problems facing corporations today is how to integrate all

FIGURE 7.2 CORPORATE NETWORK INFRASTRUCTURE



Today's corporate network infrastructure is a collection of many different networks from the public switched telephone network, to the Internet, to corporate local area networks linking workgroups, departments, or office floors.

the different communication networks and channels into a coherent system that enables information to flow from one part of the corporation to another, and from one system to another. As more and more communication networks become digital, and based on Internet technologies, it will become easier to integrate them.

KEY DIGITAL NETWORKING TECHNOLOGIES

Contemporary digital networks and the Internet are based on three key technologies: client/server computing, the use of packet switching, and the development of widely used communications standards (the most important of which is Transmission Control Protocol/Internet Protocol, or TCP/IP) for linking disparate networks and computers.

Client/Server Computing

Client/server computing, introduced in Chapter 5, is a distributed computing model in which some of the processing power is located within small, inexpensive client computers, and resides literally on desktops, laptops, or in handheld devices. These powerful clients are linked to one another through a network that is controlled by a network server computer. The server sets the rules of communication for the network and provides every client with an address so others can find it on the network.

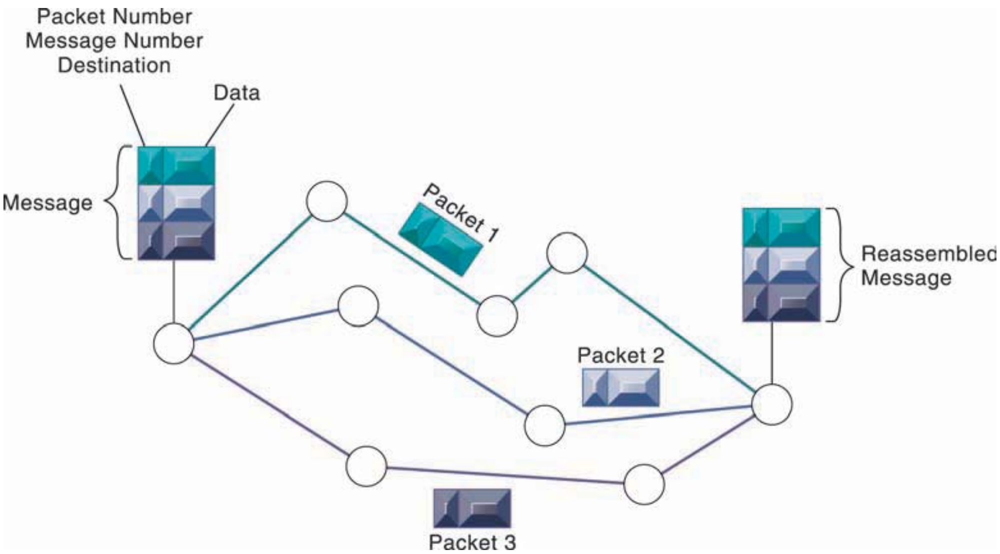
Client/server computing has largely replaced centralized mainframe computing in which nearly all of the processing takes place on a central large mainframe computer. Client/server computing has extended computing to departments, workgroups, factory floors, and other parts of the business that could not be served by a centralized architecture. The Internet is the largest implementation of client/server computing.

Packet Switching

Packet switching is a method of slicing digital messages into parcels called packets, sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destinations (see Figure 7.3). Prior to the development of packet switching, computer networks used leased, dedicated telephone circuits to communicate with other computers in remote locations. In circuit-switched networks, such as the telephone system, a complete point-to-point circuit is assembled, and then communication can proceed. These dedicated circuit-switching techniques were expensive and wasted available communications capacity—the circuit was maintained regardless of whether any data were being sent.

Packet switching makes much more efficient use of the communications capacity of a network. In packet-switched networks, messages are first broken down into small fixed bundles of data called packets. The packets include information for directing the packet to the right address and for checking transmission errors along with the data. The packets are transmitted over various communications channels using routers, each packet traveling independently. Packets of data originating at one source will be routed through many different paths and networks before being reassembled into the original message when they reach their destinations.

FIGURE 7.3 PACKED-SWITCHED NETWORKS AND PACKET COMMUNICATIONS



Data are grouped into small packets, which are transmitted independently over various communications channels and reassembled at their final destination.

TCP/IP and Connectivity

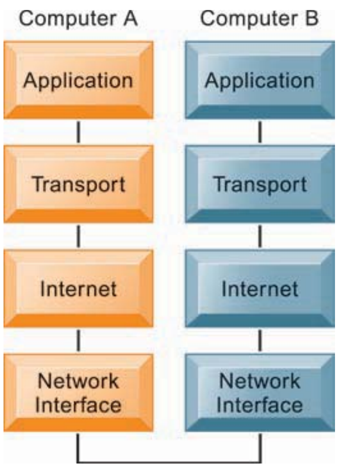
In a typical telecommunications network, diverse hardware and software components need to work together to transmit information. Different components in a network communicate with each other only by adhering to a common set of rules called protocols. A **protocol** is a set of rules and procedures governing transmission of information between two points in a network.

In the past, many diverse proprietary and incompatible protocols often forced business firms to purchase computing and communications equipment from a single vendor. But today, corporate networks are increasingly using a single, common, worldwide standard called **Transmission Control Protocol/Internet Protocol (TCP/IP)**. TCP/IP was developed during the early 1970s to support U.S. Department of Defense Advanced Research Projects Agency (DARPA) efforts to help scientists transmit data among different types of computers over long distances.

TCP/IP uses a suite of protocols, the main ones being TCP and IP. TCP refers to the Transmission Control Protocol, which handles the movement of data between computers. TCP establishes a connection between the computers, sequences the transfer of packets, and acknowledges the packets sent. IP refers to the Internet Protocol (IP), which is responsible for the delivery of packets and includes the disassembling and reassembling of packets during transmission. Figure 7.4 illustrates the four-layered Department of Defense reference model for TCP/IP, and the layers are described as follows:

1. *Application layer.* The Application layer enables client application programs to access the other layers and defines the protocols that applications use to exchange data. One of these application protocols is the Hypertext Transfer Protocol (HTTP), which is used to transfer Web page files.
2. *Transport layer.* The Transport layer is responsible for providing the Application layer with communication and packet services. This layer includes TCP and other protocols.
3. *Internet layer.* The Internet layer is responsible for addressing, routing, and packaging data packets called IP datagrams. The Internet Protocol is one of the protocols used in this layer.

FIGURE 7.4 THE TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP) REFERENCE MODEL



This figure illustrates the four layers of the TCP/IP reference model for communications.

4. *Network Interface layer.* At the bottom of the reference model, the Network Interface layer is responsible for placing packets on and receiving them from the network medium, which could be any networking technology.

Two computers using TCP/IP are able to communicate even if they are based on different hardware and software platforms. Data sent from one computer to the other passes downward through all four layers, starting with the sending computer's Application layer and passing through the Network Interface layer. After the data reach the recipient host computer, they travel up the layers and are reassembled into a format the receiving computer can use. If the receiving computer finds a damaged packet, it asks the sending computer to retransmit it. This process is reversed when the receiving computer responds.

7.2 Communications Networks

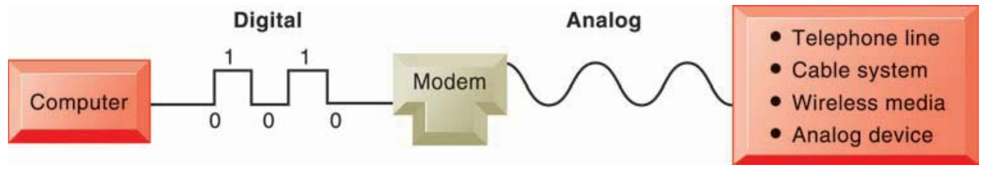
Let's look more closely at alternative networking technologies available to businesses.

SIGNALS: DIGITAL VS. ANALOG

There are two ways to communicate a message in a network: either using an analog signal or a digital signal. An *analog signal* is represented by a continuous waveform that passes through a communications medium and has been used for voice communication. The most common analog devices are the telephone handset, the speaker on your computer, or your iPod earphone, all of which create analog waveforms that your ear can hear.

A *digital signal* is a discrete, binary waveform, rather than a continuous waveform. Digital signals communicate information as strings of two discrete states: one bit and zero bits, which are represented as on-off electrical pulses. Computers use digital signals and require a modem to convert these digital signals into analog signals that can be sent over (or received from) telephone lines, cable lines, or wireless media that use analog signals (see Figure 7.5). **Modem** stands for modulator-demodulator. Cable modems connect your computer to the Internet using a cable network. DSL modems connect your computer to the Internet using a telephone company's landline network. Wireless modems perform the same function as traditional modems, connecting your computer to a wireless network that could be a cell phone network, or a Wi-Fi network. Without modems, computers could not communicate with one another using analog networks (which include the telephone system and cable networks).

FIGURE 7.5 FUNCTIONS OF THE MODEM



A modem is a device that translates digital signals into analog form (and vice versa) so that computers can transmit data over analog networks such as telephone and cable networks.

TYPES OF NETWORKS

There are many different kinds of networks and ways of classifying them. One way of looking at networks is in terms of their geographic scope (see Table 7.1).

Local Area Networks

If you work in a business that uses networking, you are probably connecting to other employees and groups via a local area network. A **local area network (LAN)** is designed to connect personal computers and other digital devices within a half-mile or 500-meter radius. LANs typically connect a few computers in a small office, all the computers in one building, or all the computers in several buildings in close proximity. LANs also are used to link to long-distance wide area networks (WANs, described later in this section) and other networks around the world using the Internet.

Review Figure 7.1, which could serve as a model for a small LAN that might be used in an office. One computer is a dedicated network file server, providing users with access to shared computing resources in the network, including software programs and data files.

The server determines who gets access to what and in which sequence. The router connects the LAN to other networks, which could be the Internet or another corporate network, so that the LAN can exchange information with networks external to it. The most common LAN operating systems are Windows, Linux, and Novell. Each of these network operating systems supports TCP/IP as their default networking protocol.

Ethernet is the dominant LAN standard at the physical network level, specifying the physical medium to carry signals between computers, access control rules, and a standardized set of bits used to carry data over the system. Originally, Ethernet supported a data transfer rate of 10 megabits per second (Mbps). Newer versions, such as Gigabit Ethernet, support a data transfer rate of 1 gigabit per second (Gbps), respectively, and are used in network backbones.

The LAN illustrated in Figure 7.1 uses a client/server architecture where the network operating system resides primarily on a single file server, and the server provides much of the control and resources for the network. Alternatively, LANs may use a peer-to-peer architecture. A peer-to-peer network treats all processors equally and is used primarily in small networks with 10 or fewer users. The various computers on the network can exchange data by direct access and can share peripheral devices without going through a separate server.

In LANs using the Windows Server family of operating systems, the **peer-to-peer** architecture is called the *workgroup network model*, in which a small group of computers can share resources, such as files, folders, and printers, over the

TABLE 7.1 TYPES OF NETWORKS

TYPE	AREA
Local area network (LAN)	Up to 500 meters (half a mile); an office or floor of a building
Campus area network (CAN)	Up to 1,000 meters (a mile); a college campus or corporate facility
Metropolitan area network (MAN)	A city or metropolitan area
Wide area network (WAN)	A transcontinental or global area

network without a dedicated server. The *Windows domain network model*, in contrast, uses a dedicated server to manage the computers in the network.

Larger LANs have many clients and multiple servers, with separate servers for specific services, such as storing and managing files and databases (file servers or database servers), managing printers (print servers), storing and managing e-mail (mail servers), or storing and managing Web pages (Web servers).

Metropolitan and Wide Area Networks

Wide area networks (WANs) span broad geographical distances—entire regions, states, continents, or the entire globe. The most universal and powerful WAN is the Internet. Computers connect to a WAN through public networks, such as the telephone system or private cable systems, or through leased lines or satellites. A **metropolitan area network (MAN)** is a network that spans a metropolitan area, usually a city and its major suburbs. Its geographic scope falls between a WAN and a LAN.

TRANSMISSION MEDIA AND TRANSMISSION SPEED

Networks use different kinds of physical transmission media, including twisted pair wire, coaxial cable, fiber optics, and media for wireless transmission. Each has advantages and limitations. A wide range of speeds is possible for any given medium depending on the software and hardware configuration. Table 7.2 compares these media.

Bandwidth: Transmission Speed

The total amount of digital information that can be transmitted through any telecommunications medium is measured in bits per second (bps). One signal change, or cycle, is required to transmit one or several bits; therefore, the transmission capacity of each type of telecommunications medium is a function of its frequency. The number of cycles per second that can be sent through that medium is measured in **hertz**—one hertz is equal to one cycle of the medium.

TABLE 7.2 PHYSICAL TRANSMISSION MEDIA

TRANSMISSION MEDIUM	DESCRIPTION	SPEED
Twisted pair wire (CAT 5)	Strands of copper wire twisted in pairs for voice and data communications. CAT 5 is the most common 10 Mbps LAN cable. Maximum recommended run of 100 meters.	10 Mbps to 1 Gbps
Coaxial cable	Thickly insulated copper wire, which is capable of high-speed data transmission and less subject to interference than twisted wire. Currently used for cable TV and for networks with longer runs (more than 100 meters).	Up to 1 Gbps
Fiber optic cable	Strands of clear glass fiber, transmitting data as pulses of light generated by lasers. Useful for high-speed transmission of large quantities of data. More expensive than other physical transmission media and harder to install; often used for network backbone.	500 Kbps to 6+Tbps
Wireless transmission media	Based on radio signals of various frequencies and includes both terrestrial and satellite microwave systems and cellular networks. Used for long-distance, wireless communication and Internet access.	Up to 600+ Mbps

The range of frequencies that can be accommodated on a particular telecommunications channel is called its **bandwidth**. The bandwidth is the difference between the highest and lowest frequencies that can be accommodated on a single channel. The greater the range of frequencies, the greater the bandwidth and the greater the channel's transmission capacity.

