PART ONE INTRODUCTION

# CHAPTER 1

# INTRODUCTION TO DATA COMMUNICATIONS



This chapter introduces the basic concepts of data communications. It describes why it is important to study data communications, how data communications fit within the discipline of Management Information Systems (MIS), and introduces you to the three fundamental questions that this book answers. Next, it discusses the basic types and components of a data communications network. Also, it examines the importance of a network model based on layers. Finally, it describes the three key trends in the future of networking.

## OBJECTIVES

- Be aware of the three fundamental questions this book answers
- Be aware of the applications of data communications networks
- Be aware of how data communications fit within the discipline of MIS
- Be familiar with the major components of and types of networks
- Understand the role of network layers
- Be familiar with the role of network standards
- Be aware of cyber security issues
- Be aware of three key trends in communications and networking

## OUTLINE



## 1.1 INTRODUCTION

What Internet connection should you use? Cable modem or DSL (formally called Digital Subscriber Line)? Cable modems are supposedly faster than DSL, providing data speeds of 50 Mbps to DSL's 1.5–25 Mbps (million bits per second). One cable company used a tortoise to represent DSL in advertisements. So which is faster? We'll give you a hint. Which won the race in the fable, the tortoise or the hare? By the time you finish this book, you'll understand which is faster and why, as well as why choosing the right company as your **Internet service provider (ISP)** is probably more important than choosing the right technology.

Over the past decade or so, it has become clear that the world has changed forever due to the third and fourth Industrial Revolutions. The first Industrial Revolution revolutionized the way people worked at the end of the 18th century by introducing machines, steam and water power. New companies and industries emerged, and old ones died off. The second Industrial Revolution in the late 19th century is known for starting mass production, electricity, and the telephone. The third Industrial Revolution, in the second half of the 20th century, is revolutionizing the way people work through electronics and information technology (IT) to automate production.

The fourth Industrial Revolution is currently underway. It builds on the technological advances of the third Industrial Revolution, but the way it merges the physical, digital, and biological worlds is unprecedented. It is deeply rooted in the Internet and digitization. Digitization enables us to build a world where interactions can happen in real time across different continents (think about email, instant messaging, and exchange of data between different devices). These interactions are possible because of technologies such as cloud, big data, big data analytics, and the Internet of Things. But the technology that enables all these technologies to communicate is the high-speed data communication network, that is, the Internet.

Today, the value of a high-speed data communications network is that it brings people together in a way never before possible. In the 1800s, it took several weeks for a message to reach North America by ship from England. By the 1900s, it could be transmitted within an hour. Today, it can be transmitted in seconds. Collapsing the *information lag* to Internet speeds means that people can communicate and access information anywhere in the world regardless of their physical location. In fact, today's problem is that we cannot handle the quantities of information we receive.

Data communications and networking is a truly global area of study, both because the technology enables global communication and because new technologies and applications often emerge from a variety of countries and spread rapidly around the world. The World Wide Web, for example, was born in a Swiss research lab, was nurtured through its first years primarily by European universities and exploded into mainstream popular culture because of a development at an American research lab.

One of the problems in studying a global phenomenon lies in explaining the different political and regulatory issues that have evolved and currently exist in different parts of the world. Rather than attempt to explain the different paths taken by different countries, we have chosen simplicity instead. Historically, the majority of readers of previous editions of this book have come from North America. Therefore, although we retain a global focus on technology and its business implications, we focus mostly on North America.

This book answers three fundamental questions.

First, how does the Internet work? When you access a website using your computer, laptop, iPad, or smartphone, what happens so that the page opens in your Web browser? This is the focus in Chapters 1–5. The short answer is that the software on your computer (or any device) creates a message composed in different software languages (HTTP, TCP/IP, and Ethernet are common) that requests the page you clicked. This message is then broken up into a series of smaller parts that we call packets. Each packet is transmitted to the nearest router, which is a special-purpose computer whose primary job is to find the best route for these packets to their final destination. The packets move from router to router over the Internet until they reach the Web server, which puts the packets back together into the same message that your computer created. The Web server reads your request and then sends the page back to you in the same way—by composing a message using HTTP, TCP/IP, and Ethernet and then sending it as a series of smaller packets back through the Internet that the software on your computer puts together into the page you requested. You might have heard a news story that the U.S. or Chinese government can read your email or see what websites you're visiting. A more shocking truth is that the person sitting next you at a coffee shop might be doing exactly the same thing—reading all the packets that come from or go to your laptop. How is this possible, you ask? After finishing Chapter 5, you will know exactly how this is possible.

Second, how do I design a network? This is the focus of Chapters 6–10. We often think about networks in four layers. The first layer is the Local Area Network, or the LAN (either wired or wireless), which enables users like you and me to access the network. The second is the backbone network that connects the different LANs within a building. The third is the core network that connects different buildings on a company's campus. The final layer is connections we have to the other campuses within the organization and to the Internet. Each of these layers has slightly different concerns, so the way we design networks for them and the technologies we use are slightly different. Although this describes the standard for building corporate networks, you will have a much better understanding of how your wireless router at home works. Perhaps more importantly, you'll learn why buying the newest and fastest wireless router for your house or apartment is probably not a good way to spend your money.

Finally, how do I manage my network to make sure it is secure, provides good performance, and doesn't cost too much? This is the focus of Chapters 11 and 12. Would it surprise you to learn that most companies spend between $1,500 and $3,500 per computer per year on network management and security? Yup, we spend way more on network management and security each year than we spend to buy the computer in the first place. And that's for well-run networks; poorly run networks cost a lot more. Many people think network security is a technical problem, and, to some extent, it is. However, the things people do and don't do cause more security risks than not having the latest technology. According to Symantec, one of the leading companies that sell antivirus software, about half of all security threats are not prevented by their software. These threats are called targeted attacks, such as phishing **attacks** (which are emails that look real but instead take you to fake websites) or ransomware (software apps that appear to be useful but actually lock your computer and demand a payment to unlock it). Therefore, network management is as much a people management issue as it is a technology management issue.

Most readers of this book will be taking classes towards their degree in management information systems (MIS) or a closely related field. How does this book relate to what MIS? Let us explain!

MIS begins with an IT strategy—a plan for buying and/or building IT to help the organization accomplish its goals. For most companies, this means increasing revenues and/or decreasing costs. Companies must deploy the right IT to support their business operations. IT has four core capabilities within organizational settings:

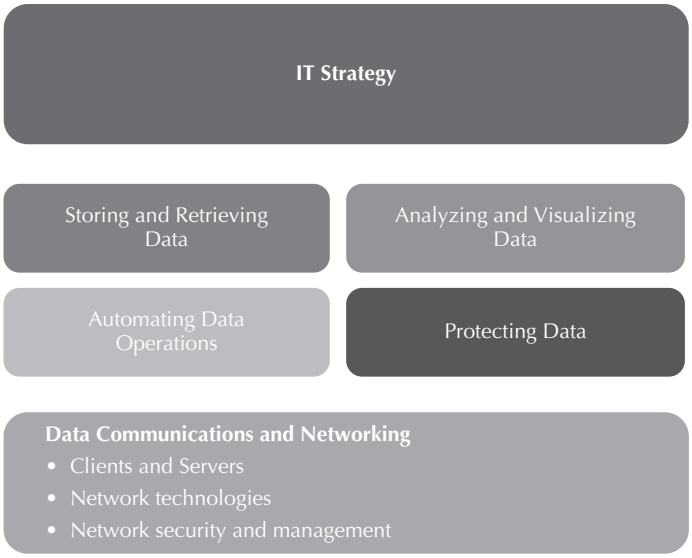
**1.** Storing and Retrieving Data—Just like humans live in houses, data created by businesses and societies must live somewhere. The "house" for data is a database. There are many different kinds of databases, just like many different kinds of houses. The most frequently used database in organizations is an SQL database.

**2.** Analyzing and Visualizing Data—Managers need to able to make decisions regarding their business, such as: What is our bestselling product? Which regions bring in the most revenue? Which regions are losing money? These decisions are made using the data stored in databases. Data is retrieved from a database and imported to a software like Excel, Tableau, or PowerBI so that these business questions can be answered using a variety of techniques (e.g., aggregation, conditional aggregation, and charting).

**3.** Automating Data Operations—Many business operations are repeated over and over again, such as calculating the total amount of a items bought at a local store or an e-commerce web site, applying any discounts, and determining appropriate taxes. To automate these kinds of every day transactions on data, we have a wide variety of IT we can buy or build using a variety of programming languages.

**4.** Protecting Data—The first three core capabilities are designed to make it easy to store and access data. However, this means that an intruder or malicious employee could also access the data. Therefore, organizations must spend resources to protect their data and ensuring the confidentiality, integrity, and availability of the data. We will discuss security capability in Chapter 11.

