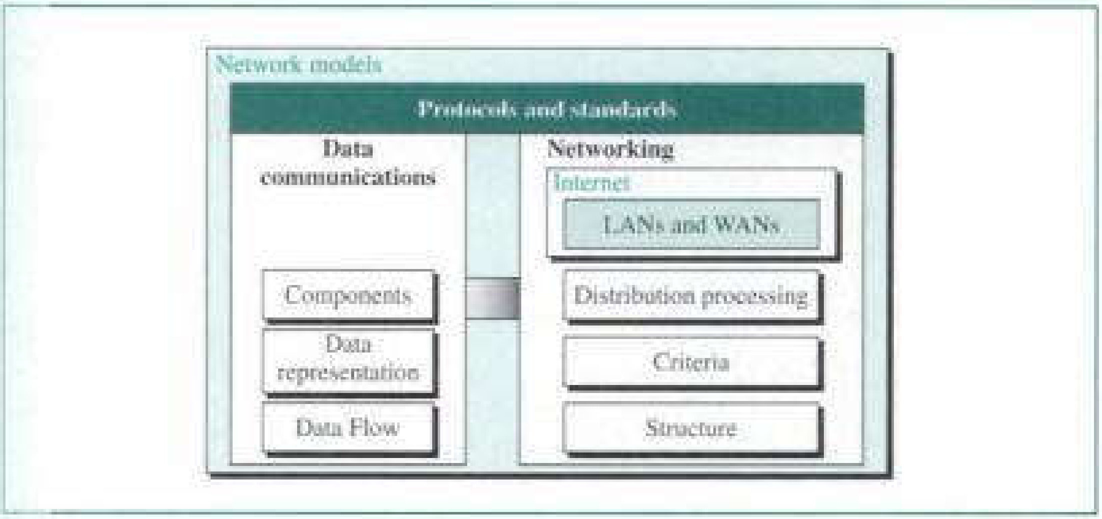
PART 1

Overview of Data Communications and Networking

Data communications and networking are topics that have moved from the technical world to the public realm. Products such as MP3 players and cellular phones are no longer the manifestations of high tech wizardry, but are gadgets toted by everyone from preteens to grandparents. Progress in data communications and networking technologies is proceeding at a rapid rate. Bunny-ear antennas on televisions have gone the way of the dinosaurs, phased out by digital cable and satellite dishes. The home office is moving toward wireless connections as well. The end user of such technologies is only required to know how to use the systems. A student in this field, however, must be familiar with the issues and concepts shown in Figure 1.

Figure 1 *Overview of data communications and networking*



Data Communications

Networks exist so that data may be sent from one place to another—the basic concept of data communications. To fully grasp this subject, we must understand the physical network components, how different types of data can be represented, and how to create a data flow.

Networking

Data communications between remote parties can be achieved through a proces networking, involving the connection of computers, media, and networking When we talk about networks, we need to keep in mind three concepts: distribu cessing, network criteria, and network structure.

Local and Wide Area Networks

Networks are divided into two main categories: local area networks (LANs) a area networks (WANs). These two types of networks have different characteris different functionalities. In general, a LAN is a collection of computers and pe devices in a limited area such as a building or campus. A LAN is usually u domain of a single organization such as a company or department. A WAN, h is a collection of LANs and spans a large geographical distance.

Internet

The Internet, the main of focus of the book, is a collection of LANs and WA together by internetworking devices. In the figure, we demonstrate this relatio having the box entitled *Internet* enclose LANs and WANs. The Internet is, h more than just a physical connection of LANs and WANs; internetworking p and standards are also needed.

Protocols and Standards

Protocols and standards are vital to the implementation of data communication working. Protocols refer to the rules; a standard is a protocol that has been ad vendors and manufacturers. In the diagram, the *Protocols and Standards* bo both data communications and networking to emphasize that each area falls u jurisdiction.

Network Models

Network models serve to organize, unify, and control the hardware and software nents of data communication and networking. Although the term "network suggests a relationship to networking, the model also encompasses data communi

Chapters

In Chapter 1 we briefly discuss the first three topics—data communications, n ing, and protocols and standards. Network models, the cornerstones for the re book, are described in Chapter 2.