7.3 THE GLOBAL INTERNET

We all use the Internet, and many of us can't do without it. It's become an indispensable personal and business tool. But what exactly is the Internet? How does it work, and what does Internet technology have to offer for business? Let's look at the most important Internet features.

WHAT IS THE INTERNET?

The Internet has become the world's most extensive, public communication system that now rivals the global telephone system in reach and range. It's also the world's largest implementation of client/server computing and internetworking, linking millions of individual networks all over the world. This global network of networks began in the early 1970s as a U.S. Department of Defense network to link scientists and university professors around the world.

Most homes and small businesses connect to the Internet by subscribing to an Internet service provider. An **Internet service provider (ISP)** is a commercial organization with a permanent connection to the Internet that sells temporary connections to retail subscribers. EarthLink, NetZero, AT&T, and Time Warner are ISPs. Individuals also connect to the Internet through their business firms, universities, or research centers that have designated Internet domains.

There are a variety of services for ISP Internet connections. Connecting via a traditional telephone line and modem, at a speed of 56.6 kilobits per second (Kbps) used to be the most common form of connection worldwide, but it has been largely replaced by broadband connections. Digital subscriber line, cable, satellite Internet connections, and T lines provide these broadband services.

Digital subscriber line (DSL) technologies operate over existing telephone lines to carry voice, data, and video at transmission rates ranging from 385 Kbps all the way up to 40 Mbps, depending on usage patterns and distance. **Cable Internet connections** provided by cable television vendors use digital cable coaxial lines to deliver high-speed Internet access to homes and businesses. They can provide high-speed access to the Internet of up to 50 Mbps, although most providers offer service ranging from 1 Mbps to 6 Mbps. In areas where DSL and cable services are unavailable, it is possible to access the Internet via satellite, although some satellite Internet connections have slower upload speeds than other broadband services.

T1 and T3 are international telephone standards for digital communication. They are leased, dedicated lines suitable for businesses or government agencies requiring high-speed guaranteed service levels. **T1 lines** offer guaranteed delivery at 1.54 Mbps, and T3 lines offer delivery at 45 Mbps. The Internet does not provide similar guaranteed service levels, but simply "best effort."

INTERNET ADDRESSING AND ARCHITECTURE

The Internet is based on the TCP/IP networking protocol suite described earlier in this chapter. Every computer on the Internet is assigned a unique **Internet**

Protocol (IP) address, which currently is a 32-bit number represented by four strings of numbers ranging from 0 to 255 separated by periods. For instance, the IP address of www.microsoft.com is 207.46.250.119.

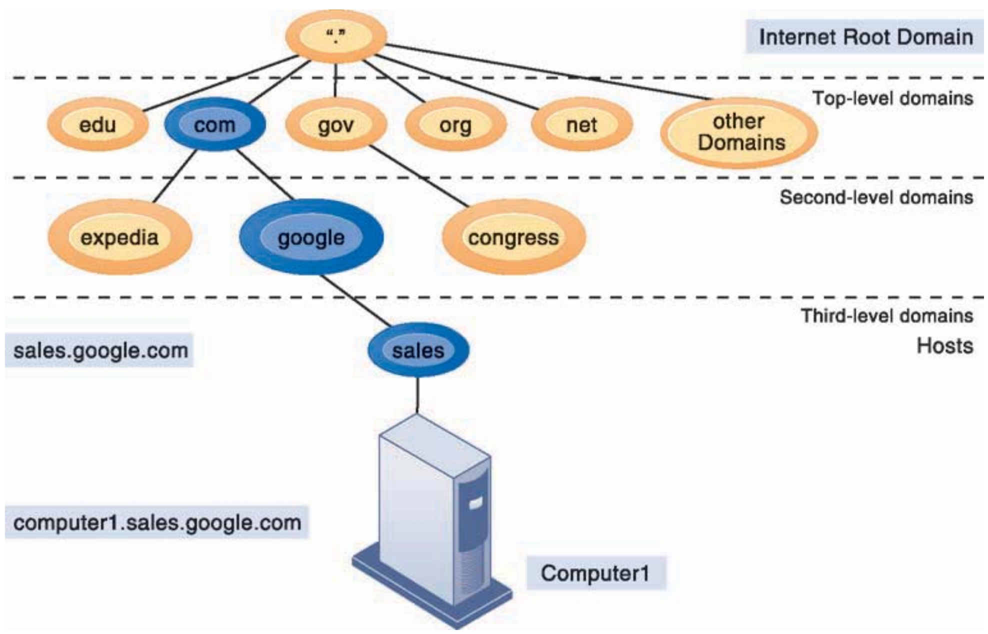
When a user sends a message to another user on the Internet, the message is first decomposed into packets using the TCP protocol. Each packet contains its destination address. The packets are then sent from the client to the network server and from there on to as many other servers as necessary to arrive at a specific computer with a known address. At the destination address, the packets are reassembled into the original message.

The Domain Name System

Because it would be incredibly difficult for Internet users to remember strings of 12 numbers, the **Domain Name System (DNS)** converts domain names to IP addresses. The **domain name** is the English-like name that corresponds to the unique 32-bit numeric IP address for each computer connected to the Internet. DNS servers maintain a database containing IP addresses mapped to their corresponding domain names. To access a computer on the Internet, users need only specify its domain name.

DNS has a hierarchical structure (see Figure 7.6). At the top of the DNS hierarchy is the root domain. The child domain of the root is called a top-level domain, and the child domain of a top-level domain is called is a second-level domain. Top-level domains are two- and three-character names you are familiar with from surfing the Web, for example, .com, .edu, .gov, and the various country codes such as .ca for Canada or .it for Italy. Second-level domains have two parts, designating a top-level name and a second-level name—such as buy.com, nyu.edu, or amazon.ca. A host name at the bottom of the hierarchy designates a specific computer on either the Internet or a private network.

FIGURE 7.6 THE DOMAIN NAME SYSTEM



Domain Name System is a hierarchical system with a root domain, top-level domains, second-level domains, and host computers at the third level.

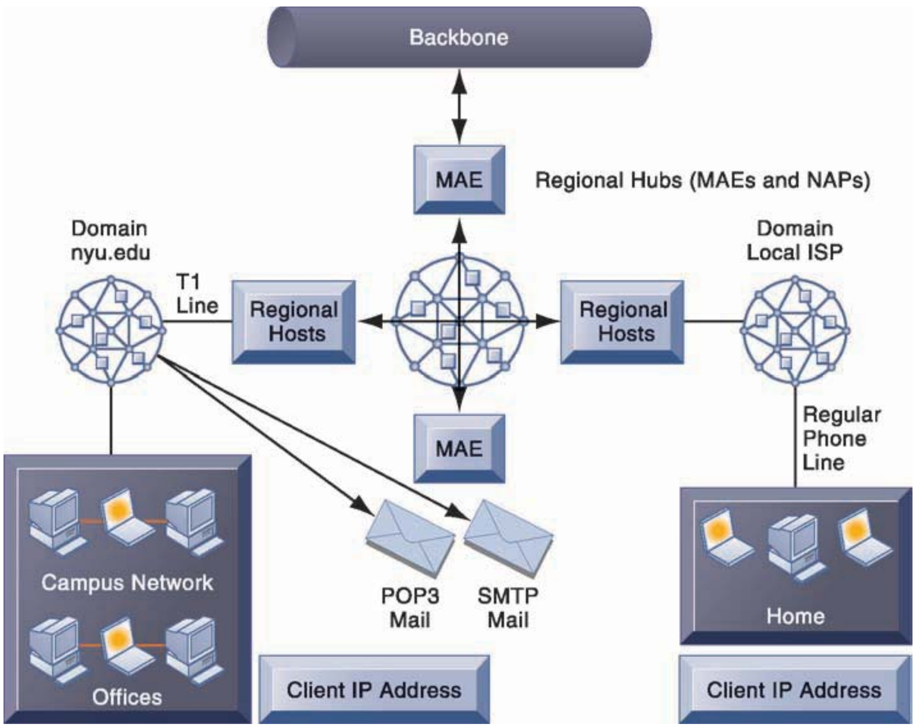
The most common domain extensions currently available and officially approved are shown in the following list. Countries also have domain names such as .uk, .au, and .fr (United Kingdom, Australia, and France, respectively), and there is a new class of "internationalized" top-level domains that use non-English characters (ICANN, 2010). In the future, this list will expand to include many more types of organizations and industries.

.com	Commercial organizations/businesses
.edu	Educational institutions
.gov	U.S. government agencies
.mil	U.S. military
.net	Network computers
.org	Nonprofit organizations and foundations
.biz	Business firms
.info	Information providers

Internet Architecture and Governance

Internet data traffic is carried over transcontinental high-speed backbone networks that generally operate in the range of 45 Mbps to 2.5 Gbps (see Figure 7.7). These trunk lines are typically owned by long-distance telephone companies (called *network service providers*) or by national governments.

FIGURE 7.7 INTERNET NETWORK ARCHITECTURE



The Internet backbone connects to regional networks, which in turn provide access to Internet service providers, large firms, and government institutions. Network access points (NAPs) and metropolitan area exchanges (MAEs) are hubs where the backbone intersects regional and local networks and where backbone owners connect with one another.

Local connection lines are owned by regional telephone and cable television companies in the United States that connect retail users in homes and businesses to the Internet. The regional networks lease access to ISPs, private companies, and government institutions.

Each organization pays for its own networks and its own local Internet connection services, a part of which is paid to the long-distance trunk line owners. Individual Internet users pay ISPs for using their service, and they generally pay a flat subscription fee, no matter how much or how little they use the Internet. A debate is now raging on whether this arrangement should continue or whether heavy Internet users who download large video and music files should pay more for the bandwidth they consume. The Interactive Session on Organizations explores this topic, by examining the pros and cons of network neutrality.

No one "owns" the Internet, and it has no formal management. However, worldwide Internet policies are established by a number of professional organizations and government bodies, including the Internet Architecture Board (IAB), which helps define the overall structure of the Internet; the Internet Corporation for Assigned Names and Numbers (ICANN), which assigns IP addresses; and the World Wide Web Consortium (W3C), which sets Hypertext Markup Language and other programming standards for the Web.

These organizations influence government agencies, network owners, ISPs, and software developers with the goal of keeping the Internet operating as efficiently as possible. The Internet must also conform to the laws of the sovereign nation-states in which it operates, as well as the technical infrastructures that exist within the nation-states. Although in the early years of the Internet and the Web there was very little legislative or executive interference, this situation is changing as the Internet plays a growing role in the distribution of information and knowledge, including content that some find objectionable.

The Future Internet: IPv6 and Internet2

The Internet was not originally designed to handle the transmission of massive quantities of data and billions of users. Because many corporations and governments have been given large blocks of millions of IP addresses to accommodate current and future workforces, and because of sheer Internet population growth, the world is about to run out of available IP addresses using the old addressing convention. The old addressing system is being replaced by a new version of the IP addressing schema called **IPv6** (Internet Protocol version 6), which contains 128-bit addresses (2 to the power of 128), or more than a quadrillion possible unique addresses. IPv6 is not compatible with the existing Internet addressing system, so the transition to the new standard will take years.

Internet2 is an advanced networking consortium representing over 350 U.S. universities, private businesses, and government agencies working with 66,000 institutions across the United States and international networking partners from more than 50 countries. To connect these communities, Internet2 developed a high-capacity 100 Gbps network that serves as a testbed for leading-edge technologies that may eventually migrate to the public Internet, including telemedicine, distance learning, and other advanced applications not possible with consumer-grade Internet services. The fourth generation of this network is being rolled out to provide 8.8 terabits of capacity.

INTERACTIVE SESSION: ORGANIZATIONS

THE BATTLE OVER NET NEUTRALITY

What kind of Internet user are you? Do you primarily use the Net to do a little e-mail and look up phone numbers? Or are you online all day, watching YouTube videos, downloading music files, or playing online games? If you have a smartphone, do you use it to make calls and check the Web every so often, or do you stream TV shows and movies on a regular basis? If you're a power Internet or smartphone user, you are consuming a great deal of bandwidth, and hundreds of millions of people like you might start to slow the Internet down. YouTube consumed as much bandwidth in 2007 as the entire Internet did in 2000, and AT&T's mobile network will carry more data in the first two months of 2015 than in all of 2010.

If user demand for the Internet overwhelms network capacity, the Internet might not come to a screeching halt, but users would be faced with very sluggish download speeds and slow performance of Netflix, Spotify, YouTube, and other data-heavy services. Heavy use of iPhones in urban areas such as New York and San Francisco has already degraded service on the AT&T wireless network. AT&T reports that 3 percent of its subscriber base accounts for 40 percent of its data traffic.

Some analysts believe that as digital traffic on the Internet grows, even at a rate of 50 percent per year, the technology for handling all this traffic is advancing at an equally rapid pace. But regardless of what happens with Internet infrastructure, costs for Internet providers will continue to increase, and prominent media companies are searching for new revenue streams to meet those costs. One solution is to make Internet users pay for the amount of bandwidth they use. But metering Internet use is not universally accepted, because of an ongoing debate about network neutrality.

Network neutrality is the idea that Internet service providers must allow customers equal access to content and applications, regardless of the source or nature of the content. Presently, the Internet is indeed neutral: all Internet traffic is treated equally on a first-come, first-served basis by Internet backbone owners. However, this arrangement prevents telecommunications and cable companies from charging differentiated prices based on the amount of bandwidth consumed by content being delivered over the Internet. These companies believe that differentiated pricing is "the fairest way" to finance necessary investments in their network infrastructures.

Internet service providers point to the upsurge in piracy of copyrighted materials over the Internet. Comcast, the second largest U.S. Internet service provider, reported that illegal file sharing of copyrighted material was consuming 50 percent of its network capacity. In 2008, the company slowed down transmission of BitTorrent files used extensively for piracy and illegal sharing of copyrighted materials, including video. The Federal Communications Commission (FCC) ruled that Comcast had to stop slowing peer-to-peer traffic in the name of network management. Comcast then filed a lawsuit challenging the FCC's authority to enforce network neutrality. In April 2010, a federal appeals court ruled in favor of Comcast that the FCC did not have the authority to regulate how an Internet provider manages its network. This was a considerable blow to net neutrality. In late 2010, Comcast reportedly began charging Level 3 Communications, which helps stream Netflix's movies, an additional fee for continued normal service. Level 3 asked the FCC to investigate the action.