**FIGURE 1-1**
What is MIS?




In order for the IT strategy to implement the core capabilities, data communications and networking infrastructure must be available. You are using this infrastructure anytime you use the Internet on your laptop and even your cell phone. MIS core capabilities and the IT strategy rest on a solid infrastructure (see Figure 1-1). Therefore, understanding how data communications

**MANAGEMENT FOCUS**

## 1-1 Career Opportunities

*I*t's a great time to be in information technology (IT)! The technology-fueled new economy has dramatically increased the demand for skilled IT professionals. According to the U.S. Bureau of Labor Statistics and Career Profiles (http://www.careerprofiles.info), 2 out of 10 fastest growing occupations are computer network administrator and computer systems analyst, which is expected to grow by 22% over the next 10 years with an annual median salary of $72,500—not counting bonuses. There are two reasons for this growth. First, companies have to continuously upgrade their networks and thus need skilled employees to support their expanding IT infrastructure. Second, people are spending more time on their mobile devices, and because employers are allowing them to use these personal devices at work (i.e., BYOD, or bring your own device), the network infrastructure has to support the data that flow from these devices as well as to make sure that they don't pose a security risk.

With a few years of experience, there is the possibility to work as an information systems manager, for which the median annual pay is as high as $117,780. An information systems manager plans, coordinates, and directs IT-related activities in such a way that they can fully support the goals of any business. Thus, this job requires a good understanding not only of the business but also of the technology so that appropriate and reliable technology can be implemented at a reasonable cost to keep everything operating smoothly and to guard against cybercriminals.

Because of the expanding job market for IT and networking-related jobs, certifications become important. Most large vendors of network technologies, such as the Microsoft Corporation and Cisco Systems Inc., provide certification processes (usually a series of courses and formal exams) so that individuals can document their knowledge. Certified network professionals often earn $10,000 to $15,000 more than similarly skilled uncertified professionals—provided that they continue to learn and maintain their certification as new technologies emerge.

Sources: http://jobs.aol.com, "In Demand Careers That Pay $100,00 a Year or More"; www.careerpath.com, "Today's 20 Fastest-Growing Occupations"; www.cnn.com, "30 Jobs Needing Most Workers in Next Decade," http://www.careerprofiles.info/top-careers.html.

and networking works will enable you to understand what it takes for a modern organization to stay in business and for you to be able to work and connect with your family and friends.

By the time you finish this book, you'll understand how networks work, how to design networks, and how to manage networks. You won't be an expert, but you'll be ready to enter an organization and have an educated conversation about the role of data communications and networks or move on to more advanced courses and workshops.

## 1.2 DATA COMMUNICATIONS NETWORKS

*Data communications* is the movement of computer information from one point to another by means of electrical or optical transmission systems. Such systems are often called *data communications networks*. This is in contrast to the broader term *telecommunications*, which includes the transmission of voice and video (images and graphics) as well as data and usually implies longer distances. In general, data communications networks collect data from personal computers and other devices and transmit those data to a central server that is a more powerful personal computer, minicomputer, or mainframe, or they perform the reverse process, or some combination of the two. Data communications networks facilitate more efficient use of computers and improve the day-to-day control of a business by providing faster information flow. They also provide message transfer services to allow computer users to talk to one another via email, chat, and video streaming.

TECHNICAL FOCUS

### 1-1 Internet Domain Names

Internet address names are strictly controlled; otherwise, someone could add a computer to the Internet that had the same address as another computer. Each address name has two parts, the computer name and its domain. The general format of an Internet address is therefore computer.domain. Some computer names have several parts separated by periods, so some addresses have the format computer.computer.computer.domain. For example, the main university Web server at Indiana University (IU) is called www.indiana.edu, whereas the Web server for the Kelley School of Business at IU is www.kelley.indiana.edu.

Since the Internet began in the United States, the American address board was the first to assign domain names to indicate types of organizations. Some common U.S. domain names are as follows:

| | |
|---|---|
| EDU | for an educational institution, usually a university |
| COM | for a commercial business |
| GOV | for a government department or agency |
| MIL | for a military unit |
| ORG | for a nonprofit organization |

As networks in other countries were connected to the Internet, they were assigned their own domain names. Some international domain names are as follows:

| | |
|---|---|
| CA | for Canada |
| AU | for Australia |
| UK | for the United Kingdom |
| DE | for Germany |

New top-level domains that focus on specific types of businesses continue to be introduced, such as the following:

| | |
|---|---|
| AERO | for aerospace companies |
| MUSEUM | for museums |
| NAME | for individuals |
| PRO | for professionals, such as accountants and lawyers |
| BIZ | for businesses |

Many international domains structure their addresses in much the same way as the United States does. For example, Australia uses *EDU* to indicate academic institutions, so an address such as xyz.edu.au would indicate an Australian university.

For a full list of domain names, see www.iana.org/domains/root/db.

### 1.2.1 Components of a Network

There are three basic hardware components for a data communications network: a server (e.g., personal computer, mainframe), a client (e.g., personal computer, terminal), and a circuit (e.g., cable, modem) over which messages flow. Both the server and client also need special-purpose network software that enables them to communicate.

The **server** stores data or software that can be accessed by the clients. In client–server computing, several servers may work together over the network with a client computer to support the business application.

The **client** is the input–output hardware device at the user's end of a communication circuit. It typically provides users with access to the network and the data and software on the server.

The **circuit** is the pathway through which the messages travel. It is typically a copper wire, although fiber-optic cable and wireless transmission are becoming common. There are many devices in the circuit that perform special functions such as switches and routers.

Strictly speaking, a network does not need a server. Some networks are designed to connect a set of similar computers that share their data and software with each other. Such networks are called **peer-to-peer networks** because the computers function as equals, rather than relying on a central server to store the needed data and software.

Figure 1-2 shows a small network that has several personal computers (clients) connected through a **switch** and **cables** (circuit) and wirelessly through a **wireless access point** (AP). In this network, messages move through the switch to and from the computers. The **router** is a special device that connects two or more networks. The router enables computers on this network to communicate with computers on the same network or on other networks (e.g., the Internet).

The network in Figure 1-3 has three servers. Although one server can perform many functions, networks are often designed so that a separate computer is used to provide different services. The **file server** stores data and software that can be used by computers on the network. The **Web server** stores documents and graphics that can be accessed from any Web browser, such as Internet Explorer. The Web server can respond to requests from computers on this network or any computer on the Internet. The **mail server** handles and delivers email over the network. Servers