CHAPTER 1

Introduction

Data communications and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the decision makers require immediate access to accurate information. Why wait a week for that report from Germany to arrive by mail when it could appear almost instantaneously through computer networks? Businesses today rely on computer networks and internetworks. But before we ask how quickly we can get hooked up, we need to know how networks operate, what types of technologies are available, and which design best fills which set of needs.

The development of the personal computer brought about tremendous changes for business, industry, science, and education. A similar revolution is occurring in data communications and networking. Technological advances are making it possible for communications links to carry more and faster signals. As a result, services are evolving to allow use of the expanded capacity, including the extension to established telephone services such as conference calling, call waiting, voice mail, and caller ID.

Data communications and networking are in their infancy. The goal is to be able to exchange data such as text, audio, and video from any point in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

This chapter addresses four issues: data communications, networks, the Internet, and protocols and standards. First we give a broad definition of data communications. Then we define networks as a highway on which data can travel. The Internet is discussed as a good example of an internetwork (i.e., a network of networks). Finally, we discuss different types of protocols, the difference between protocols and standards, and the organizations that set those standards.

1.1 DATA COMMUNICATIONS

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term **telecommunication,** which includes telephony, telegraphy, and television, means communication at a distance (*tele* is Greek for "far").

The word **data** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

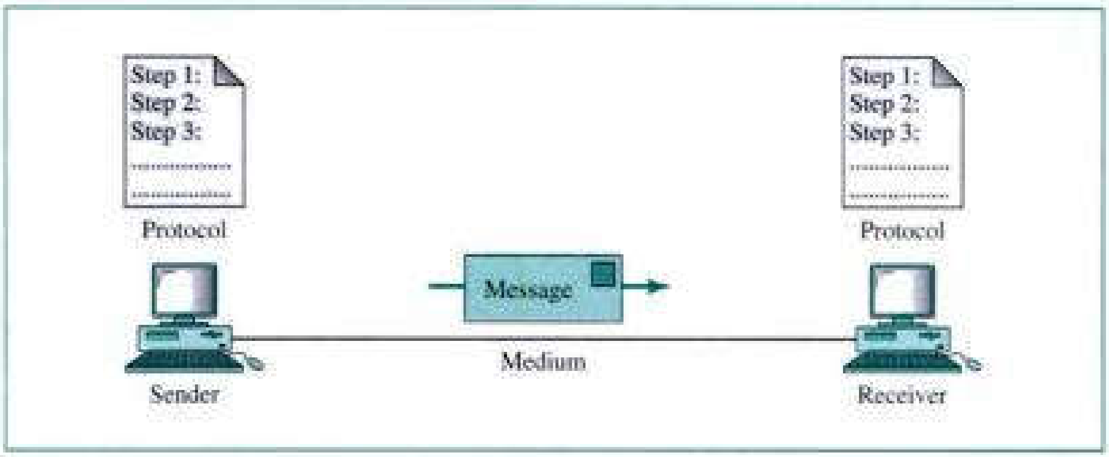
Data communications is the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on three fundamental characteristics: delivery, accuracy, and timeliness.

1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.

Components

A data communications system has five components (see Fig. 1.1).

Figure 1.1 *Five components of data communication*



1. **Message.** The **message** is the information (data) to be communicated. It can consist of text, numbers, pictures, sound, or video—or any combination of these.
2. **Sender.** The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The **receiver** is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Medium.** The **transmission medium** is the physical path by which a message travels from sender to receiver. It could be a twisted-pair wire, coaxial cable, fiber-optic cable, or radio waves (terrestrial or satellite microwave).
5. **Protocol.** A **protocol** is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). The number of bits in a pattern depends on the number of symbols in the language. For example, the English language uses 26 symbols (A, B, C, . . . , Z) to represent uppercase letters, 26 symbols (a, b, c, . . . , z) to represent lowercase letters, 10 symbols (0, 1, 2, . . . , 9) to represent numeric characters, and symbols (., ?, :, ;, . . . , !) to represent punctuation. Other symbols such as the blank, the newline, and the tab are used for text alignment and readability.