Groups favoring net neutrality are pushing Congress to find ways to regulate the industry to prevent network providers from adopting Comcast-like practices. The strange alliance of net neutrality advocates includes MoveOn.org, the Christian Coalition, the American Library Association, every major consumer group, and a host of bloggers and small businesses, as well as streaming-video services like Netflix.

Net neutrality advocates argue that the risk of censorship increases when network operators can selectively block or slow access to certain content such as Netflix video streams or access to competing low-cost services such as Skype. Proponents of net neutrality also argue that a neutral Internet encourages everyone to innovate without permission from the phone and cable companies or other authorities, and this level playing field has spawned countless new businesses. Allowing unrestricted information flow becomes essential to free markets and democracy as commerce and society increasingly move online.

Network owners believe regulation to enforce net neutrality will impede U.S. competitiveness by stifling innovation, discouraging capital expenditures for new networks, and curbing their networks' ability to cope with the exploding demand for Internet and wireless traffic. U.S. Internet service lags behind many other nations in overall speed, cost, and quality of service, adding credibility to this argument.

And with enough options for Internet access, regulation would not be essential for promoting net neutrality. Dissatisfied consumers could simply switch to providers who enforce net neutrality and allow unlimited Internet use.

In December 2010, the FCC approved measures that would allow the federal government to regulate Internet traffic. Broadband providers would be required to provide information regarding Internet speeds and service to their subscribers, and they could not block access to sites or products that compete against their own products. However, the regulations did not officially safeguard net neutrality, and wireless providers may block applications that use too much bandwidth.

Wireless providers have already moved to develop tiered plans that charge heavy bandwidth users larger service fees, and online content providers have struck exclusive deals with distributors that leave their competitors at a disadvantage. For example, in 2012, Comcast struck a deal with Microsoft to provide streaming video via its Xfinity TV service through the Xbox 360 that does not count against its broadband data cap of 250 gigabytes per month. This gives Comcast's television programming an edge over rival streaming shows, which will consume subscribers' data allotment. Netflix and other competitors are incensed, arguing that this flies in the face of the concept of net neutrality and represents an anti-competitive practice.

In 2011, nearly every broadband provider instituted a cap on data, charging additional fees to users that go over that limit. Many analysts have long argued in favor of these caps, but deals like those between Comcast and Microsoft are likely to draw the ire of the FCC going forward. Currently, the net neutrality laws on the books are riddled with loopholes. For example, they allow broadband providers to allocate portions of their networks for special "managed" services. Still, public sentiment in favor of net neutrality is still strong.

Sources: Eduardo Porter, "Keeping the Internet Neutral," *The New York Times*, May 8, 2012; Matt Peckham, "Netflix CEO Takes Swing at Comcast Xfinity over Net Neutrality," *Time Techland*, April 16, 2012; Greg Bensinger, "AT&T Ends All-You-Can-Eat," *The Wall Street Journal*, March 1, 2012; John Eggerton, "Net Neutrality Rules Signed Off On By OMB," *Broadcasting & Cable*, September 13, 2011; "FCC Approves Net Neutrality But With Concessions," *eWeek*, December 22, 2010; and Brian Stelter, "Comcast Fee Ignites Fight Over Videos on Internet," *The New York Times*, November 30, 2010.

CASE STUDY QUESTIONS

1. What is network neutrality? Why has the Internet operated under net neutrality up to this point in time?
2. Who's in favor of net neutrality? Who's opposed? Why?
3. What would be the impact on individual users, businesses, and government if Internet providers switched to a tiered service model?
4. Are you in favor of legislation enforcing network neutrality? Why or why not?

INTERNET SERVICES AND COMMUNICATION TOOLS

The Internet is based on client/server technology. Individuals using the Internet control what they do through client applications on their computers, such as Web browser software. The data, including e-mail messages and Web pages, are stored on servers. A client uses the Internet to request information from a particular Web server on a distant computer, and the server sends the requested information back to the client over the Internet. Chapters 5 and 6 describe how Web servers work with application servers and database servers to access information from an organization's internal information systems applications and their associated databases. Client platforms today include not only PCs and other computers but also cell phones, small handheld digital devices, and other information appliances.

Internet Services

A client computer connecting to the Internet has access to a variety of services. These services include e-mail, chatting and instant messaging, electronic discussion groups, **Telnet, File Transfer Protocol (FTP)**, and the Web. Table 7.3 provides a brief description of these services.

Each Internet service is implemented by one or more software programs. All of the services may run on a single server computer, or different services may be allocated to different machines. Figure 7.8 illustrates one way that these services can be arranged in a multitiered client/server architecture.

E-mail enables messages to be exchanged from computer to computer, with capabilities for routing messages to multiple recipients, forwarding messages, and attaching text documents or multimedia files to messages. Most e-mail today is sent through the Internet. The cost of e-mail is far lower than equivalent voice, postal, or overnight delivery costs, making the Internet a very inexpensive and rapid communications medium. Most e-mail messages arrive anywhere in the world in a matter of seconds.

Nearly 90 percent of U.S. workplaces have employees communicating interactively using **chat** or instant messaging tools. Chatting enables two or more people who are simultaneously connected to the Internet to hold live, interactive conversations. Chat systems now support voice and video chat as well as written conversations. Many online retail businesses offer chat services on their Web sites to attract visitors, to encourage repeat purchases, and to improve customer service.

Instant messaging is a type of chat service that enables participants to create their own private chat channels. The instant messaging system alerts the user whenever someone on his or her private list is online so that the user can initiate a chat session with other individuals. Instant messaging systems for consumers include Yahoo! Messenger, Google Talk, and Windows Messenger. Companies concerned with security use proprietary communications and messaging systems such as IBM Sametime.

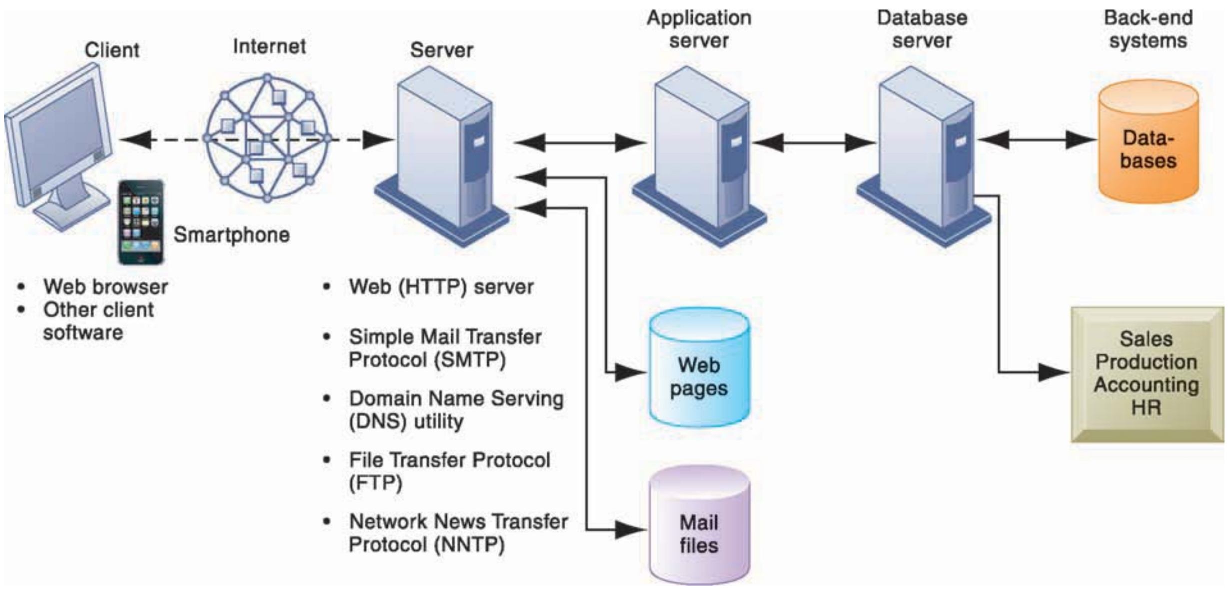
Newsgroups are worldwide discussion groups posted on Internet electronic bulletin boards on which people share information and ideas on a defined topic, such as radiology or rock bands. Anyone can post messages on these bulletin boards for others to read. Many thousands of groups exist that discuss almost all conceivable topics.

Employee use of e-mail, instant messaging, and the Internet is supposed to increase worker productivity, but the accompanying Interactive Session on

TABLE 7.3 MAJOR INTERNET SERVICES

CAPABILITY	FUNCTIONS SUPPORTED
E-mail	Person-to-person messaging; document sharing
Chatting and instant messaging	Interactive conversations
Newsgroups	Discussion groups on electronic bulletin boards
Telnet	Logging on to one computer system and doing work on another
File Transfer Protocol (FTP)	Transferring files from computer to computer
World Wide Web	Retrieving, formatting, and displaying information (including text, audio, graphics, and video) using hypertext links

FIGURE 7.8 CLIENT/SERVER COMPUTING ON THE INTERNET



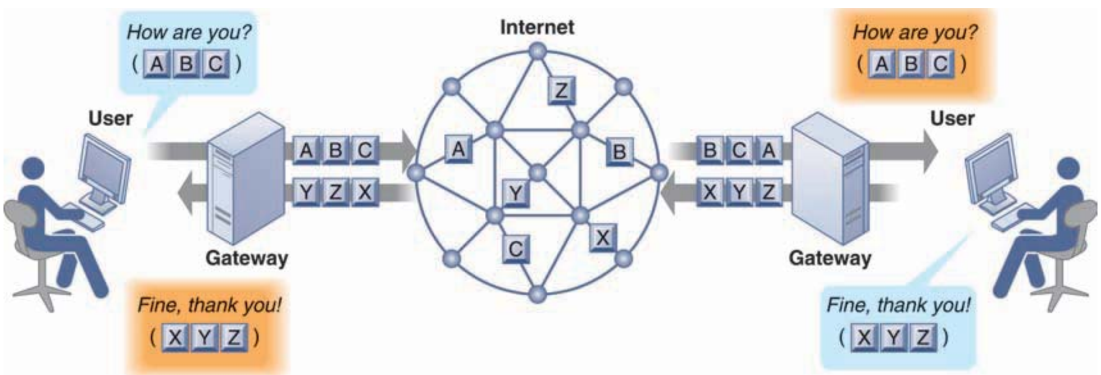
Client computers running Web browser and other software can access an array of services on servers over the Internet. These services may all run on a single server or on multiple specialized servers.

Management shows that this may not always be the case. Many company managers now believe they need to monitor and even regulate their employees' online activity. But is this ethical? Although there are some strong business reasons why companies may need to monitor their employees' e-mail and Web activities, what does this mean for employee privacy?

Voice over IP

The Internet has also become a popular platform for voice transmission and corporate networking. **Voice over IP (VoIP)** technology delivers voice information in digital form using packet switching, avoiding the tolls charged by local and long-distance telephone networks (see Figure 7.9). Calls that

FIGURE 7.9 HOW VOICE OVER IP WORKS



A VoIP phone call digitizes and breaks up a voice message into data packets that may travel along different routes before being reassembled at the final destination. A processor nearest the call's destination, called a gateway, arranges the packets in the proper order and directs them to the telephone number of the receiver or the IP address of the receiving computer.

INTERACTIVE SESSION: MANAGEMENT

MONITORING EMPLOYEES ON NETWORKS: UNETHICAL OR GOOD BUSINESS?

When you were at work, how many minutes (or hours) did you spend on Facebook today? Did you send personal e-mail or visit some sports Web sites? If so, you're not alone. According to a Nucleus Research study, 77 percent of workers with Facebook accounts use them during work hours. A Ponemon Institute study reported that the average employee wastes approximately 30 percent of the workday on non-work-related Web browsing, while other studies report as many as 90 percent of employees receive or send personal e-mail at work.

This behavior creates serious business problems. Checking e-mail, responding to instant messages, or sneaking in a brief YouTube video creates a series of nonstop interruptions that divert employee attention from the job tasks they are supposed to be performing. According to Basex, a New York City business research company, these distractions result in $650 billion in lost productivity each year!

Many companies have begun monitoring employee use of e-mail and the Internet, sometimes without their knowledge. A 2010 study from Proofpoint Plus found that more than one in three large U.S corporations assign staff to read or analyze employee e-mail. Another recent survey from the American Management Association (AMA) and the ePolicy Institute found that two out of three of the small, medium, and large companies surveyed monitored Web use. Instant messaging and text message monitoring are also increasing. Although U.S. companies have the legal right to monitor employee Internet and e-mail activity while they are at work, is such monitoring unethical, or is it simply good business?

Managers worry about the loss of time and employee productivity when employees are focusing on personal rather than company business. Too much time on personal business translates into lost revenue. Some employees may even be billing time they spend pursuing personal interests online to clients, thus overcharging them.

If personal traffic on company networks is too high, it can also clog the company's network so that legitimate business work cannot be performed. Procter & Gamble (P&G) found that on an average day, employees were listening to 4,000 hours of music on Pandora and viewing 50,000 five-minute YouTube videos. These activities involved streaming huge quantities of data, which slowed down P&G's Internet connection.

When employees use e-mail or the Web (including social networks) at employer facilities or with employer equipment, anything they do, including anything illegal, carries the company's name. Therefore, the employer can be traced and held liable. Management in many firms fear that racist, sexually explicit, or other potentially offensive material accessed or traded by their employees could result in adverse publicity and even lawsuits for the firm. Even if the company is found not to be liable, responding to lawsuits could run up huge legal bills. Symantec's 2011 Social Media Protection Flash Poll found that the average litigation cost for companies with social media incidents ran over $650,000.

Companies also fear leakage of confidential information and trade secrets through e-mail or social networks. Another survey conducted by the American Management Association and the ePolicy Institute found that 14 percent of the employees polled admitted they had sent confidential or potentially embarrassing company e-mails to outsiders.