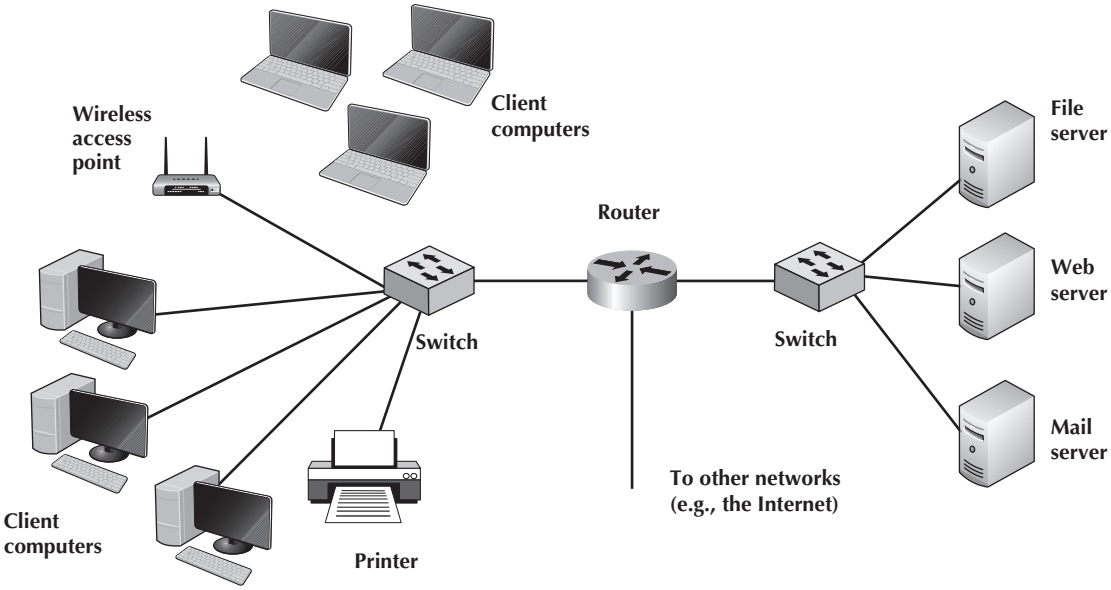



**FIGURE 1-2** Example of a local area network (LAN)

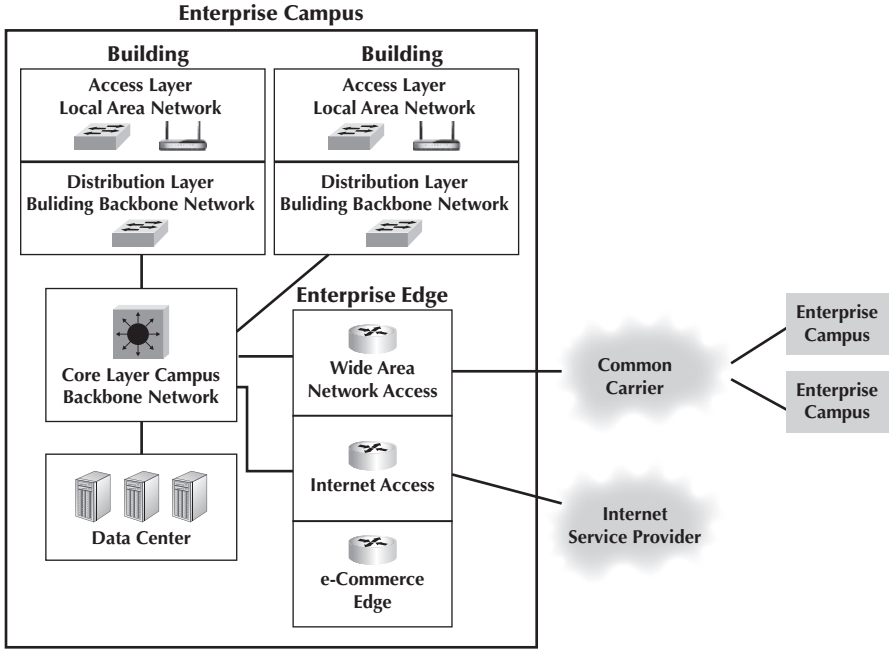



**FIGURE 1-3**
Network architecture components

are usually personal computers (often more powerful than the other personal computers on the network) but may be mainframes too.

There are three computers that make networks what they are. These are the client, the server, and the router. The client initiates a communication with the server by sending a request to the server. Once the server receives the request, it processes it, and responds with a response. The router makes this connection possible.

All three devices are computers, and their hardware is pretty much the same—they have a motherboard with CPU (central processing unit), memory, and some storage space. However, only the client had a screen, keyboard, and mouse. Why? Are the server and router less deserving? No. Their purpose is not to receive an input from the user (keyboard or mouse) or display output (screen) but rather to respond to requests, so they have no need for. Pretty clever, isn't it!

You probably know that a client can have a variety of client operating systems (e.g., Windows, Mac OS, or Linux) and application software (e.g., a web browser, outlook). Likewise, a server can have different operating systems (e.g., Windows, Linux, or z/OS) and application software (e.g., web server software, Exchange). What do you think is the operating system on a router? It turns out that about 90% of routers run Cisco IOS (Inter-operating system) that was specifically created for routers. In fact, Cisco IOS is the second most popular operating system in the world, ahead of Mac and Linux. Interesting, right?

### 1.2.2 Types of Networks

There are many different ways to categorize networks. One of the most common ways is to look at the geographic scope of the network. Figure 1-3 illustrates three types of networks: local area networks (LANs), backbone networks (BNs), and wide area networks (WANs). The distinctions among these are becoming blurry because some network technologies now used in LANs were originally developed for WANs, and vice versa. Any rigid classification of technologies is certain to have exceptions.

A **local area network (LAN)** is a group of computers located in the same general area. A LAN covers a clearly defined small area, such as one floor or work area, a single building, or a group of buildings. The upper-left diagram in Figure 1-3 shows a small LAN located in the records building at the former McClellan Air Force Base in Sacramento. LANs support high-speed data transmission compared with standard telephone circuits, commonly operating 100 million bits per second (100 Mbps). LANs and wireless LANs are discussed in detail in Chapter 6.

Most LANs are connected to a **backbone network (BN)**, a larger, central network connecting several LANs, other BNs, MANs, and WANs. BNs typically span from hundreds of feet to several miles and provide very high-speed data transmission, commonly 100–1,000 Mbps. The second diagram in Figure 1-3 shows a BN that connects the LANs located in several buildings at McClellan Air Force Base. BNs are discussed in detail in Chapter 7.

**Wide area networks (WANs)** connect BNs and MANs (see Figure 1-1). Most organizations do not build their own WANs by laying cable, building microwave towers, or sending up satellites (unless they have unusually heavy data transmission needs or highly specialized requirements, such as those of the Department of Defense). Instead, most organizations lease circuits from IXCs (e.g., AT&T, Sprint) and use those to transmit their data. WAN circuits provided by IXCs come in all types and sizes but typically span hundreds or thousands of miles and provide data transmission rates from 64 Kbps to 10 Gbps. WANs are discussed in detail in Chapter 8.

Two other common terms are **intranets** and **extranets**. An intranet is a LAN that uses the same technologies as the Internet (e.g., Web servers, Java, HTML [Hypertext Markup Language]) but is open to only those inside the organization. For example, although some pages on a Web server may be open to the public and accessible by anyone on the Internet, some pages may be on an intranet and therefore hidden from those who connect to the Web server from the Internet at large. Sometimes, an intranet is provided by a completely separate Web server hidden from the Internet. The intranet for the Information Systems Department at Indiana University, for example, provides information on faculty expense budgets, class scheduling for future semesters (e.g., room, instructor), and discussion forums.

An extranet is similar to an intranet in that it, too, uses the same technologies as the Internet but instead is provided to invited users outside the organization who access it over the Internet. It can provide access to information services, inventories, and other internal organizational databases that are provided only to customers, suppliers, or those who have paid for access. Typically, users are given passwords to gain access, but more sophisticated technologies such as smart cards or special software may also be required. Many universities provide extranets for Web-based courses so that only those students enrolled in the course can access course materials and discussions.

## 1.3 NETWORK MODELS

There are many ways to describe and analyze data communications networks. All networks provide the same basic functions to transfer a message from sender to receiver, but each network can use different network hardware and software to provide these functions. All of these hardware and software products have to work together to successfully transfer a message.

One way to accomplish this is to break the entire set of communications functions into a series of **layers**, each of which can be defined separately. In this way, vendors can develop software and hardware to provide the functions of each layer separately. The software or hardware can work in any manner and can be easily updated and improved, as long as the interface between that layer and the ones around it remains unchanged. Each piece of hardware and software can then work together in the overall network.

There are many different ways in which the network layers can be designed. The two most important network models are the Open Systems Interconnection Reference (OSI) model and the

Internet model. Of the two, the Internet model is the most commonly used; few people use the OSI model, although understand it is commonly required for network certification exams.

### 1.3.1 Open Systems Interconnection Reference Model

The **Open Systems Interconnection Reference model** (usually called the **OSI model** for short) helped change the face of network computing. Before the OSI model, most commercial networks used by businesses were built using nonstandardized technologies developed by one vendor (remember that the Internet was in use at the time but was not widespread and certainly was not commercial). During the late 1970s, the International Organization for Standardization (ISO) created the Open System Interconnection Subcommittee, whose task was to develop a framework of standards for computer-to-computer communications. In 1984, this effort produced the OSI model.

The OSI model is the most talked about and most referred to network model. If you choose a career in networking, questions about the OSI model will be on the network certification exams offered by Microsoft, Cisco, and other vendors of network hardware and software. However, you will probably never use a network based on the OSI model. Simply put, the OSI model never caught on commercially in North America, although some European networks use it, and some network components developed for use in the United States arguably use parts of it. Most networks today use the Internet model, which is discussed in the next section. However, because there are many similarities between the OSI model and the Internet model, and because most people in networking are expected to know the OSI model, we discuss it here. The OSI model has seven layers (see Figure 1-4).

**Layer 1: Physical Layer** The *physical layer* is concerned primarily with transmitting data bits (zeros or ones) over a communication circuit. This layer defines the rules by which ones and zeros are transmitted, such as voltages of electricity, number of bits sent per second, and the physical format of the cables and connectors used.

**Layer 2: Data Link Layer** The *data link layer* manages the physical transmission circuit in layer 1 and transforms it into a circuit that is free of transmission errors as far as layers above are concerned. Because layer 1 accepts and transmits only a raw stream of bits without understanding their meaning or structure, the data link layer must create and recognize message boundaries; that is, it must mark where a message starts and where it ends. Another major task of layer 2 is

**FIGURE 1-4**
Network models. OSI = Open Systems Interconnection Reference

| OSI Model | Internet Model | Groups of Layers | Examples |
|---|---|---|---|
| 7. Application Layer | 5. Application Layer | *Application Layer* | Internet Explorer and Web pages |
| 6. Presentation Layer | | | |
| 5. Session Layer | | | |
| 4. Transport Layer | 4. Transport Layer | *Internetwork Layer* | TCP/IP software |
| 3. Network Layer | 3. Network Layer | | |
| 2. Data Link Layer | 2. Data Link Layer | *Hardware Layer* | Ethernet port, Ethernet cables, and Ethernet software drivers |
| 1. Physical Layer | 1. Physical Layer | | |

to solve the problems caused by damaged, lost, or duplicate messages so the succeeding layers are shielded from transmission errors. Thus, layer 2 performs error detection and correction. It also decides when a device can transmit so that two computers do not try to transmit at the same time. We say, that data link layer has a local responsibility.