Different sets of bit patterns have been designed to represent text symbols. Each set is called a **code,** and the process of representing symbols is called coding.

ASCII The American National Standards Institute (ANSI) developed a code called the American Standard Code for Information Interchange (ASCII). This code uses 7 bits for each symbol. This means 128 (2^7) different symbols can be defined by this code. The full bit patterns for ASCII code are found in Appendix A.

Extended ASCII To make the size of each pattern 1 byte (8 bits), the ASCII bit patterns are augmented with an extra 0 at the left. Now each pattern is exactly 1 byte of memory. In other words, in extended ASCII, the first pattern is 00000000 and the last one is 01111111.

Unicode Neither of the foregoing codes represents symbols belonging to languages other than English. For that, a code with much greater capacity is needed. A coalition of hardware and software manufacturers have designed a code called Unicode that uses 16 bits and can represent up to 65,536 (2^{16}) symbols. Different sections of the code are allocated to symbols from different languages in the world. Some parts of the code are used for graphical and special symbols.

ISO The International Organization for Standardization, known as ISO, has designed a code using a 32-bit pattern. This code can represent up to 4,294,967,296 (2^{32}) symbols, which is definitely enough to represent any symbol in the world today.

Numbers

Numbers are also represented by using bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number. The reason is to simplify mathematical operations on numbers. Appendix B lists the binary numbers and their equivalents.

Images

Images today are also represented by bit patterns. However, the mechanism is different. In its simpler form, an image is divided into a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on what is called the *resolution.* For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black-and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.

To represent color images, each colored pixel is decomposed into three primary colors: red, green, and blue (RGB). Then the intensity of each color is measured, and a bit pattern (usually 8 bits) is assigned to it. In other words, each pixel has three bit patterns: one to represent the intensity of the red color, one to represent the intensity of the green color, and one to represent the intensity of the blue color.

Audio

Audio is a representation of sound. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. In Chapters 4 and 5, we learn how to change audio to a digital or an analog signal.

Video

Video can be produced either as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal, as we will see in Chapters 4 and 5.

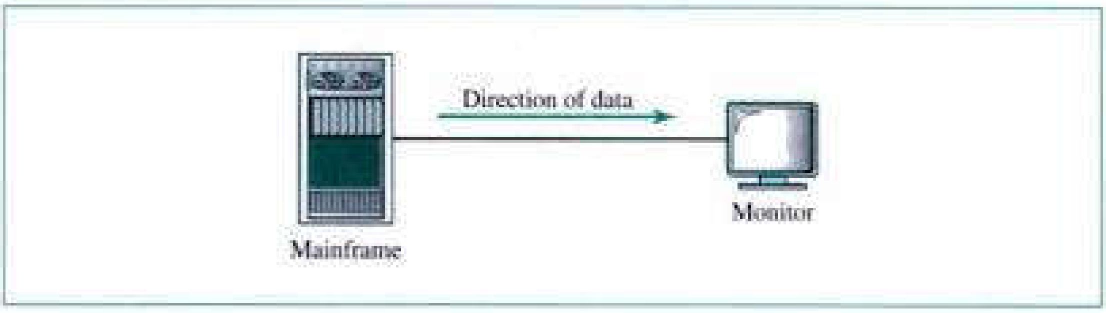
Direction of Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

Simplex

In **simplex mode,** the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Fig. 1.2).