U.S. companies have the legal right to monitor what employees are doing with company equipment during business hours. The question is whether electronic surveillance is an appropriate tool for maintaining an efficient and positive workplace. Some companies try to ban all personal activities on corporate networks—zero tolerance. Others block employee access to specific Web sites or social sites, closely monitor e-mail messages, or limit personal time on the Web.

For example, P&G blocks Netflix and has asked employees to limit their use of Pandora. It still allows some YouTube viewing, and is not blocking access to social networking sites because staff use them for digital marketing campaigns. Ajax Boiler in Santa Ana, California, uses software from SpectorSoft Corporation that records all the Web sites employees visit, time spent at each site, and all e-mails sent. Financial services and investment firm Wedbush Securities monitors the daily e-mails, instant messaging, and social networking activity of its 1,000-plus employees. The firm's e-mail monitoring software flags certain types of messages and keywords within messages for further investigation.

A number of firms have fired employees who have stepped out of bounds. A Proofpoint survey found that one in five large U.S. companies fired an employee for violating e-mail policies in the past year. Among managers who fired employees for Internet misuse, the majority did so because the employees' e-mail contained sensitive, confidential, or embarrassing information.

No solution is problem free, but many consultants believe companies should write corporate policies on employee e-mail, social media, and Web use. The policies should include explicit ground rules that state, by position or level, under what circumstances employees can use company facilities for e-mail, blogging, or Web surfing. The policies should also inform employees whether these activities are monitored and explain why.

IBM now has "social computing guidelines" that cover employee activity on sites such as Facebook and Twitter. The guidelines urge employees not to conceal their identities, to remember that they are personally responsible for what they publish, and to refrain from discussing controversial topics that are not related to their IBM role.

The rules should be tailored to specific business needs and organizational cultures. For example, investment firms will need to allow many of their employees access to other investment sites. A company dependent on widespread information sharing, innovation, and independence could very well find that monitoring creates more problems than it solves.

Sources: Emily Glazer, "P&G Curbs Employees' Internet Use," *The Wall Street Journal*, April 4, 2012; David L. Barron, "Social Media: Frontier for Employee Disputes," *Baseline*, January 19, 2012; Jennifer Lawinski, "Social Media Costs Companies Bigtime," *Baseline*, August 29, 2011; Don Reisinger, "March Madness: The Great Productivity Killer," *CIO Insight,* March 18, 2011; "Seven Employee Monitoring Tips for Small Business," IT BusinessEdge, May 29, 2011; Catey Hill, "Things Your Boss Won't Tell You," *Smart Money,* January 12, 2011.

CASE STUDY QUESTIONS

1. Should managers monitor employee e-mail and Internet usage? Why or why not?

2. Describe an effective e-mail and Web use policy for a company.

3. Should managers inform employees that their Web behavior is being monitored? Or should managers monitor secretly? Why or why not?

would ordinarily be transmitted over public telephone networks travel over the corporate network based on the Internet Protocol, or the public Internet. Voice calls can be made and received with a computer equipped with a microphone and speakers or with a VoIP-enabled telephone.

Cable firms such as Time Warner and Cablevision provide VoIP service bundled with their high-speed Internet and cable offerings. Skype offers free VoIP worldwide using a peer-to-peer network, and Google has its own free VoIP service.

Although there are up-front investments required for an IP phone system, VoIP can reduce communication and network management costs by 20 to 30 percent. For example, VoIP saves Virgin Entertainment Group $700,000 per year in long-distance bills. In addition to lowering long-distance costs and eliminating monthly fees for private lines, an IP network provides a single voice-data infrastructure for both telecommunications and computing services. Companies no longer have to maintain separate networks or provide support services and personnel for each different type of network.

Another advantage of VoIP is its flexibility. Unlike the traditional telephone network, phones can be added or moved to different offices without rewiring or reconfiguring the network. With VoIP, a conference call is arranged by a simple click-and-drag operation on the computer screen to select the names of the conferees. Voice mail and e-mail can be combined into a single directory.

Unified Communications

In the past, each of the firm's networks for wired and wireless data, voice communications, and videoconferencing operated independently of each other and had to be managed separately by the information systems department. Now, however, firms are able to merge disparate communications modes into a single universally accessible service using unified communications technology. **Unified communications** integrates disparate channels for voice communications, data communications, instant messaging, e-mail, and electronic conferencing into a single experience where users can seamlessly switch back and forth between different communication modes. Presence technology shows whether a person is available to receive a call. Companies will need to examine how work flows and business processes will be altered by this technology in order to gauge its value.

CenterPoint Properties, a major Chicago area industrial real estate company, used unified communications technology to create collaborative Web sites for each of its real estate deals. Each Web site provides a single point for accessing structured and unstructured data. Integrated presence technology lets team members e-mail, instant message, call, or videoconference with one click.

Virtual Private Networks

What if you had a marketing group charged with developing new products and services for your firm with members spread across the United States? You would want to be able to e-mail each other and communicate with the home office without any chance that outsiders could intercept the communications. In the past, one answer to this problem was to work with large private networking firms who offered secure, private, dedicated networks to customers. But this was an expensive solution. A much less-expensive solution is to create a virtual private network within the public Internet.

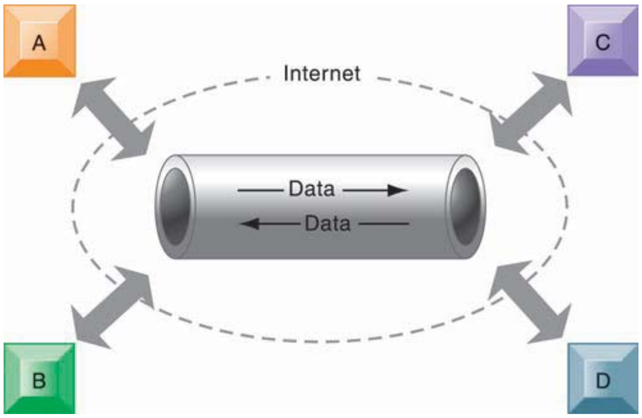
A **virtual private network (VPN)** is a secure, encrypted, private network that has been configured within a public network to take advantage of the economies of scale and management facilities of large networks, such as the Internet (see Figure 7.10). A VPN provides your firm with secure, encrypted communications at a much lower cost than the same capabilities offered by traditional non-Internet providers who use their private networks to secure communications. VPNs also provide a network infrastructure for combining voice and data networks.

Several competing protocols are used to protect data transmitted over the public Internet, including *Point-to-Point Tunneling Protocol (PPTP)*. In a process called tunneling, packets of data are encrypted and wrapped inside IP packets. By adding this wrapper around a network message to hide its content, business firms create a private connection that travels through the public Internet.

THE WEB

About 239 million people of all ages use the Web in the U.S.—three-quarters of the population. The Web is the most popular Internet service. It's a system with universally accepted standards for storing, retrieving, formatting, and displaying information using a client/server architecture. Web pages are formatted using

FIGURE 7.10 A VIRTUAL PRIVATE NETWORK USING THE INTERNET



This VPN is a private network of computers linked using a secure "tunnel" connection over the Internet. It protects data transmitted over the public Internet by encoding the data and "wrapping" them within the Internet Protocol (IP). By adding a wrapper around a network message to hide its content, organizations can create a private connection that travels through the public Internet.

hypertext with embedded links that connect documents to one another and that also link pages to other objects, such as sound, video, or animation files. When you click a graphic and a video clip plays, you have clicked a hyperlink. A typical **Web site** is a collection of Web pages linked to a home page.

Hypertext

Web pages are based on a standard Hypertext Markup Language (HTML), which formats documents and incorporates dynamic links to other documents and pictures stored in the same or remote computers (see Chapter 5). Web pages are accessible through the Internet because Web browser software operating your computer can request Web pages stored on an Internet host server using the **Hypertext Transfer Protocol (HTTP)**. HTTP is the communications standard used to transfer pages on the Web. For example, when you type a Web address in your browser, such as http://www.sec.gov, your browser sends an HTTP request to the sec.gov server requesting the home page of sec.gov.

HTTP is the first set of letters at the start of every Web address, followed by the domain name, which specifies the organization's server computer that is storing the document. Most companies have a domain name that is the same as or closely related to their official corporate name. The directory path and document name are two more pieces of information within the Web address that help the browser track down the requested page. Together, the address is called a **uniform resource locator (URL)**. When typed into a browser, a URL tells the browser software exactly where to look for the information. For example, in the URL *http://www.megacorp.com/content/features/082610.html*, *http* names the protocol used to display Web pages, *www.megacorp.com* is the domain name, *content/features* is the directory path that identifies where on the domain Web server the page is stored, and *082610.html* is the document name and the name of the format it is in (it is an HTML page).

Web Servers

A Web server is software for locating and managing stored Web pages. It locates the Web pages requested by a user on the computer where they are stored and delivers the Web pages to the user's computer. Server applications usually run on dedicated computers, although they can all reside on a single computer in small organizations.

The most common Web server in use today is Apache HTTP Server, which controls 65 percent of the market. Apache is an open source product that is free of charge and can be downloaded from the Web. Microsoft Internet Information Services (IIS) is the second most commonly used Web server, with 15 percent market share.

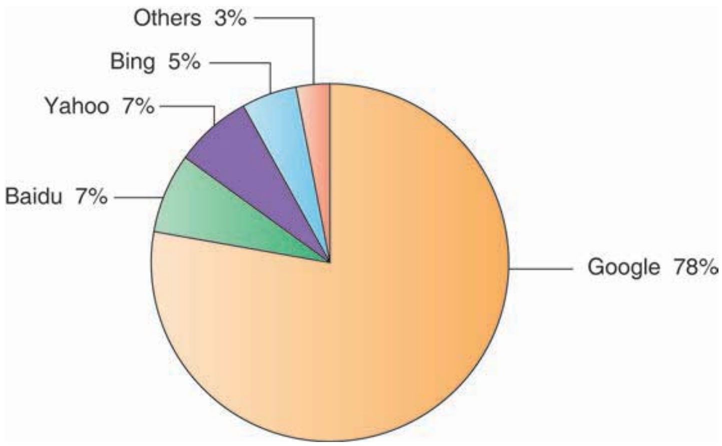
Searching for Information on the Web

No one knows for sure how many Web pages there really are. The surface Web is the part of the Web that search engines visit and about which information is recorded. For instance, Google visited about 400 billion pages in 2012, and this reflects a large portion of the publicly accessible Web page population. But there is a "deep Web" that contains an estimated 1 trillion additional pages, many of them proprietary (such as the pages of the *Wall Street Journal Online*, which cannot be visited without a subscription or access code) or that are stored in protected corporate databases.

Search Engines Obviously, with so many Web pages, finding specific Web pages that can help you or your business, nearly instantly, is an important problem. The question is, how can you find the one or two pages you really want and need out of billions of indexed Web pages? **Search engines** attempt to solve the problem of finding useful information on the Web nearly instantly, and, arguably, they are the "killer app" of the Internet era. Today's search engines can sift through HTML files, files of Microsoft Office applications, PDF files, as well as audio, video, and image files. There are hundreds of different search engines in the world, but the vast majority of search results are supplied by Google, Yahoo!, Baidu, and Microsoft's Bing search engine (see Figure 7.11).

Web search engines started out in the early 1990s as relatively simple software programs that roamed the nascent Web, visiting pages and gathering

FIGURE 7.11 TOP WEB SEARCH ENGINES



Google is the most popular search engine, handling 78 percent of Web searches.

Sources: Based on data from comScore Inc., September 2012.

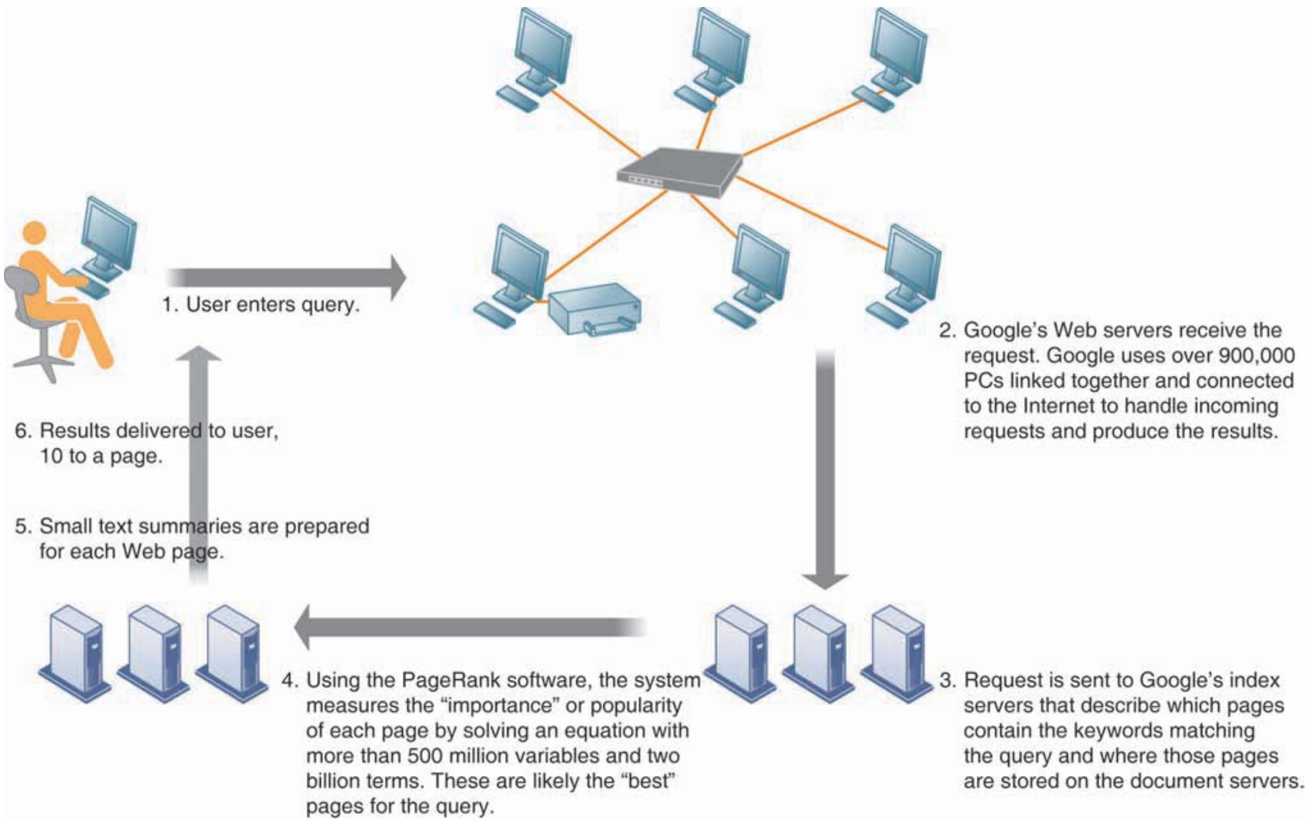
information about the content of each page. The first search engines were simple keyword indexes of all the pages they visited, leaving the user with lists of pages that may not have been truly relevant to their search.