**Layer 3: Network Layer** The *network layer* performs routing. It determines the next computer to which the message should be sent, so it can follow the best route through the network and finds the full address for that computer if needed.

**Layer 4: Transport Layer** The *transport layer* deals with end-to-end issues, such as procedures for entering and departing from the network. It establishes, maintains, and terminates logical connections for the transfer of data between the original sender and the final destination of the message. It is responsible for breaking a large data transmission into smaller packets (if needed), ensuring that all the packets have been received, eliminating duplicate packets, and performing flow control to ensure that no computer is overwhelmed by the number of messages it receives. Although error control is performed by the data link layer, the transport layer can also perform error checking. Therefore, transport layer has a global responsibility.

**Layer 5: Session Layer** The *session layer* is responsible for managing and structuring all sessions. Session initiation must arrange for all the desired and required services between session participants, such as logging on to circuit equipment, transferring files, and performing security checks. Session termination provides an orderly way to end the session, as well as a means to abort a session prematurely. It may have some redundancy built in to recover from a broken transport (layer 4) connection in case of failure. The session layer also handles session accounting so the correct party receives the bill.

**Layer 6: Presentation Layer** The *presentation layer* formats the data for presentation to the user. Its job is to accommodate different interfaces on different computers so the application program need not worry about them. It is concerned with displaying, formatting, and editing user inputs and outputs. For example, layer 6 might perform data compression, translation between different data formats, and screen formatting. Any function (except those in layers 1 through 5) that is requested sufficiently often to warrant finding a general solution is placed in the presentation layer, although some of these functions can be performed by separate hardware and software (e.g., encryption).

**Layer 7: Application Layer** The *application layer* is the end user's access to the network. The primary purpose is to provide a set of utilities for application programs. Each user program determines the set of messages and any action it might take on receipt of a message. Other network-specific applications at this layer include network monitoring and network management.

### 1.3.2 Internet Model

The network model that dominates current hardware and software is a more simple five-layer **Internet model**. Unlike the OSI model that was developed by formal committees, the Internet model evolved from the work of thousands of people who developed pieces of the Internet. The OSI model is a formal standard that is documented in one standard, but the Internet model has never been formally defined; it has to be interpreted from a number of standards. The two models have very much in common (see Figure 1-4); simply put, the Internet model collapses the top

three OSI layers into one layer. Because it is clear that the Internet has won the "war," we use the five-layer Internet model for the rest of this book.

**Layer 1: The Physical Layer** The **physical layer** in the Internet model, as in the OSI model, is the physical connection between the sender and receiver. Its role is to transfer a series of electrical, radio, or light signals through the circuit. The physical layer includes all the *hardware* devices (e.g., computers, modems, and switches) and physical *media* (e.g., cables and satellites). The physical layer specifies the type of connection and the electrical signals, radio waves, or light pulses that pass through it. Chapter 3 discusses the physical layer in detail.

**Layer 2: The Data Link Layer** The **data link layer** is responsible for moving a message from one computer to the next computer in the network path from the sender to the receiver. The data link layer in the Internet model performs the same three functions as the data link layer in the OSI model. First, it controls the physical layer by deciding when to transmit messages over the media. Second, it formats the messages by indicating where they start and end. Third, it detects and may correct any errors that have occurred during transmission. Chapter 4 discusses the data link layer in detail.

**Layer 3: The Network Layer** The **network layer** in the Internet model performs the same functions as the network layer in the OSI model. First, it performs routing, in that it selects the next computer to which the message should be sent. Second, it can find the address of that computer if it doesn't already know it. Chapter 5 discusses the network layer in detail.

**Layer 4: The Transport Layer** The **transport layer** in the Internet model is very similar to the transport layer in the OSI model. It performs two functions. First, it is responsible for linking the application layer software to the network and establishing end-to-end connections between the sender and receiver when such connections are needed. Second, it is responsible for breaking long messages into several smaller messages to make them easier to transmit and then recombining the smaller messages back into the original larger message at the receiving end. The transport layer can also detect lost messages and request that they be resent. Chapter 5 discusses the transport layer in detail.

**Layer 5: Application Layer** The **application layer** is the application software used by the network user and includes much of what the OSI model contains in the application, presentation, and session layers. It is the user's access to the network. By using the application software, the user defines what messages are sent over the network. Because it is the layer that most people understand best and because starting at the top sometimes helps people understand better, Chapter 2 begins with the application layer. It discusses the architecture of network applications and several types of network application software and the types of messages they generate.

**Groups of Layers** The layers in the Internet are often so closely coupled that decisions in one layer impose certain requirements on other layers. The data link layer and the physical layer are closely tied together because the data link layer controls the physical layer in terms of when the physical layer can transmit. Because these two layers are so closely tied together, decisions about the data link layer often drive the decisions about the physical layer. For this reason, some people group the physical and data link layers together and call them the **hardware layers**. Likewise, the transport and network layers are so closely coupled that sometimes these layers are called the **internetwork layers** (see Figure 1-4). When you design a network, you often think about the network design

in terms of three groups of layers: the hardware layers (physical and data link), the internetwork layers (network and transport), and the application layer.

### 1.3.3 Message Transmission Using Layers

Each computer in the network has software that operates at each of the layers and performs the functions required by those layers (the physical layer is hardware, not software). Each layer in the network uses a formal language, or **protocol**, that is simply a set of rules that define what the layer will do and that provides a clearly defined set of messages that software at the layer needs to understand. For example, the protocol used for Web applications is HTTP (Hypertext Transfer Protocol, which is described in more detail in Chapter 2). In general, all messages sent in a network pass through all layers. All layers except the physical layer create a new **Protocol Data Unit (PDU)** as the message passes through them. The PDU contains information that is needed to transmit the message through the network. Some experts use the word *packet* to mean a PDU. Figure 1-5 shows how a message requesting a Web page would be sent on the Internet.

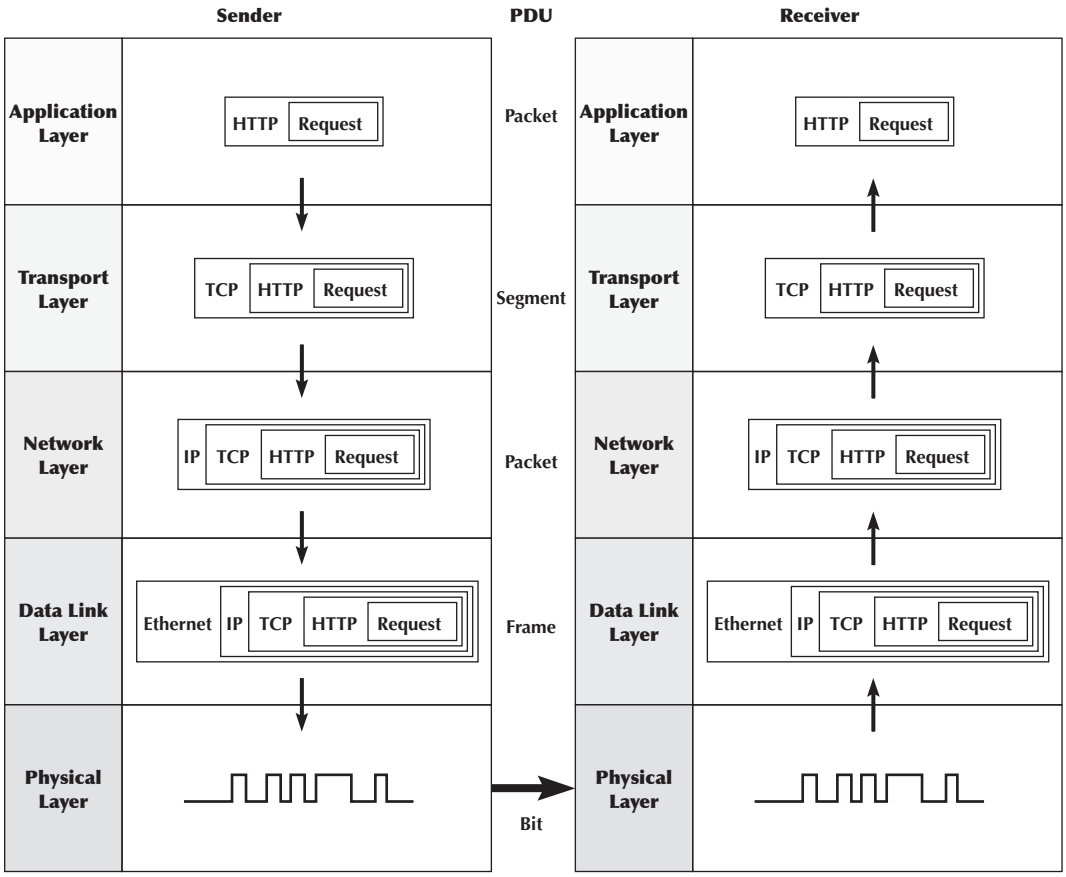



**FIGURE 1-5** Message transmission using layers. IP = Internet Protocol; HTTP = Hypertext Transfer Protocol; TCP = Transmission Control Protocol