In 1994, Stanford University computer science students David Filo and Jerry Yang created a hand-selected list of their favorite Web pages and called it "Yet Another Hierarchical Officious Oracle," or Yahoo. Yahoo was not initially a search engine but rather an edited selection of Web sites organized by categories the editors found useful, but currently relies on Microsoft for search results.

In 1998, Larry Page and Sergey Brin, two other Stanford computer science students, released their first version of Google. This search engine was different: Not only did it index each Web page's words but it also ranked search results based on the relevance of each page. Page patented the idea of a page ranking system (called PageRank System), which essentially measures the popularity of a Web page by calculating the number of sites that link to that page as well as the number of pages which it links to. The premise is that really popular Web pages are more "relevant" to users. Brin contributed a unique Web crawler program that indexed not only keywords on a page but also combinations of words (such as authors and the titles of their articles). These two ideas became the foundation for the Google search engine. Figure 7.12 illustrates how Google works.

Search engine Web sites are so popular that many people use them as their home page, the page where they start surfing the Web (see Chapter 10). Search engines are also the foundation for the fastest growing form of marketing and advertising, search engine marketing.

FIGURE 7.12 HOW GOOGLE WORKS



The Google search engine is continuously crawling the Web, indexing the content of each page, calculating its popularity, and storing the pages so that it can respond quickly to user requests to see a page. The entire process takes about one-half second.

Mobile Search With the growth of mobile smartphones and tablet computers, and with about 122 million Americans accessing the Internet via mobile devices, the nature of e-commerce and search is changing. Mobile search now makes up about 20 percent of all searches in 2012, and according to Google will expand rapidly in the next few years. Both Google and Yahoo have developed new search interfaces to make searching and shopping from smartphones more convenient. Amazon, for instance, sold over $1 billion in goods in 2012 through mobile searches of its store (Marin Software, 2012; Miller, 2012; eMarketer, 2011).

Search Engine Marketing Search engines have become major advertising platforms and shopping tools by offering what is now called **search engine marketing**. When users enter a search term at Google, Bing, Yahoo, or any of the other sites serviced by these search engines, they receive two types of listings: sponsored links, for which advertisers have paid to be listed (usually at the top of the search results page), and unsponsored "organic" search results. In addition, advertisers can purchase small text boxes on the side of search results pages. The paid, sponsored advertisements are the fastest growing form of Internet advertising and are powerful new marketing tools that precisely match consumer interests with advertising messages at the right moment. Search engine marketing monetizes the value of the search process. In 2012, search engine marketing generated $19.5 billion in revenue, over half of all online advertising ($37.3 billion). Google will account for over 40% of all online advertising in 2012. About 97% of Google's revenue of $39 billion in 2011 comes from online advertising, and 95% of the ad revenue comes from search engine marketing (Google,2012; eMarketer, 2012).

Because search engine marketing is so effective (it has the highest click-through rate and the highest return on ad investment), companies seek to optimize their Web sites for search engine recognition. The better optimized the page is, the higher a ranking it will achieve in search engine result listings. **Search engine optimization (SEO)** is the process of improving the quality and volume of Web traffic to a Web site by employing a series of techniques that help a Web site achieve a higher ranking with the major search engines when certain keywords and phrases are put in the search field. One technique is to make sure that the keywords used in the Web site description match the keywords likely to be used as search terms by prospective customers. For example, your Web site is more likely to be among the first ranked by search engines if it uses the keyword "lighting" rather than "lamps" if most prospective customers are searching for "lighting." It is also advantageous to link your Web site to as many other Web sites as possible because search engines evaluate such links to determine the popularity of a Web page and how it is linked to other content on the Web. Search engines can be gamed by scammers who create thousands of phony Web site pages and link them altogether, or link them to a single retailer's site in an attempt to fool Google's search engine. Firms can also pay so-called "link farms" to link to their site. Google changed its search algorithm in 2012. Code named "Penguin," the new algorithm examines the quality of links more carefully. The assumption is that the more links there are to a Web site, the more useful the Web site must be.

In general, search engines have been very helpful to small businesses that cannot afford large marketing campaigns. Because shoppers are looking for a specific product or service when they use search engines, they are what marketers call "hot prospects"—people who are looking for information and often intending to buy. Moreover, search engines charge only for click-throughs to a site. Merchants do not have to pay for ads that don't work, only for ads that receive a click. Consumers benefit from search engine marketing because ads for merchants appear only when consumers are looking for a specific product. There are no pop-ups, Flash animations, videos, interstitials, e-mails, or other irrelevant communications to deal with. Thus, search engine marketing saves consumers cognitive energy and reduces search costs (including the cost of transportation needed to physically search for products). In a recent study, the global value of search to both merchants and consumers was estimated to be more than $800 billion, with about 65 percent of the benefit going to consumers in the form of lower search costs and lower prices (McKinsey, 2011).

Social Search One problem with Google and mechanical search engines is that they are so thorough: enter a search for "ultra computers" and in .2 seconds you will receive over 300 million reponses! Search engines are not very discriminating. **Social search** is an effort to provide fewer, more relevant, and trustworthy search results based on a person's network of social contacts. In contrast to the top search engines that use a mathematical algorithm to find pages that satisfy your query, a social search Web site would review your friends' recommendations (and their friends'), their past Web visits, and their use of "Like" buttons.

For instance, Google has developed Google +1 as a social layer on top of its existing search engine. Users can place a +1 next to the Web sites they found helpful, and their friends will be notified automatically. Subsequent searches by their friends would list the +1 sites recommended by friends higher up on the page. Facebook's Like button is a similar social search tool. So far, neither Facebook nor Google has fully implemented a social search engine (Efrati, 2011). One problem with social search is that your close friends may not have intimate knowledge of topics you are exploring, or they may have tastes you don't appreciate. It's also possible your close friends don't have any knowledge about what you are searching for.

Semantic Search Another way for search engines to become more discriminating and helpful is to make search engines that could understand what it is we are really looking for. Called "semantic search" the goal is to build a search engine that could really understand human language and behavior. For instance, in 2012 Google's search engine began delivering more than millions of links. It started to give users more facts and direct answers, and to provide more relevant links to sites based on the search engines estimation of what the user intended, and even on the user's past search behavior. Google's search engine is trying to understand what people are most likely thinking about when they search for something. Google hopes to use its massive database of objects (people, places, things), and smart software, to provide users a better resulting than just millions of hits. For instance, do a search on "Lake Tahoe" and the search engine will return basic facts about Tahoe (altitude, average temperature, and local fish), a map, and hotel accommodations. (Efrati, 2012).

Although search engines were originally designed to search text documents, the explosion of photos and videos on the Internet created a demand for searching and classifying these visual objects. Facial recognition software can create a digital version of a human face. In 2012 Facebook introduced its facial recognition software and combined it with tagging, to create a new feature called Tag Suggest. The software creates a digital facial print, similar to a finger print. Users can put their own tagged photo on their timeline, and their friend's timelines. Once a person's photo is tagged, Facebook can pick that person out of a group photo, and identify for others who is in the photo. You can also search for people on Facebook using their digital image to find and identify them.

Intelligent Agent Shopping Bots Chapter 11 describes the capabilities of software agents with built-in intelligence that can gather or filter information and perform other tasks to assist users. **Shopping bots** use intelligent agent software for searching the Internet for shopping information. Shopping bots such as MySimon or Google Product Search can help people interested in making a purchase filter and retrieve information about products of interest, evaluate competing products according to criteria the users have established, and negotiate with vendors for price and delivery terms. Many of these shopping agents search the Web for pricing and availability of products specified by the user and return a list of sites that sell the item along with pricing information and a purchase link.

Web 2.0

Today's Web sites don't just contain static content—they enable people to collaborate, share information, and create new services and content online. These second-generation interactive Internet-based services are referred to as **Web 2.0**. If you have shared photos over the Internet at Flickr or another photo site, pinned a photo on Pinterest, posted a video to YouTube, created a blog, or added an app to your Facebook page, you've used some of these Web 2.0 services.

Web 2.0 has four defining features: interactivity, real-time user control, social participation (sharing), and user-generated content. The technologies and services behind these features include cloud computing, software mashups and apps, blogs, RSS, wikis, and social networks.

Mashups, which we introduced in Chapter 5, are software services that enable users and system developers to mix and match content or software components to create something entirely new. For example, Yahoo's photo storage and sharing site Flickr combines photos with other information about the images provided by users and tools to make it usable within other programming environments. Web 2.0 tools and services have fueled the creation of social networks and other online communities where people can interact with one another in the manner of their choosing.

A **blog**, the popular term for a Weblog, is a personal Web site that typically contains a series of chronological entries (newest to oldest) by its author, and links to related Web pages. The blog may include a *blogroll* (a collection of links to other blogs) and *trackbacks* (a list of entries in other blogs that refer to a post on the first blog). Most blogs allow readers to post comments on the blog entries as well. The act of creating a blog is often referred to as "blogging." Blogs can be hosted by a third-party service such as Blogger.com, TypePad.com, and Xanga.com, and blogging features have been incorporated into social networks such as Facebook and collaboration platforms such as Lotus Notes. WordPress is a leading open source blogging tool and content management system. **Microblogging**, used in Twitter, is a type of blogging that features short posts of 140 characters or less.

Blog pages are usually variations on templates provided by the blogging service or software. Therefore, millions of people without HTML skills of any kind can post their own Web pages and share content with others. The totality of blog-related Web sites is often referred to as the **blogosphere**. Although blogs have become popular personal publishing tools, they also have business uses (see Chapters 2 and 10).

If you're an avid blog reader, you might use RSS to keep up with your favorite blogs without constantly checking them for updates. **RSS**, which stands for

Really Simple Syndication or Rich Site Summary, pulls specified content from Web sites and feeds it automatically to users' computers. RSS reader software gathers material from the Web sites or blogs that you tell it to scan and brings new information from those sites to you. RSS readers are available through Web sites such as Google and Yahoo, and they have been incorporated into the major Web browsers and e-mail programs.

Blogs allow visitors to add comments to the original content, but they do not allow visitors to change the original posted material. **Wikis**, in contrast, are collaborative Web sites where visitors can add, delete, or modify content on the site, including the work of previous authors. Wiki comes from the Hawaiian word for "quick."

Wiki software typically provides a template that defines layout and elements common to all pages, displays user-editable software program code, and then renders the content into an HTML-based page for display in a Web browser. Some wiki software allows only basic text formatting, whereas other tools allow the use of tables, images, or even interactive elements, such as polls or games. Most wikis provide capabilities for monitoring the work of other users and correcting mistakes.

Because wikis make information sharing so easy, they have many business uses. The U.S. Department of Homeland Security's National Cyber Security Center (NCSC) deployed a wiki to facilitate collaboration among federal agencies on cybersecurity. NCSC and other agencies use the wiki for real-time information sharing on threats, attacks, and responses and as a repository for technical and standards information. Pixar Wiki is a collaborative community wiki for publicizing the work of Pixar Animation Studios. The wiki format allows anyone to create or edit an article about a Pixar film.

Social networking sites enable users to build communities of friends and professional colleagues. Members typically create a "profile," a Web page for posting photos, videos, MP3 files, and text, and then share these profiles with others on the service identified as their "friends" or contacts. Social networking sites are highly interactive, offer real-time user control, rely on user-generated content, and are broadly based on social participation and sharing of content and opinions. Leading social networking sites include Facebook, Twitter (with 1 billion and 140 million active users respectively in 2012), and LinkedIn (for professional contacts).

For many, social networking sites are the defining Web 2.0 application, and one that has radically changed how people spend their time online; how people communicate and with whom; how business people stay in touch with customers, suppliers, and employees; how providers of goods and services learn about their customers; and how advertisers reach potential customers. The large social networking sites are also morphing into application development platforms where members can create and sell software applications to other members of the community. Facebook alone has over 1 million developers who created over 550,000 applications for gaming, video sharing, and communicating with friends and family. We talk more about business applications of social networking in Chapters 2 and 10, and you can find social networking discussions in many other chapters of this book. You can also find a more detailed discussion of Web 2.0 in our Learning Tracks.

Web 3.0: The Future Web

Every day, about 120 million Americans enter 600 million queries into search engines (about 17 billion per month). How many of these 600 million queries produce a meaningful result (a useful answer in the first three listings)?

Arguably, fewer than half. Google, Yahoo, Microsoft, and Amazon are all trying to increase the odds of people finding meaningful answers to search engine queries. But with over 400 billion Web pages indexed, the means available for finding the information you really want are quite primitive, based on the words used on the pages, and the relative popularity of the page among people who use those same search terms. In other words, it's hit or miss.

To a large extent, the future of the Web involves developing techniques to make searching the 400 billion public Web pages more productive and meaningful for ordinary people. Web 1.0 solved the problem of obtaining access to information. Web 2.0 solved the problem of sharing that information with others and building new Web experiences. **Web 3.0** is the promise of a future Web where all this digital information, all these contacts, can be woven together into a single meaningful experience.

Sometimes this is referred to as the **Semantic Web**. "Semantic" refers to meaning. Most of the Web's content today is designed for humans to read and for computers to display, not for computer programs to analyze and manipulate. Semantic Search, described above, is a subset of a larger effort to make the Web more intelligent, more human like (W3C, 2012). Search engines can discover when a particular term or keyword appears in a Web document, but they do not really understand its meaning or how it relates to other information on the Web. You can check this out on Google by entering two searches. First, enter "Paris Hilton". Next, enter "Hilton in Paris". Because Google does not understand ordinary English, it has no idea that you are interested in the Hilton Hotel in Paris in the second search. Because it cannot understand the meaning of pages it has indexed, Google's search engine returns the most popular pages for those queries where "Hilton" and "Paris" appear on the pages.

First described in a 2001 *Scientific American* article, the Semantic Web is a collaborative effort led by the World Wide Web Consortium to add a layer of meaning atop the existing Web to reduce the amount of human involvement in searching for and processing Web information (Berners-Lee et al., 2001). For instance, in 2011 the New York Times lanched a semantic application called Longitude which provides a graphical interface to access the Times content. For instance, you can ask for stories about Germany in the last 24 hours, or a city in the United States, to retrieve all recent stories in the Times. (Donaldson, 2012).

Views on the future of the Web vary, but they generally focus on ways to make the Web more "intelligent," with machine-facilitated understanding of information promoting a more intuitive and effective user experience. For instance, let's say you want to set up a party with your tennis buddies at a local restaurant Friday night after work. One problem is that you are already scheduled to go to a movie with another friend. In a Semantic Web 3.0 environment, you would be able to coordinate this change in plans with the schedules of your tennis buddies and the schedule of your movie friend, and make a reservation at the restaurant all with a single set of commands issued as text or voice to your handheld smartphone. Right now, this capability is beyond our grasp.

Work proceeds slowly on making the Web a more intelligent experience, in large part because it is difficult to make machines, including software programs, that are truly intelligent like humans. But there are other views of the future Web. Some see a 3-D Web where you can walk through pages in a 3-D environment. Others point to the idea of a pervasive Web that controls everything from the lights in your living room to your car's rear view mirror, not to mention managing your calendar and appointments. This is referred to as the "Web of things."

Other complementary trends leading toward a future Web 3.0 include more widespread use of cloud computing and software as a service (SaaS) business models, ubiquitous connectivity among mobile platforms and Internet access devices, and the transformation of the Web from a network of separate siloed applications and content into a more seamless and interoperable whole. These more modest visions of the future Web 3.0 are more likely to be realized in the near term.

7.4 The Wireless Revolution

Welcome to the wireless revolution! Cell phones, smartphones, tablets, and wireless-enabled personal computers have morphed into portable media and computing platforms that let you perform many of the computing tasks you used to do at your desk, and a whole lot more. We introduced smartphones in our discussions of the mobile digital platform in Chapters 1 and 5. **Smartphones** such as the iPhone, Android phones, and BlackBerry combine the functionality of a cell phone with that of a mobile laptop computer with Wi-Fi capability. This makes it possible to combine music, video, Internet access, and telephone service in one device. Smartphones are the fastest growing wireless devices with respect to Internet access. A large part of the Internet is becoming a mobile, access-anywhere, broadband service for the delivery of video, music, and Web search.

CELLULAR SYSTEMS

In 2012, an estimated 1.5 billion cell phones will be sold worldwide. In the United States, there are 358 million cell phone subscriptions, and 115 million people have smartphones. About 120 million people access the Web using their phone (eMarketer, 2012). In a few years, smartphones will be the predominant source of searches, not the desktop PC. Digital cellular service uses several competing standards. In Europe and much of the rest of the world outside the United Sates, the standard is Global System for Mobile Communications (GSM). GSM's strength is its international roaming capability. There are GSM cell phone systems in the United States, including T-Mobile and AT&T.

A competing standard in the United States is Code Division Multiple Access (CDMA), which is the system used by Verizon and Sprint. CDMA was developed by the military during World War II. It transmits over several frequencies, occupies the entire spectrum, and randomly assigns users to a range of frequencies over time, making it more efficient than GSM.

Earlier generations of cellular systems were designed primarily for voice and limited data transmission in the form of short text messages. Today wireless carriers offer 3G and 4G networks. **3G networks**, with transmission speeds ranging from 144 Kbps for mobile users in, say, a car, to more than 2 Mbps for stationary users, offer fair transmission speeds for e-mail, browsing the Web, and online shopping, but are too slow for videos. **4G networks,** also called Long Term Evolution (LTE) networks, have much higher speeds: 100 megabits/second download, and 50 megabits upload speed. Equivalent to a home Wi-Fi connection, LTE provides more than enough capacity for watching high definition video on your smartphone. A less well developed high speed network standard is WiMax which uses Wi-Fi standards but with an extended range of nearly 30 miles, enough to cover a metropolitan area, and potentially entire small countries.

WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

If you have a laptop computer, you might be able to use it to access the Internet as you move from room to room in your home or dorm, or table to table in your university library. An array of technologies provide high-speed wireless access to the Internet for PCs and other wireless handheld devices as well as for cell phones. These new high-speed services have extended Internet access to numerous locations that could not be covered by traditional wired Internet services.

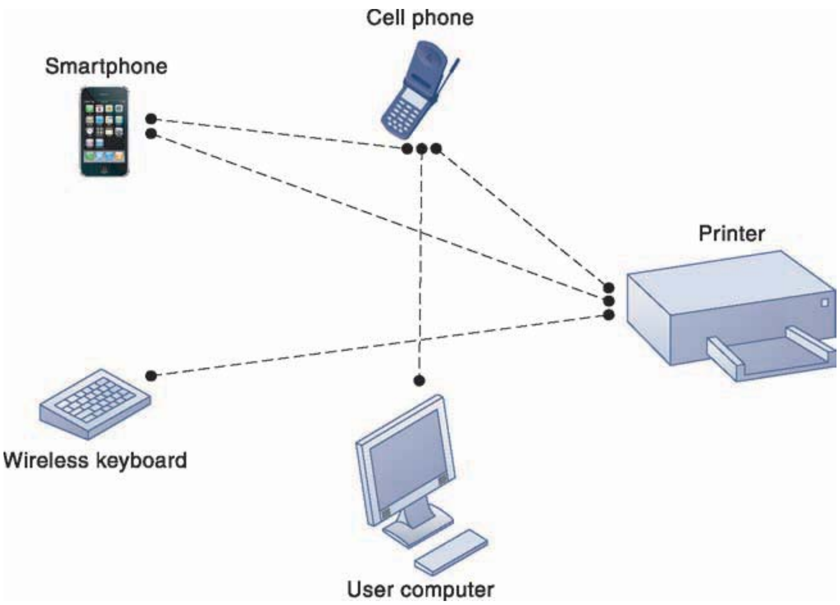
Bluetooth

Bluetooth is the popular name for the 802.15 wireless networking standard, which is useful for creating small **personal area networks (PANs)**. It links up to eight devices within a 10-meter area using low-power, radio-based communication and can transmit up to 722 Kbps in the 2.4-GHz band.

Wireless phones, pagers, computers, printers, and computing devices using Bluetooth communicate with each other and even operate each other without direct user intervention (see Figure 7.13). For example, a person could direct a notebook computer to send a document file wirelessly to a printer. Bluetooth connects wireless keyboards and mice to PCs or cell phones to earpieces without wires. Bluetooth has low-power requirements, making it appropriate for battery-powered handheld computers or cell phones.

Although Bluetooth lends itself to personal networking, it has uses in large corporations. For example, FedEx drivers use Bluetooth to transmit the delivery data captured by their handheld PowerPad computers to cellular transmitters, which forward the data to corporate computers. Drivers no longer need to spend time docking their handheld units

FIGURE 7.13 A BLUETOOTH NETWORK (PAN)



Bluetooth enables a variety of devices, including cell phones, smartphones, wireless keyboards and mice, PCs, and printers, to interact wirelessly with each other within a small 30-foot (10-meter) area. In addition to the links shown, Bluetooth can be used to network similar devices to send data from one PC to another, for example.

physically in the transmitters, and Bluetooth has saved FedEx $20 million per year.

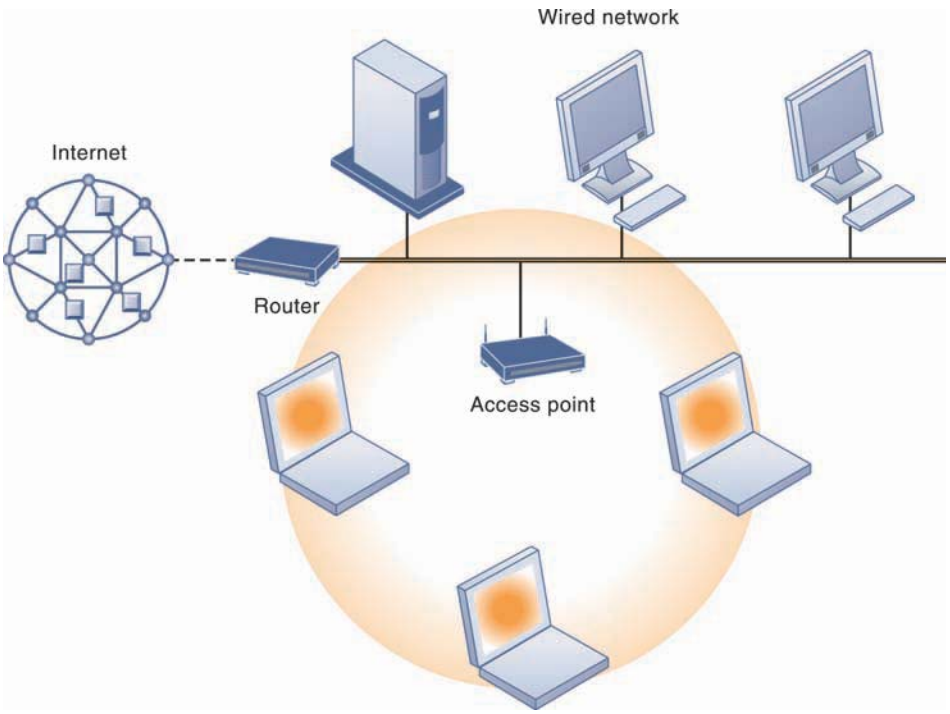
Wi-Fi and Wireless Internet Access

The 802.11 set of standards for wireless LANs and wireless Internet access is also known as **Wi-Fi**. The first of these standards to be widely adopted was 802.11b, which can transmit up to 11 Mbps in the unlicensed 2.4-GHz band and has an effective distance of 30 to 50 meters. The 802.11g standard can transmit up to 54 Mbps in the 2.4-GHz range. 802.11n is capable of transmitting over 100 Mbps. Today's PCs and netbooks have built-in support for Wi-Fi, as do the iPhone, iPad, and other smartphones.

In most Wi-Fi communication, wireless devices communicate with a wired LAN using access points. An access point is a box consisting of a radio receiver/transmitter and antennas that links to a wired network, router, or hub. Mobile access points such as Verizon's Mobile Hotspots use the existing cellular network to create Wi-Fi connections.

Figure 7.14 illustrates an 802.11 wireless LAN that connects a small number of mobile devices to a larger wired LAN and to the Internet. Most wireless devices are client machines. The servers that the mobile client stations need to use are on the wired LAN. The access point controls the wireless stations and acts as a bridge between the main wired LAN and the wireless LAN. (A bridge connects two LANs based on different technologies.) The access point also controls the wireless stations.

FIGURE 7.14 AN 802.11 WIRELESS LAN



Mobile laptop computers equipped with network interface cards link to the wired LAN by communicating with the access point. The access point uses radio waves to transmit network signals from the wired network to the client adapters, which convert them into data that the mobile device can understand. The client adapter then transmits the data from the mobile device back to the access point, which forwards the data to the wired network.

The most popular use for Wi-Fi today is for high-speed wireless Internet service. In this instance, the access point plugs into an Internet connection, which could come from a cable service or DSL telephone service. Computers within range of the access point use it to link wirelessly to the Internet.

Hotspots typically consist of one or more access points providing wireless Internet access in a public place. Some hotspots are free or do not require any additional software to use; others may require activation and the establishment of a user account by providing a credit card number over the Web.

Businesses of all sizes are using Wi-Fi networks to provide low-cost wireless LANs and Internet access. Wi-Fi hotspots can be found in hotels, airport lounges, libraries, cafes, and college campuses to provide mobile access to the Internet. Dartmouth College is one of many campuses where students now use Wi-Fi for research, course work, and entertainment.

Wi-Fi technology poses several challenges, however. One is Wi-Fi's security features, which make these wireless networks vulnerable to intruders. We provide more detail about Wi-Fi security issues in Chapter 8.

Another drawback of Wi-Fi networks is susceptibility to interference from nearby systems operating in the same spectrum, such as wireless phones, microwave ovens, or other wireless LANs. However, wireless networks based on the 802.11n standard are able to solve this problem by using multiple wireless antennas in tandem to transmit and receive data and technology called *MIMO* (multiple input multiple output) to coordinate multiple simultaneous radio signals.

WiMax

A surprisingly large number of areas in the United States and throughout the world do not have access to Wi-Fi or fixed broadband connectivity. The range of Wi-Fi systems is no more than 300 feet from the base station, making it difficult for rural groups that don't have cable or DSL service to find wireless access to the Internet.

The IEEE developed a new family of standards known as WiMax to deal with these problems. **WiMax**, which stands for Worldwide Interoperability for Microwave Access, is the popular term for IEEE Standard 802.16. It has a wireless access range of up to 31 miles and transmission speed of up to 75 Mbps.

WiMax antennas are powerful enough to beam high-speed Internet connections to rooftop antennas of homes and businesses that are miles away. Cellular handsets and laptops with WiMax capabilities are appearing in the marketplace. Mobile WiMax is one of the 4G network technologies we discussed earlier in this chapter.