**Application Layer** First, the user creates a message at the application layer using a Web browser by clicking on a link (e.g., get the home page at www.somebody.com). The browser translates the user's message (the click on the Web link) into HTTP. The rules of HTTP define a specific PDU—called an HTTP packet—that all Web browsers must use when they request a Web page. For now, you can think of the HTTP packet as an envelope into which the user's message (*get the Web page*) is placed. In the same way that an envelope placed in the mail needs certain information written in certain places (e.g., return address, destination address), so too does the HTTP packet. The Web browser fills in the necessary information in the HTTP packet, drops the user's request inside the packet, then passes the HTTP packet (containing the Web page request) to the transport layer.

**Transport Layer** The transport layer on the Internet uses a protocol called TCP (transmission control protocol), and it, too, has its own rules and its own PDUs. TCP is responsible for breaking large files into smaller packets and for opening a connection to the server for the transfer of a large set of packets. The transport layer places the HTTP packet inside a TCP PDU (which is called a TCP segment), fills in the information needed by the TCP segment, and passes the TCP segment (which contains the HTTP packet, which, in turn, contains the message) to the network layer.

**Network Layer** The network layer on the Internet uses a protocol called IP (Internet Protocol), which has its rules and PDUs. IP selects the next stop on the message's route through the network. It places the TCP segment inside an IP PDU, which is called an IP packet, and passes the IP packet, which contains the TCP segment, which, in turn, contains the HTTP packet, which, in turn, contains the message, to the data link layer.

**Data Link Layer** If you are connecting to the Internet using a LAN, your data link layer may use a protocol called Ethernet, which also has its own rules and PDUs. The data link layer formats the message with start and stop markers, adds error checks information, places the IP packet inside an Ethernet PDU, which is called an Ethernet frame, and instructs the physical hardware to transmit the Ethernet frame, which contains the IP packet, which contains the TCP segment, which contains the HTTP packet, which contains the message.

**Physical Layer** The physical layer in this case is network cable connecting your computer to the rest of the network. The computer will take the Ethernet frame (complete with the IP packet, the TCP segment, the HTTP packet, and the message) and send it as a series of electrical pulses through your cable to the server.

When the server gets the message, this process is performed in reverse. The physical hardware translates the electrical pulses into computer data and passes the message to the data link layer. The data link layer uses the start and stop markers in the Ethernet frame to identify the message. The data link layer checks for errors and, if it discovers one, requests that the message be resent. If a message is received without error, the data link layer will strip off the Ethernet frame and pass the IP packet (which contains the TCP segment, the HTTP packet, and the message) to the network layer. The network layer checks the IP address and, if it is destined for this computer, strips off the IP packet and passes the TCP segment, which contains the HTTP packet and the message, to the transport layer. The transport layer processes the message, strips off the TCP segment, and passes the HTTP packet to the application layer for processing. The application layer (i.e., the Web server) reads the HTTP packet and the message it contains (the request for the Web page) and processes it by generating an HTTP packet containing the Web page you requested. Then the process starts again as the page is sent back to you.

**The Pros and Cons of Using Layers** There are three important points in this example. First, there are many different software packages and many different PDUs that operate at different layers to successfully transfer a message. Networking is in some ways similar to the Russian *matryoshka*, nested dolls that fit neatly inside each other. This is called *encapsulation*, because the PDU at a higher level is placed inside the PDU at a lower level so that the lower-level PDU encapsulates the higher-level one. The major advantage of using different software and protocols is that it is easy to develop new software, because all one has to do is write software for one level at a time. The developers of Web applications, for example, do not need to write software to perform error checking or routing, because those are performed by the data link and network layers. Developers can simply assume those functions are performed and just focus on the application layer. Similarly, it is simple to change the software at any level (or add new application protocols), as long as the interface between that layer and the ones around it remains unchanged.

Second, it is important to note that for communication to be successful, each layer in one computer must be able to communicate with its matching layer in the other computer. For example, the physical layer connecting the client and server must use the same type of electrical signals to enable each to understand the other (or there must be a device to translate between them). Ensuring that the software used at the different layers is the same as accomplished by using *standards*. A standard defines a set of rules, called *protocols*, that explain exactly how hardware and software that conform to the standard are required to operate. Any hardware and software that conform to a standard can communicate with any other hardware and software that conform to the same standard. Without standards, it would be virtually impossible for computers to communicate.

Third, the major disadvantage of using a layered network model is that it is somewhat inefficient. Because there are several layers, each with its own software and PDUs, sending a message involves many software programs (one for each protocol) and many PDUs. The PDUs add to the total amount of data that must be sent (thus increasing the time it takes to transmit), and the different software packages increase the processing power needed in computers. Because the protocols are used at different layers and are stacked on top of one another (take another look at Figure 1-5), the set of software used to understand the different protocols is often called a **protocol stack**.

## 1.4 NETWORK STANDARDS

### 1.4.1 The Importance of Standards

**Standards** are necessary in almost every business and public service entity. For example, before 1904, fire hose couplings in the United States were not standard, which meant a fire department in one community could not help in another community. The transmission of electric current was not standardized until the end of the nineteenth century, so customers had to choose between Thomas Edison's direct current (DC) and George Westinghouse's alternating current (AC).

The primary reason for standards is to ensure that hardware and software produced by different vendors can work together. Without networking standards, it would be difficult—if not impossible—to develop networks that easily share information. Standards also mean that customers are not locked into one vendor. They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices.

The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

### 1.4.2 The Standards-Making Process

There are two types of standards: *de jure* and *de facto*. A *de jure* standard is developed by an official industry or a government body and is often called a formal standard. For example, there are *de jure* standards for applications such as Web browsers (e.g., HTTP, HTML), for network layer software (e.g., IP), for data link layer software (e.g., Ethernet IEEE 802.3), and for physical hardware (e.g., V.90 modems). *De jure* standards typically take several years to develop, during which time technology changes, making them less useful.

*De facto* standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a *de facto* standard. In the communications industry, *de facto* standards often become *de jure* standards once they have been widely accepted.

The *de jure standardization process* has three stages: specification, identification of choices, and acceptance. The *specification* stage consists of developing a nomenclature and identifying the problems to be addressed. In the *identification of choices* stage, those working on the standard identify the various solutions and choose the optimum solution from among the alternatives. *Acceptance*, which is the most difficult stage, consists of defining the solution and getting recognized industry leaders to agree on a single, uniform solution. As with many other organizational processes that have the potential to influence the sales of hardware and software, standards-making processes are not immune to corporate politics and the influence of national governments.

**International Organization for Standardization** One of the most important standards-making bodies is the International Organization for Standardization (ISO), which makes technical recommendations about data communication interfaces (see www.iso.org). ISO is based in Geneva, Switzerland. The membership is composed of the national standards organizations of each ISO member country.

**International Telecommunications Union-Telecommunications Group** The **International Telecommunications Union-Telecommunications Group (ITU-T)** is the technical standards-setting organization of the United Nations International Telecommunications Union, which is also based in Geneva (see www.itu.int). ITU is composed of representatives from about 200 member countries. Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).

**American National Standards Institute** The **American National Standards Institute (ANSI)** is the coordinating organization for the U.S. national system of standards for both technology and nontechnology (see www.ansi.org). ANSI has about 1,000 members from both public and private organizations in the United States. ANSI is a standardization organization, not a standards-making body, in that it accepts standards developed by other organizations and publishes them as American standards. Its role is to coordinate the development of voluntary national standards and to interact with the ISO to develop national standards that comply with the ISO's international recommendations. ANSI is a voting participant in the ISO.

MANAGEMENT FOCUS

## 1-2 How Network Protocols Become Standards

There are many standards organizations around the world, but perhaps the best known is the **Internet Engineering Task Force (IETF)**. IETF sets the standards that govern how much of the Internet operates.