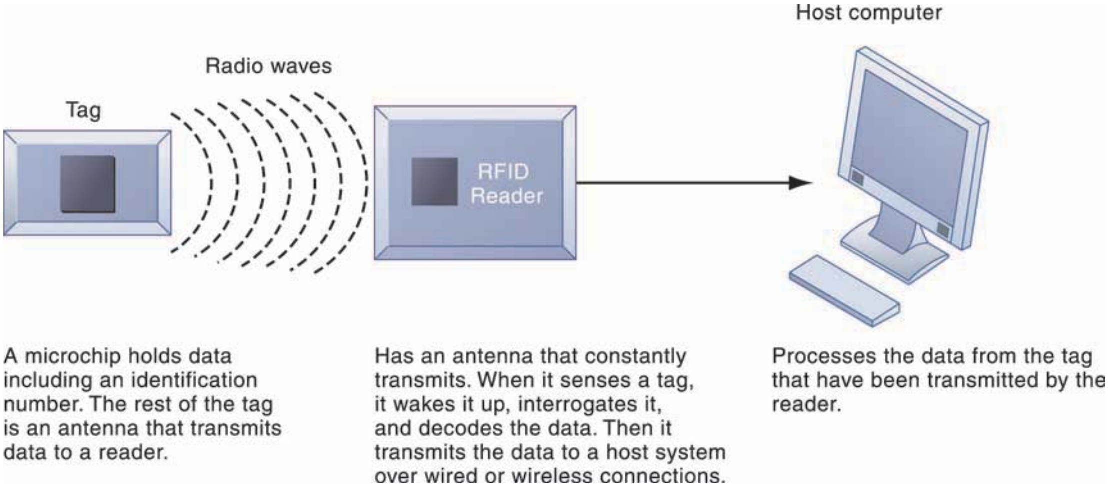
RFID AND WIRELESS SENSOR NETWORKS

Mobile technologies are creating new efficiencies and ways of working throughout the enterprise. In addition to the wireless systems we have just described, radio frequency identification systems and wireless sensor networks are having a major impact.

Radio Frequency Identification (RFID)

Radio frequency identification (RFID) systems provide a powerful technology for tracking the movement of goods throughout the supply chain. RFID systems use tiny tags with embedded microchips containing data about an item and its location to transmit radio signals over a short distance to RFID readers. The RFID readers then pass the data over a network to a computer for

FIGURE 7.15 HOW RFID WORKS



RFID uses low-powered radio transmitters to read data stored in a tag at distances ranging from 1 inch to 100 feet. The reader captures the data from the tag and sends them over a network to a host computer for processing.

processing. Unlike bar codes, RFID tags do not need line-of-sight contact to be read.

The RFID tag is electronically programmed with information that can uniquely identify an item plus other information about the item, such as its location, where and when it was made, or its status during production. Embedded in the tag is a microchip for storing the data. The rest of the tag is an antenna that transmits data to the reader.

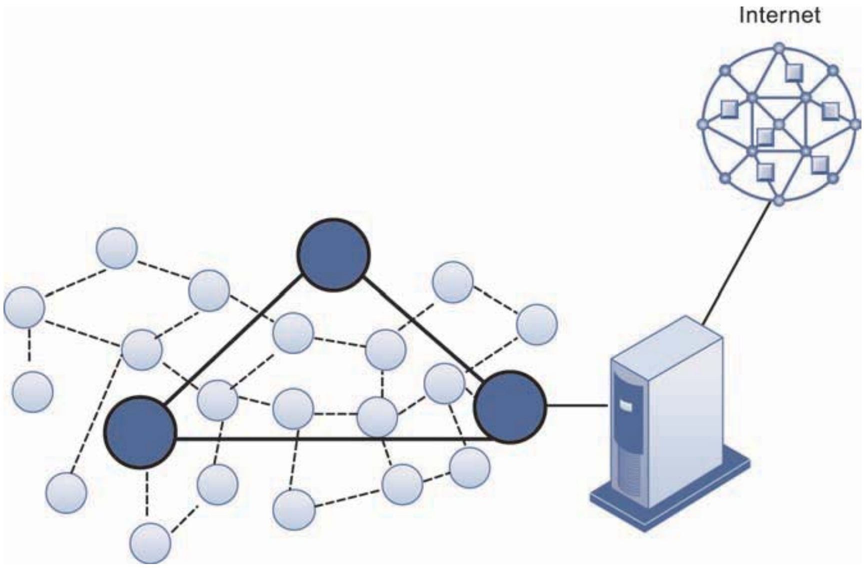
The reader unit consists of an antenna and radio transmitter with a decoding capability attached to a stationary or handheld device. The reader emits radio waves in ranges anywhere from 1 inch to 100 feet, depending on its power output, the radio frequency employed, and surrounding environmental conditions. When an RFID tag comes within the range of the reader, the tag is activated and starts sending data. The reader captures these data, decodes them, and sends them back over a wired or wireless network to a host computer for further processing (see Figure 7.15). Both RFID tags and antennas come in a variety of shapes and sizes.

Active RFID tags are powered by an internal battery and typically enable data to be rewritten and modified. Active tags can transmit for hundreds of feet but may cost several dollars per tag. Automated toll-collection systems such as New York's E-ZPass use active RFID tags.

Passive RFID tags do not have their own power source and obtain their operating power from the radio frequency energy transmitted by the RFID reader. They are smaller, lighter, and less expensive than active tags, but only have a range of several feet.

In inventory control and supply chain management, RFID systems capture and manage more detailed information about items in warehouses or in production than bar coding systems. If a large number of items are shipped together, RFID systems track each pallet, lot, or even unit item in the shipment. This technology may help companies such as Walmart improve receiving and storage operations by improving their ability to "see" exactly what stock is stored in warehouses or on retail store shelves. Continental Tires, described

FIGURE 7.16 A WIRELESS SENSOR NETWORK



The small circles represent lower-level nodes and the larger circles represent high-end nodes. Lower-level nodes forward data to each other or to higher-level nodes, which transmit data more rapidly and speed up network performance.

in the chapter-opening case, used RFID technology to precisely track the location of tire components as they moved through the production process.

Walmart has installed RFID readers at store receiving docks to record the arrival of pallets and cases of goods shipped with RFID tags. The RFID reader reads the tags a second time just as the cases are brought onto the sales floor from backroom storage areas. Software combines sales data from Walmart's point-of-sale systems and the RFID data regarding the number of cases brought out to the sales floor. The program determines which items will soon be depleted and automatically generates a list of items to pick in the warehouse to replenish store shelves before they run out. This information helps Walmart reduce out-of-stock items, increase sales, and further shrink its costs.

The cost of RFID tags used to be too high for widespread use, but now it starts at around 7 cents per passive tag in the United States. As the price decreases, RFID is starting to become cost-effective for many applications.

In addition to installing RFID readers and tagging systems, companies may need to upgrade their hardware and software to process the massive amounts of data produced by RFID systems—transactions that could add up to tens or hundreds of terabytes.

Software is used to filter, aggregate, and prevent RFID data from overloading business networks and system applications. Applications often need to be redesigned to accept large volumes of frequently generated RFID data and to share those data with other applications. Major enterprise software vendors, including SAP and Oracle PeopleSoft, now offer RFID-ready versions of their supply chain management applications.

Wireless Sensor Networks

If your company wanted state-of-the art technology to monitor building security or detect hazardous substances in the air, it might deploy a wireless sensor network. **Wireless sensor networks (WSNs)** are networks of interconnected wireless devices that are embedded into the physical environment to provide measurements of many points over large spaces. These devices have built-in processing, storage, and radio frequency sensors and antennas. They are linked into an interconnected network that routes the data they capture to a computer for analysis.

These networks range from hundreds to thousands of nodes. Because wireless sensor devices are placed in the field for years at a time without any maintenance or human intervention, they must have very low power requirements and batteries capable of lasting for years.

Figure 7.16 illustrates one type of wireless sensor network, with data from individual nodes flowing across the network to a server with greater processing power. The server acts as a gateway to a network based on Internet technology.

Wireless sensor networks are valuable in areas such as monitoring environmental changes, monitoring traffic or military activity, protecting property, efficiently operating and managing machinery and vehicles, establishing security perimeters, monitoring supply chain management, or detecting chemical, biological, or radiological material.

Learning Track Modules

The following Learning Tracks provide content relevant to topics covered in this chapter:

1. LAN Topologies
2. Broadband Network Services and Technologies
3. Cellular System Generations
4. Wireless Applications for Customer Relationship Management, Supply Chain Management, and Healthcare
5. Web 2.0

Review Summary

1. ***What are the principal components of telecommunications networks and key networking technologies?***

   A simple network consists of two or more connected computers. Basic network components include computers, network interfaces, a connection medium, network operating system software, and either a hub or a switch. The networking infrastructure for a large company includes the traditional telephone system, mobile cellular communication, wireless local area networks, videoconferencing systems, a corporate Web site, intranets, extranets, and an array of local and wide area networks, including the Internet.

   Contemporary networks have been shaped by the rise of client/server computing, the use of packet switching, and the adoption of Transmission Control Protocol/Internet Protocol (TCP/IP) as a universal communications standard for linking disparate networks and computers, including the Internet. Protocols provide a common set of rules that enable communication among diverse components in a telecommunications network.

2. ***What are the different types of networks?***

   The principal physical transmission media are twisted copper telephone wire, coaxial copper cable, fiber-optic cable, and wireless transmission.

   Local area networks (LANs) connect PCs and other digital devices together within a 500-meter radius and are used today for many corporate computing tasks. Wide area networks (WANs) span broad geographical distances, ranging from several miles to continents, and are private networks that are independently managed. Metropolitan area networks (MANs) span a single urban area.

   Digital subscriber line (DSL) technologies, cable Internet connections, and T1 lines are often used for high-capacity Internet connections.

3. ***How do the Internet and Internet technology work, and how do they support communication and e-business?***

   The Internet is a worldwide network of networks that uses the client/server model of computing and the TCP/IP network reference model. Every computer on the Internet is assigned a unique numeric IP address. The Domain Name System (DNS) converts IP addresses to more user-friendly domain names. Worldwide Internet policies are established by organizations and government bodies, such as the Internet Architecture Board (IAB) and the World Wide Web Consortium (W3C).

   Major Internet services include e-mail, newsgroups, chatting, instant messaging, Telnet, FTP, and the Web. Web pages are based on Hypertext Markup Language (HTML) and can display text, graphics, video, and audio. Web site directories, search engines, and RSS technology help users locate the information they need on the Web. RSS, blogs, social networking, and wikis are features of Web 2.0.

   Firms are also starting to realize economies by using VoIP technology for voice transmission and by using virtual private networks (VPNs) as low-cost alternatives to private WANs.

4. ***What are the principal technologies and standards for wireless networking, communication, and Internet access?***

   Cellular networks are evolving toward high-speed, high-bandwidth, digital packet-switched transmission. Broadband 3G networks are capable of transmitting data at speeds ranging from 144 Kbps to more than 2 Mbps. 4G networks capable of transmission speeds that could reach 1 Gbps are starting to be rolled out.

   Major cellular standards include Code Division Multiple Access (CDMA), which is used primarily in the United States, and Global System for Mobile Communications (GSM), which is the standard in Europe and much of the rest of the world.

   Standards for wireless computer networks include Bluetooth (802.15) for small personal area networks (PANs), Wi-Fi (802.11) for local area networks (LANs), and WiMax (802.16) for metropolitan area networks (MANs).

5. ***Why are radio frequency identification (RFID) and wireless sensor networks valuable for business?***

   Radio frequency identification (RFID) systems provide a powerful technology for tracking the movement of goods by using tiny tags with embedded data about an item and its location. RFID readers read the radio signals transmitted by these tags and pass the data over a network to a computer for processing. Wireless sensor networks (WSNs) are networks of interconnected wireless sensing and transmitting devices that are embedded into the physical environment to provide measurements of many points over large spaces.

Key Terms

3G Networks, 307
4G networks, 307
Bandwidth, 288
Blog, 304
Blogosphere, 304
Bluetooth, 308
Broadband, 280
Cable Internet connections, 288
Chat, 294
Digital subscriber line (DSL), 288
Domain name, 289
Domain Name System (DNS), 289
E-mail, 294
File Transfer Protocol (FTP), 294
Hertz, 287
Hotspots, 310
Hubs, 281
Hypertext Transfer Protocol (HTTP), 299
Instant messaging, 294
Internet Protocol (IP) address, 288
Internet service provider (ISP), 288
Internet2, 291
IPv6, 291
Local area network (LAN), 286
Metropolitan area network (MAN), 287
Microblogging, 304
Modem, 285
Network operating system (NOS), 281
Packet switching, 283
Peer-to-peer, 286
Personal area networks (PANs), 308
Protocol, 284
Radio frequency identification (RFID), 310
Router, 281
RSS, 304
Search engines, 300
Search engine marketing, 302
Search engine optimization (SEO), 302
Semantic Web, 306
Shopping bots, 304
Smartphones, 307
Social networking, 305
Social search, 303
Software-defined networking, 281
Switch, 281
T1 lines, 288
Telnet, 294
Transmission Control Protocol/Internet Protocol (TCP/IP), 284
Unified communications, 298
Uniform resource locator (URL), 299
Virtual private network (VPN), 298
Voice over IP (VoIP), 295
Web 2.0, 304
Web 3.0, 306
Web site, 299
Wide area networks (WANs), 287
Wi-Fi, 309
Wiki, 305
WiMax, 310
Wireless sensor networks (WSNs), 313

Review Questions

1. What are the principal components of telecommunications networks and key networking technologies?
- Describe the features of a simple network and the network infrastructure for a large company.
- Name and describe the principal technologies and trends that have shaped contemporary telecommunications systems.

2. What are the main telecommunications transmission media and types of networks?
- Name the different types of physical transmission media and compare them in terms of speed and cost.
- Define a LAN, and describe its components and the functions of each component.
- Name and describe the principal network topologies.

3. How do the Internet and Internet technology work, and how do they support communication and e-business?
- Define the Internet, describe how it works, and explain how it provides business value.
- Explain how the Domain Name System (DNS) and IP addressing system work.
- List and describe the principal Internet services.

- Define and describe VoIP and virtual private networks, and explain how they provide value to businesses.
- List and describe alternative ways of locating information on the Web.
- Compare Web 2.0 and Web 3.0.