The IETF, like all standards organizations, tries to seek consensus among those involved before issuing a standard. Usually, a standard begins as a protocol (i.e., a language or set of rules for operating) developed by a vendor (e.g., HTML). When a protocol is proposed for standardization, the IETF forms a working group of technical experts to study it. The working group examines the protocol to identify potential problems and possible extensions and improvements, and then issues a report to the IETF.

If the report is favorable, the IETF issues a **Request for Comment (RFC)** that describes the proposed standard and solicits comments from the entire world. Most large software companies likely to be affected by the proposed standard prepare detailed responses. Many "regular" Internet users also send their comments to the IETF.

The IETF reviews the comments and possibly issues a new and improved RFC, which again is posted for more comments. Once no additional changes have been identified, it becomes a proposed standard.

Usually, several vendors adopt the proposed standard and develop products based on it. Once at least two vendors have developed hardware or software based on it and it has proven successful in operation, the proposed standard is changed to a draft standard. This is usually the final specification, although some protocols have been elevated to Internet standards, which usually signifies mature standards not likely to change.

The process does not focus solely on technical issues; almost 90% of the IETF's participants work for manufacturers and vendors, so market forces and politics often complicate matters. One former IETF chairperson who worked for a hardware manufacturer has been accused of trying to delay the standards process until his company had a product ready, although he and other IETF members deny this. Likewise, former IETF directors have complained that members try to standardize every product their firms produce, leading to a proliferation of standards, only a few of which are truly useful.

*Sources:* "How Networking Protocols Become Standards," *PC Week*, March 17, 1997; "Growing Pains," *Network World*, April 14, 1997.

MANAGEMENT FOCUS

## 1-3 Keeping Up with Technology

The data communications and networking arena changes rapidly. Significant new technologies are introduced and new concepts are developed almost every year. It is therefore important for network managers to keep up with these changes.

There are at least three useful ways to keep up with change. First and foremost for users of this book is the website for this book, which contains updates to the book, additional sections, teaching materials, and links to useful websites.

Second, there are literally hundreds of thousands of websites with data communications and networking information. Search engines can help you find them. A good initial starting point is the telecom glossary at http://www.atis.org. Three other useful sites are http://www.zdnet.com, http://www.networkcomputing.com, and http://www.zdnet.com.

Third, there are many useful magazines that discuss computer technology in general and networking technology in particular, including *Network Computing, Info World, Info Week*, and *CIO Magazine*.

| Layer | Common Standards |
|---|---|
| 5. Application layer | HTTP, HTML (Web)<br>MPEG, H.323 (audio/video)<br>SMTP, IMAP, POP (email) |
| 4. Transport layer | TCP (Internet and LANs) |
| 3. Network layer | IP (Internet and LANs) |
| 2. Data link layer | Ethernet (LAN)<br>Frame relay (WAN)<br>T1 (MAN and WAN) |
| 1. Physical layer | RS-232C cable (LAN)<br>Category 5 cable (LAN)<br>V.92 (56 Kbps modem) |

**FIGURE 1-6**
Some common data communications standards. HTML = Hypertext Markup Language; HTTP = Hypertext Transfer Protocol; IMAP = Internet Message Access Protocol; IP = Internet Protocol; LAN = Local Area Network; MPEG = Motion Picture Experts Group; POP = Post Office Protocol; TCP = Transmission Control Protocol

**Institute of Electrical and Electronics Engineers** The **Institute of Electrical and Electronics Engineers (IEEE)** is a professional society in the United States whose Standards Association (IEEE-SA) develops standards (see www.standards.ieee.org). The IEEE-SA is probably most known for its standards for LANs. Other countries have similar groups; for example, the British counterpart of IEEE is the Institution of Electrical Engineers (IEE).

**Internet Engineering Task Force** The **Internet Engineering Task Force (IETF)** sets the standards that govern how much of the Internet will operate (see www.ietf.org). The IETF is unique in that it doesn't really have official memberships. Quite literally anyone is welcome to join its mailing lists, attend its meetings, and comment on developing standards. The role of the IETF and other Internet organizations is discussed in more detail in Chapter 8; also, see the box entitled "How Network Protocols Become Standards."

### 1.4.3 Common Standards

There are many different standards used in networking today. Each standard usually covers one layer in a network. Some of the most commonly used standards are shown in Figure 1-6. At this point, these models are probably just a maze of strange names and acronyms to you, but by the end of the book, you will have a good understanding of each of these. Figure 1-6 provides a brief road map for some of the important communication technologies we discuss in this book.

For now, there is one important message you should understand from Figure 1-6: For a network to operate, many different standards must be used simultaneously. The sender of a message must use one standard at the application layer, another one at the transport layer, another one at the network layer, another one at the data link layer, and another one at the physical layer. Each layer and each standard is different, but all must work together to send and receive messages.

Either the sender and receiver of a message must use the same standards or, more likely, there are devices between the two that translate from one standard into another. Because different networks often use software and hardware designed for different standards, there is often a lot of translation between different standards.

## 1.5 FUTURE TRENDS

The field of data communications has grown faster and become more important than computer processing itself. Both go hand in hand, but we have moved from the computer era to the communication era. Three major trends are driving the future of communications and networking.

### 1.5.1 Wireless LAN and BYOD

The rapid development of mobile devices, such as smartphones and tablets, has encouraged employers to allow their employees to bring these devices to work and use them to access data, such as their work email. This movement, called bring your own device, or **Bring Your On Device (BYOD)**, is a great way to get work quickly, saves money, and makes employees happy. But BYOD also brings its own problems. Employers need to add or expand their Wireless Local Area Networks (WLANs) to support all these new devices.

Another important problem is security. Employees bring these devices to work so that they can access not only their email but also other critical company assets, such as information about their clients, suppliers, or sales. Employers face myriad decisions about how to manage access to company applications for BYOD. Companies can adopt two main approaches: (1) native apps or (2) browser-based technologies. **Native apps** require an app to be developed for each application that an employee might be using for every potential device that the employee might use (e.g., iPhone, Android, Windows). The **browser-based** approach (often referred to as responsive design using HTML5) doesn't create an app but rather requires employees to access the application through a Web browser. Both these approaches have their pros and cons, and only the future will show which one is the winner.

What if an employee loses his or her mobile phone or tablet so that the application that accesses critical company data now can be used by anybody who finds the device? Will the company's data be compromised? Device and data loss practices now have to be added to the general security practices of the company. Employees need to have apps to allow their employer to wipe their phones clean in case of loss so that no company data are compromised (e.g., SOTI's MobiControl). In some cases, companies require the employee to allow monitoring of the device at all times, to ensure that security risks are minimized. However, some argue that this is not a good practice because the device belongs to the employee, and monitoring it 24/7 invades the employee's privacy.

### 1.5.2 The Internet of Things

Telephones and computers used to be separate. Today voice and data have converged into unified communications, with phones plugged into computers or directly into the LAN using Voice over Internet Protocol (VoIP). Vonage and Skype have taken this one step further and offer telephone service over the Internet at dramatically lower prices than traditional separate landline phones, whether from traditional phones or via computer microphones and speakers.

Computers and networks can also be built into everyday things, such as kitchen appliances, doors, and shoes. In the future, the Internet will move from being a Web of computers to also being an **Internet of Things (IoT),** as smart devices become common, that creates the **Network of Things (NoT)** where all this interaction between IoT devices will happen seamlessly, without human intervention. And you might already be asking Alexa or Siri for advice on where to eat, lock, and unlock your apartment, turn on/off your lights, or change the thermostat setting. For this to happen, Alexa/Siri must be able to communicate with your lock or thermostat without any intervention from you.

Google is a leading innovator in the IoT world. It entered the IoT playground with the Nest thermostat. Google has also been developing a self-driving car that not only passes a standard


Photo courtesy of the authors

**FIGURE 1-7**
A security robot on the IOT

driving test but also has fewer collisions than cars driven by humans. Other car developers are also developing autonomous vehicles.

IoT technologies are not restricted to consumer use. To the contrary, they are used in many places such as manufacturing, process automation, decision analytics, and smart electrical grids. However, the underlying principle of all the applications is that IoT devices are connected to the Internet either through wired or wireless Ethernet. Figure 1-7 shows an IOT device that we encountered in a mall in Boston. It is semi-autonomous security robot, meaning it can be controlled by a human or set to roam its environment. Ten years ago, network managers would never have thought about the need to manage robots over their networks.

### 1.5.3 Massively Online

You have probably heard of massively multiplayer online games, such as World of Warcraft, where you can play with thousands of players in real time. Well, today not only games are massively online. Education is massively online. Edx, Khan Academy, Lynda.com, or Code Academy have websites that offer thousands of education modules for children and adults in myriad fields to help them learn. Your class very likely also has an online component. You may even use this textbook online and decide whether your comments are for you only, for your instructor, or for the entire class to read. In addition, you may have heard about massive open online courses, or MOOC. MOOC enable students who otherwise wouldn't have access to elite universities to get access to top knowledge without having to pay the tuition. These classes are offered by universities, such as Stanford, UC Berkeley, MIT, UCLA, Carnegie Mellon, and of course, Indiana University, free of charge and for no credit (although at some universities, you can pay and get credit toward your degree).

Politics has also moved massively online. President Obama reached out to the crowds and ordinary voters not only through his Facebook page but also through Reddit and Google Hangouts. President Trump's use of Twitter is unprecedented. He can directly reach millions of followers—a strategy that paid off in the 2016 elections. Finally, massively online allows activists to reach masses of people in a very short period of time to initiate change. Examples of use of YouTube videos or Facebook for activism include the Arab Spring, Kony 2012, or the use of sarin gas in Syria.

So what started as a game with thousands of people being online at the same time is being reinvented for good use in education, politics, and activism. Only the future will show what humanity can do with what massively online has to offer.

What these three trends have in common is that there will be an increasing demand for professionals who understand development of data communications and networking infrastructure to support this growth. There will be more and more need to build faster and more secure networks that will allow individuals and organizations to connect to resources, probably stored on cloud infrastructure (either private or public). This need will call not only for engineers who deeply understand the technical aspects of networks but also for highly social individuals who embrace technology in creative ways to allow business to achieve a competitive edge through utilizing this technology. So the call is for you who are reading this book—you are in the right place at the right time!

## 1.6 IMPLICATIONS FOR CYBER SECURITY

At the end of each chapter, we provide key implications for **cyber security** that arise from the topics discussed in the chapter. We draw implications that focus on improving the management of networks and information systems as well as implications for cyber security of an individual and an organization.

There are three key implications for management from this chapter. First, networks and the Internet change almost everything. Computer networks and the Internet are designed to quickly and easily move information from distant locations and to enable individuals inside and outside the firm to access information and products from around the world. However, this ease of doing work on the Internet makes it also easy for cyber criminals to steal files from your computer or to put files on your computer (such as viruses or malware). Understanding how computer networks and the Internet work and how computers communicate via networks is the first step toward defending your own computer and the computers on a company's network.

Second, today's networking environment requires that a wide variety of devices could connect. Employees' use of their own devices under BYOD policies increases security risks, as does the move to the IoT. Several security experts say that IoT doesn't stand for Internet of Things; it stands for Internet of Targets. Individuals and companies have to balance BYOD and IoT risks and rewards to create a useful and secure computing infrastructure.

Third, as the demand for network services and network capacity increases, so too will the need for secure storage and server space and secure transfer of data. Finding efficient ways to securely store all the information we generate will open new market opportunities. Today, Google has almost a million Web servers (see Figure 1-8). If we assume that each server costs an average of $1,000, the money large companies spend on storage is close to $1 billion. Capital expenditure of this scale is then increased by money spent on power and staffing. One way companies can reduce this amount of money is to store their data using cloud computing. The good news is that more and more cloud providers meet or exceed government required security measures for data storage and transfer.

**FIGURE 1-8**
One server farm with more than 1,000 servers

zentilia/Getty Images

## SUMMARY

**Introduction** The information society, where information and intelligence are the key drivers of personal, business, and national success, has arrived. Data communications is the principal enabler of the rapid information exchange and will become more important than the use of computers themselves in the future. Successful users of data communications, such as Wal-Mart, can gain significant competitive advantage in the marketplace.

**Network Definitions** A LAN is a group of computers located in the same general area. A BN is a large central network that connects almost everything on a single company site. A metropolitan area network (MAN) encompasses a city or county area. A wide area network (WAN) spans city, state, or national boundaries.

**Network Model** Communication networks are often broken into a series of layers, each of which can be defined separately, to enable vendors to develop software and hardware that can work together in the overall network. In this book, we use a five-layer model. The application layer is the application software used by the network user. The transport layer takes the message generated by the application layer and, if necessary, breaks it into several smaller messages. The network layer addresses the message and determines its route through the network. The data link layer formats the message to indicate where it starts and ends, decides when to transmit it over the physical media, and detects and corrects any errors that occur in transmission. The physical layer is the physical connection between the sender and receiver, including the hardware devices (e.g., computers, terminals, and modems) and physical media (e.g., cables and satellites). Each layer, except the physical layer, adds a Protocol Data Unit (PDU) to the message.

**Standards** Standards ensure that hardware and software produced by different vendors can work together. A *de jure* standard is developed by an official industry or a government body. *De facto* standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. Many different standards and standards-making organizations exist.

**Future Trends** At the same time as the use of BYOD offers efficiency at the workplace, it opens up the doors for security problems that companies need to consider. Our interactions with

colleagues and family will very likely change in the next 5–10 years because of the Internet of Things (IoT), where devices will interact with each other without human intervention. Finally, massively online not only changed the way we play computer games but also showed that humanity can change its history.

## KEY TERMS



## QUESTIONS

1. How can data communications networks affect businesses?
2. How do data communications networks support the four core capabilities of MIS?
3. Discuss three important applications of data communications networks in business and personal use.
4. How do LANs differ from WANs and BNs?
5. What is a circuit?
6. What is a client?
7. What is a server?
8. What is a router?
9. There are three computers that make the Internet work. Name them and describe their similarities and differences.
10. Why are network layers important?
11. Describe the seven layers in the OSI network model and what they do.
12. Describe the five layers in the Internet network model and what they do.
13. Explain how a message is transmitted from one computer to another using layers.
14. Describe the three stages of standardization.
15. How are Internet standards developed?
16. Describe two important data communications standards-making bodies. How do they differ?
17. What is the purpose of a data communications standard?
18. Discuss three trends in communications and networking.
19. Why has the Internet model replaced the OSI model?
20. In the 1980s, when we wrote the first edition of this book, there were many, many more protocols in common use at the data link, network, and transport layers than there are today. Why do you think the number of commonly used protocols at these layers has declined? Do you think this trend will continue? What are the implications for those who design and operate networks?

21. The number of standardized protocols in use at the application layer has significantly increased since the 1980s. Why? Do you think this trend will continue? What are the implications for those who design and operate networks?
22. How many bits (not bytes) are there in a 10-page text document? Hint: There are approximately 350 words on a double-spaced page. We need 8 bits to encode each character.
23. What are three current cyber security issues we face on the Internet?
24. What is the Internet of Things (IoT)? What are the benefits and risks of IoT?

## EXERCISES

**A.** Investigate the latest cyber security threats. What services and/or data were affected by these threats? What was done to recover from this situation?

**B.** It turns out that not all industries are equally sensitive to cyber-attacks. There are multiple industries that belong to the "critical infrastructure." Investigate which industries belong to the critical infrastructure, why are they part of it, and what laws govern this group of industries regarding cyber security.

**C.** Discuss the issue of communications monopolies and open competition with an economics instructor and relate his or her comments to your data communication class.

**D.** Find a college or university offering a specialized degree in telecommunications or data communications and describe the program.

**E.** Investigate the IoT. What IoT devices are you most interested in? Why?

**F.** Investigate the networks in your school or organization. Describe the important LANs and BNs in use (but do not describe the specific clients, servers, or devices on them).

**G.** Visit the Internet Engineering Task (IETF) website (www.ietf.org). Describe one standard that is in the RFC stage.

**H.** Discuss how the revolution/evolution of communications and networking is likely to affect how you will work and live in the future.

**I.** Investigate the pros and cons of developing native apps versus taking a browser-based approach.

## MINICASES

**I. Global Consultants** John Adams is the chief information officer (CIO) of Global Consultants (GC), a very large consulting firm with offices in more than 100 countries around the world. GC is about to purchase a set of several Internet-based financial software packages that will be installed in all of their offices. There are no standards at the application layer for financial software but several software companies that sell financial software (call them group A) use one *de facto* standard to enable their software to work with one another's software. However, another group of financial software companies (call them group B) use a different *de facto* standard. Although both groups have software packages that GC could use, GC would really prefer to buy one package from group A for one type of financial analysis and one package from group B for a different type of financial analysis. The problem, of course, is that then the two packages cannot communicate and GC's staff would end up having to type the same data into both packages. The alternative is to buy two packages from the same group—so that data could be easily shared—but that would mean having to settle for second best for one of the packages. Although there have been some reports in the press about the two groups of companies working together to develop one common standard that will enable software to work together, there is no firm agreement yet. What advice would you give Adams?

**II. Atlas Advertising** Atlas Advertising is a regional advertising agency with offices in Boston, New York, Providence, Washington, D.C., and Philadelphia. (1) Describe the types of networks you think they would have (e.g., LANs, BNs, WANs) and where they are likely to be located. (2) What types of standard protocols and

technologies do you think they are using at each layer (e.g., see Figures 1-3 and 1-5)?