4. What are the principal technologies and standards for wireless networking, communications, and Internet access?

- Define Bluetooth, Wi-Fi, WiMax, and 3G and 4G networks.
- Describe the capabilities of each and for which types of applications each is best suited.

5. Why are RFID and wireless sensor networks (WSNs) valuable for business?

- Define RFID, explain how it works, and describe how it provides value to businesses.
- Define WSNs, explain how they work, and describe the kinds of applications that use them.

Discussion Questions

1. It has been said that within the next few years, smartphones will become the single most important digital device we own. Discuss the implications of this statement.

2. Should all major retailing and manufacturing companies switch to RFID? Why or why not?

3. Compare Wi-Fi and high-speed cellular systems for accessing the Internet. What are the advantages and disadvantages of each?

Hands-On MIS Projects

The projects in this section give you hands-on experience evaluating and selecting communications technology, using spreadsheet software to improve selection of telecommunications services, and using Web search engines for business research.

Management Decision Problems

1. Your company supplies ceramic floor tiles to Home Depot, Lowe's, and other home improvement stores. You have been asked to start using radio frequency identification tags on each case of tiles you ship to help your customers improve the management of your products and those of other suppliers in their warehouses. Use the Web to identify the cost of hardware, software, and networking components for an RFID system for your company. What factors should be considered? What are the key decisions that have to be made in determining whether your firm should adopt this technology?

2. BestMed Medical Supplies Corporation sells medical and surgical products and equipment from over 700 different manufacturers to hospitals, health clinics, and medical offices. The company employs 500 people at seven different locations in western and midwestern states, including account managers, customer service and support representatives, and warehouse staff. Employees communicate via traditional telephone voice services, e-mail, instant messaging, and cell phones. Management is inquiring about whether the company should adopt a system for unified communications. What factors should be considered? What are the key decisions that have to be made in determining whether to adopt this technology? Use the Web, if necessary, to find out more about unified communications and its costs.

Improving Decision Making: Using Spreadsheet Software to Evaluate Wireless Services

Software skills: Spreadsheet formulas, formatting
Business skills: Analyzing telecommunications services and costs

In this project, you'll use the Web to research alternative wireless services and use spreadsheet software to calculate wireless service costs for a sales force.

You would like to equip your sales force of 35, based in Cincinnati, Ohio, with mobile phones that have capabilities for voice transmission, text messaging, and taking and sending photos. Use the Web to select a wireless service provider that provides nationwide service as well as good service in your home area. Examine the features of the mobile handsets offered by each of these vendors. Assume that each of the 35 salespeople will need to spend three hours per weekday between 8 a.m. and 6 p.m. on mobile voice communication, send 30 text messages per weekday, and send five photos per week. Use your spreadsheet software to determine the wireless service and handset that will offer the best pricing per user over a two-year period. For the purposes of this exercise, you do not need to consider corporate discounts.

Achieving Operational Excellence: Using Web Search Engines for Business Research

Software skills: Web search tools
Business skills: Researching new technologies

This project will help develop your Internet skills in using Web search engines for business research.

Use Google and Bing to obtain information about ethanol as an alternative fuel for motor vehicles. If you wish, try some other search engines as well. Compare the volume and quality of information you find with each search tool. Which tool is the easiest to use? Which produced the best results for your research? Why?

Video Cases

Video Cases and Instructional Videos illustrating some of the concepts in this chapter are available. Contact your instructor to access these videos.

Collaboration and Teamwork Project

In MyMISLab, you will find a Collaboration and Teamwork Project dealing with the concepts in this chapter. You will be able to use Google Sites, Google Docs, and other open source collaboration tools to complete the assignment.

Apple, Google, and Microsoft Battle for your Internet Experience
CASE STUDY

The three Internet titans—Google, Microsoft, and Apple—are in an epic struggle to dominate your Internet experience. They are competing on several fronts: digital content, from music to videos and books for sale in their online stores; physical devices, from Apple's iPhone to Google's Android phones, to Microsoft's Windows 8 phones. And let's not forget they all offer tablets as well. The prize is a projected $400 billion e-commerce marketplace by 2015 where the major access device will be a smartphone or tablet computer. Each firm generates extraordinary amounts of cash based on different business models and is using that cash in hopes of being the top dog on the Internet.

In this triangular fight, at one point or another, each firm has allied with one of their two major foes to team up on the third. Two of the firms—Google and Apple—are determined to prevent Microsoft from expanding its dominance beyond the PC desktop and onto the new mobile platform. So Google and Apple are friends. But when it comes to mobile phones and apps, Google and Apple are enemies: both want to dominate the mobile market. Apple and Microsoft are determined to prevent Google from extending beyond its dominance in search and advertising. So Apple and Microsoft are friends. But when it comes to the mobile marketplace for devices and apps, Apple and Microsoft are enemies. Google and Microsoft are just plain enemies in a variety of battles. Google is trying to weaken Microsoft's PC software dominance, and Microsoft is trying to break into the search advertising market with Bing.

The Internet, along with hardware devices and software applications, is going through a major expansion. Mobile devices with advanced functionality and ubiquitous Internet access are rapidly gaining on traditional desktop computing as the most popular form of computing, changing the basis for competition throughout the industry. Some analysts predict that by 2015, mobile devices will account for the majority of Internet traffic. Today, mobile devices account for approximately 30 percent of the traffic on the Web. These mobile Internet devices are made possible by a growing cloud of computing capacity available to anyone with a smartphone and Internet connectivity. Who needs a desktop PC anymore when you can listen to music and watch videos anytime, anywhere on mobile devices? It's no surprise, then, that today's tech titans are so aggressively battling for control of this brave new mobile world.

Apple, Google, and Microsoft already compete in an assortment of fields. Google has a huge edge in advertising, thanks to its dominance in Internet search. Microsoft's offering, Bing, has about 5 percent of the search market, and about 80 percent belongs to Google. Apple is the leader in mobile software applications, thanks to the popularity of the App Store for its iPhones. Google and Microsoft have less popular app offerings on the Web. Microsoft is still the leader in PC operating systems, but has struggled with many of its other efforts, including smartphone hardware and software, mobile computing, cloud-based software apps, and its Internet portal. Even though Microsoft's Xbox consoles and games are popular, they contribute less than 5 percent of Microsoft's revenue (the rest of its revenue comes from Windows, Office, and network software). While Windows XP, Windows 7, and Windows Vista are still the operating systems for approximately 90 percent of the world's PCs, Google's Android OS and Apple's iOS are the dominant players in the mobile computing market, and all three of these companies now realize that this market will only increase in size and scope going forward.

Apple has several advantages that will serve it well in the battle for mobile supremacy. It's no coincidence that since the Internet exploded in size and popularity, so too did Apple's revenue, which totaled well over $108 billion in 2011, up from $65 billion the previous year despite an ongoing economic downturn. The iMac, iPod, and iPhone have all contributed to the company's enormous success in the Internet era, and the iPad has followed the trend of profitability set by these previous products. Apple has a loyal user base that has steadily grown and is very likely to buy future product and offerings.

Part of the reason for the popularity of the iPhone, and for the optimism surrounding Internet-equipped smartphones in general, has been the success of the App Store. A vibrant selection of applications distinguishes Apple's offerings from its competitors', and gives Apple a measurable head start in this marketplace. Apple already offers approximately 700,000 applications for their devices, and Apple takes a 30 percent cut of all app sales. Applications greatly enrich the experience of using a mobile device, and without them, the predictions for the future of mobile Internet would not be nearly as bright. Whoever creates the most appealing set of devices and applications will derive a significant competitive advantage over rival companies. Right now, that company is Apple.

But the development of smartphones and mobile Internet is still in its infancy. Google has acted swiftly to enter the battle for mobile supremacy while they can still "win." More and more people are likely to switch to mobile computing as their primary method of using the Internet, so it's no surprise that Google is aggressively following the eyeballs. Google is as strong as the size of its advertising network. With the impending shift towards mobile computing looming, it's not certain that they'll be able to maintain their dominant position in search. That's why the dominant online search company began developing its Android operating system, which is used on almost 60 percent of smartphones worldwide. Google offers Android for free to manufacturers of handsets that run the operating system. Via Android, Google hopes to control its own destiny in an increasingly mobile world.

Because Google provides Android at no cost to smartphone manufacturers, competitors have sought to weigh it down with patent claims and other lawsuits. That's part of the reason why Google made its biggest acquisition yet in August 2011, buying Motorola Mobility Holdings for $12.5 billion. The deal gives Google 17,000 patents and another 7,000 more in the pipeline that will help the company defend Android from these patent lawsuits. But buying Motorola's phone business does more than just give Google patents. It also gives Google the ability to make its own cell phones and tablet devices, which would be its most aggressive move against Apple yet.

Analysts were skeptical regarding whether or not Google would even try to enter this marketplace, let alone whether it could succeed in doing so. But in June 2012, Google released its Nexus 7 tablet, developed by Asus, to rave reviews. The sleek 7-inch tablet is priced between $199 and $249, and effectively competes with the iPad and Kindle Fire. Google is entering completely new territory. It has never sold devices before, the profit margins will be much tighter than they are for their search business, and it places Motorola in an awkward position among the smartphone manufacturers that Google works with. And Google's previous attempts to sell hardware have been unsuccessful: their Nexus One smartphone, released in 2010, was widely considered to be a failure despite impressive technical capabilities.

Google has been particularly aggressive with moves such as the acquisition of Motorola's phone business because it is concerned about Apple's preference for "closed," proprietary standards on its phones. Apple retains the final say over whether or not its users can access various services on the Web, and that includes services provided by Google. Google doesn't want Apple to be able to block it from providing its services on iPhones, or any other smartphone. Apple is reliant on sales of its devices to remain profitable. It has had no problems with this so far, but Google only needs to spread its advertising networks onto these devices to make a profit. In fact, some analysts speculate that Google envisions a future where mobile phones cost a fraction of what they do today, or are even free, requiring only the advertising revenue generated by the devices to turn a profit. Apple would struggle to remain competitive in this environment. Apple has kept the garden closed for a simple reason: you need an Apple device to play there.

Apple's $1.05 billion victory in a patent lawsuit against Samsung on August 24, 2012, could be a blow to Google. Samsung smartphones and tablets were found to have violated a series of Apple patents protecting a number of designs and functions, including the pinch-to-zoom gesture in the user interface. The verdict discourages other handset companies from making devices that use Google's Android operating system, and Android may be forced to make design changes.

In 2012, Apple announced a mapping application to rival Google Maps. Approximately half of Google Maps traffic comes from Apple devices, and that traffic generates valuable location data that helps to improve the service, holding great value for marketers and advertisers. Apple has made several smaller acquisitions in the past two years that have prepared it to compete with Google in this field, and Apple now has its sights set on the valuable location data generated by Google Maps. Apple does not want Google gathering useful data about Apple users on their own devices.

Microsoft hasn't given up trying to establish a cloud and mobile presence. Its Office 2013 productivity suite operates in the cloud as well as on the desktop, giving users the option of saving documents to Microsoft's

SkyDrive cloud storage service. Microsoft launched its Surface tablet computers around the same time as the launch of the Windows 8 operating system.

The struggle between Apple, Google, and Microsoft wouldn't matter much if there wasn't so much potential money at stake. Billions of dollars hang in the balance, and the majority of that money will come from advertising. App sales are another important component, especially for Apple. Apple has the edge in selection and quality of apps, but while sales have been brisk, developers have complained that making money is too difficult. Roughly a quarter of the apps available in the App Store are free, which makes no money for developers or for Apple, but it does bring consumers to the Apple marketplace where they can be sold other apps or entertainment services.

The three-way struggle between Microsoft, Apple, and Google really has no precedent in the history of computing platforms. In early contests, it was typically a single firm that rode the crest of a new technology to become the dominant player. Examples include IBM's dominance of the mainframe market, Digital Equipment's dominance of minicomputers, Microsoft's dominance of operating systems and PC productivity applications, and Cisco's dominance of the Internet router market. In the current struggle, three firms are trying to dominate the customer experience on the Internet. Each firm brings certain strengths and weaknesses to the fray. It's too early to tell if a single firm will "win," or if all three can survive the contest for the consumer Internet experience.

Sources: Nick Wingfield, "Apple Case Muddies the Future of Innovations," *The New York Times*, August 27, 2012; Michael Vizard, "The Path of Least Mobile Computing Resistance", Channel Insider.com, June 6, 2012; Reuters, "Apple Versus Google War Heats Up," June 9, 2012; "Microsoft Counting on Office 2013 to Retain Enterprise App Dominance," *CIO Insight*, July 18, 2012; John Letzing and Amir Efrati, "Google's New Role as Gadget Maker," *The Wall Street Journal*, June 28, 2012; Nick Wingfield, "With Tablet, Microsoft Takes Aim at Hardware Missteps," *The New York Times*, June 24, 2012; Jessica Vascellaro, "Apple and Google Expand Their Battle to Mobile Maps," *The Wall Street Journal*, June 4, 2012; Amir Efrati and Spencer E. Ante, "Google's $12.5 Billion Gamble," *The Wall Street Journal*, August 16, 2011; Evelyn M. Rusli, "Google's Big Bet on the Mobile Future," *The New York Times*, August 15, 2011; Claire Cain Miller, "Google, a Giant in Mobile Search, Seeks New Ways to Make It Pay," *The New York Times*, April 24, 2011; Brad Stone and Miguel Helft, "Apple's Spat with Google Is Getting Personal," *The New York Times,* March 12, 2010; and Peter Burrows, "Apple vs. Google," *BusinessWeek*, January 14, 2010.

CASE STUDY QUESTIONS

1. Compare the business models and areas of strength of Apple, Google, and Microsoft.
2. Why is mobile computing so important to these three firms? Evaluate the mobile platform offerings of each firm.
3. What is the significance of mobile applications, app stores, and closed vs. open app standards to the success or failure of mobile computing?
4. Which company and business model do you think will prevail in this epic struggle? Explain your answer.
5. What difference would it make to a business or to an individual consumer if Apple, Google, or Microsoft dominated the Internet experience? Explain your answer.