III. **Consolidated Supplies** Consolidated Supplies is a medium-sized distributor of restaurant supplies that operates in Canada and several northern U.S. states. They have 12 large warehouses spread across both countries to service their many customers. Products arrive from the manufacturers and are stored in the warehouses until they are picked and put on a truck for delivery to their customers. The networking equipment in their warehouses is old and is starting to give them problems; these problems are expected to increase as the equipment gets older. The vice president of operations, Pat McDonald, would like to replace the existing LANs and add some new wireless LAN technology into all the warehouses, but he is concerned that now may not be the right time to replace the equipment. He has read several technology forecasts that suggest there will be dramatic improvements in networking speeds over the next few years, especially in wireless technologies. He has asked you for advice about upgrading the equipment. Should Consolidated Supplies replace all the networking equipment in all the warehouses now, should it wait until newer networking technologies are available, or should it upgrade some of the warehouses this year, some next year, and some the year after, so that some warehouses will benefit from the expected future improvements in networking technologies?

IV. **Asia Importers** Caisy Wong is the owner of a small catalog company that imports a variety of clothes and houseware from several Asian countries and sells them to its customers over the Web and by telephone through a traditional catalog. She has read about the convergence of voice and data and is wondering about changing her current traditional, separate, and rather expensive telephone and data services into one service offered by a new company that will supply both telephone and data over her Internet connection. What are the potential benefits and challenges that Asia Importers should consider in making the decision about whether to move to one integrated service?

## TECH UPDATES

In every chapter, we will offer couple ideas to investigate.

### Topic A: From ARPANET To NoT: What Happened to the Internet?

What started as a secret military project in the 1960s, grew to the largest network of interconnected computers known as the Internet, which is changing into the largest network of interconnected devices that (at the time they were discovered) were not meant to talk to each other. Discuss the history of the Internet (ARPANET) and the future of it (NoT).

### Topic B: A Brief History of Cyber Attacks

We all heard about modern ransomware that encrypts every file on your computer and you must pay a ransom (in bitcoin, of course!) to get these files unencrypted, or phishing attacks (emails that pretend to be real) that ask you to download a file or click on link and can cause lot of harm to you and your data. But, when did this start? What was the evolution of attacks on the Internet? How did individuals, business, and governments respond to these attacks? What is the current citation with cyber-attacks?

### Deliverables

Your job will be to prepare a presentation/video (7–10 minutes long) that addresses the topic and provides information on the following items:

1. Title Slide
2. Short description of topic
3. Main players—these could be people, processes, software, hardware, etc.
4. How it works—use lot of pictures and be as technical as possible; create this part as a tutorial so that your audience can follow along
5. How does it relate to material covered in class so far (and in the future)
6. Additional material/books/links where to learn more about this topic
7. Credits
8. List of References
9. Memo addressed to your professor describing all of the above information

## HANDS-ON ACTIVITY 1A

### Internet as We Know It Today

We think about access to the Internet as a daily normal. We check our email, news, chat with friends and family, and do shopping on the Internet. The objective of this activity is for you to experience this convergence.

1. Investigate the history of the Internet at http://www.vox.com/a/internet-maps that shows you a history of the Internet through maps.
2. See how many people are using the Internet in your state/country at https://www.akamai.com/us/en/resources/visualizing-akamai/real-time-web-monitor.jsp?tab=traffic&theme=dark.
3. See the cyber security attacks in progress on information systems connected to the Internet by clicking on the **Attacks** tab at https://www.akamai.com/us/en/resources/visualizing-akamai/real-time-web-monitor.jsp?tab=attacks&theme=dark.

### Deliverable

Write a one-page summary of the history and current state of the Internet. What was the most surprising thing you learned during your investigation?

## HANDS-ON ACTIVITY 1B

### Seeing the PDUs in Your Messages

We talked about how messages are transferred using layers and the different PDUs used at each layer. The objective of this activity is for you to see the different PDUs in the messages that you send. To do this, we'll use Wireshark, which is one of the world's foremost network protocol analyzers and is the de facto standard that most professional and education institutions use today. It is used for network troubleshooting, network analysis, software and communications protocol development, and general education about how networks work.

Wireshark enables you to see all messages sent by your computer, as well as some or all of the messages sent by other computers on your LAN, depending on how your LAN is designed. Most modern LANs are designed to prevent you from eavesdropping on other computer's messages, but some older ones still permit this. Normally, your computer will ignore the messages that are not addressed for your computer, but Wireshark enables you to eavesdrop and read messages sent to and from other computers.

Wireshark is free. Before you start this activity, download and install it from https://www.wireshark.org.

1. Start Wireshark.
2. Click on Capture and then Interfaces. Click the Start button next to the active interface (the one that is receiving and sending packets). Your network data will be captured from this moment on.
3. Open your browser and go to a Web page that you have not visited recently (a good one is www.iana.org).
4. Once the Web page has loaded, go back to Wireshark and stop the packet capture by clicking on Capture and then Stop (the hot key for this is Ctrl + E).
5. You will see results similar to those in Figure 1-9. There are three windows below the tool bar:
   a. The top window is the Packet List. Each line represents a single message or packet that was captured by Wireshark. Different types of packets will have different colors. For example, HTTP packets are colored green. Depending on how busy your network is, you may see a small number of packets in this window or a very large number of packets.
   b. The middle window is the Packet Detail. This will show the details for any packet you click on in the top window.
   c. The bottom window shows the actual contents of the packet in hexadecimal format, so it is usually hard to read. This window is typically used by network programmers to debug errors.
6. Let's take a look at the packets that were used to request the Web page and send it to your computer. The application layer protocol used on the Web is HTTP, so we'll want to find the HTTP packets. In the Filter toolbar, type http and hit enter.

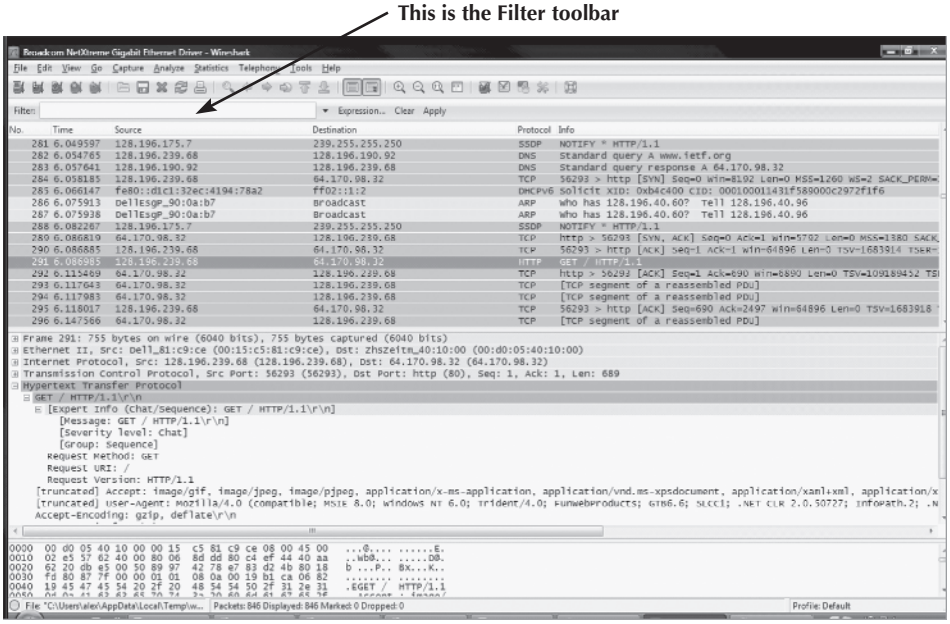



**FIGURE 1-9** Wireshark capture

7. This will highlight all the packets that contain HTTP packets and will display the first one in Packet Detail window. Look at the Packet Detail window in Figure 1-8 to see the PDUs in the message we've highlighted. You'll see that it contains an Ethernet II Frame, an IP packet, a TCP segment, and an HTTP packet. You can see inside any or all of these PDUs by clicking on the +box in front of them. In Figure 1-8, you'll see that we've clicked the +box in front of the HTTP packet to show you what's inside it.

## Deliverables

1. List the PDU at layers 2, 3, and 4 that were used to transmit your HTTP GET packet.
   a. Locate your HTTP GET packet in the Packet List and click on it.
   b. Look in the Packet Detail window to get the PDU information.
2. How many different HTTP GET packets were sent by your browser? Not all the HTTP packets are GET packets, so you'll have to look through them to answer this question.
3. List at least five other protocols that Wireshark displayed in the Packet List window. You will need to clear the filter by clicking on the "Clear" icon that is on the right of the Filter toolbar.