Figure 1.2 *Simplex*

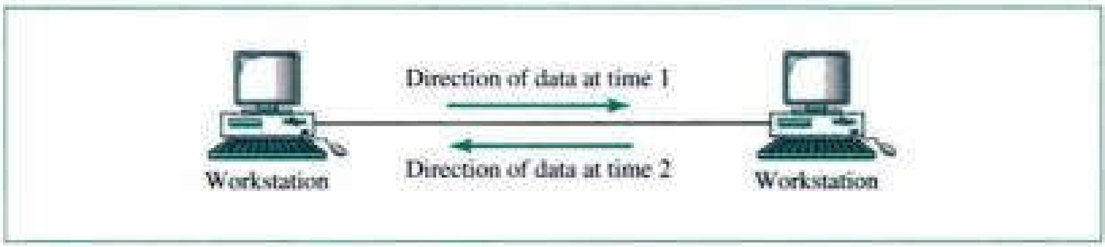


Keyboards and traditional monitors are both examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.

Half-Duplex

In **half-duplex mode,** each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Fig. 1.3).

Figure 1.3 *Half-duplex*

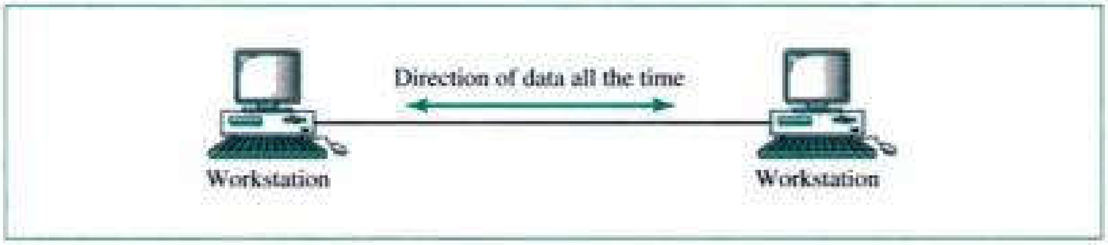


The half-duplex mode is like a one-lane road with two-directional traffic. While cars are traveling one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

In **full-duplex mode** (also called **duplex**), both stations can transmit and receive simultaneously (see Fig. 1.4).

Figure 1.4 *Full-duplex*



The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in either direction share the capacity of the link. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

1.2 NETWORKS

A **network** is a set of devices (often referred to as *nodes*) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Distributed Processing

Most networks use **distributed processing,** in which a task is divided among multiple computers. Instead of a single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Reliability

In addition to accuracy of delivery, network **reliability** is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network **security** issues include protecting data from unauthorized access.

Physical Structures

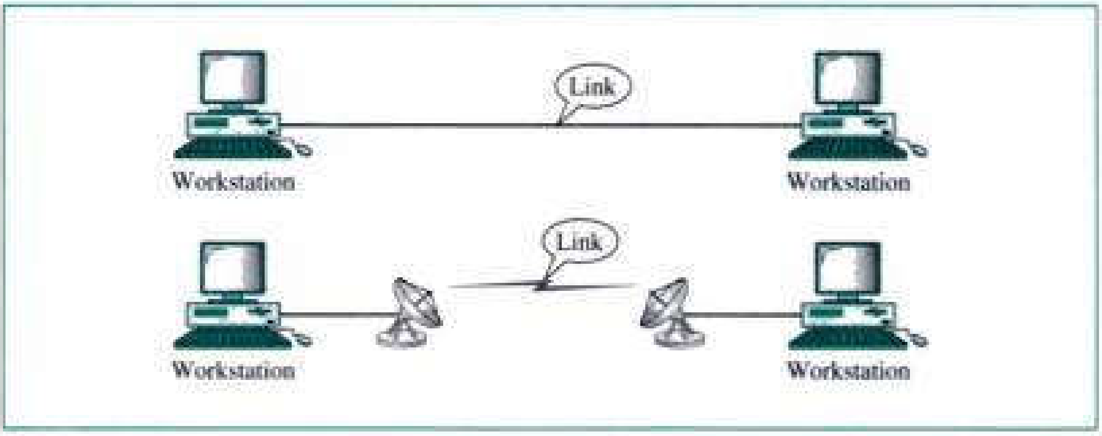
Before discussing networks, we need to define some network attributes.

Type of Connection

A network is two or more devices connected together through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible type of connections: point-to-point and multipoint.

Point-to-Point A **point-to-point** connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Fig. 1.5). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

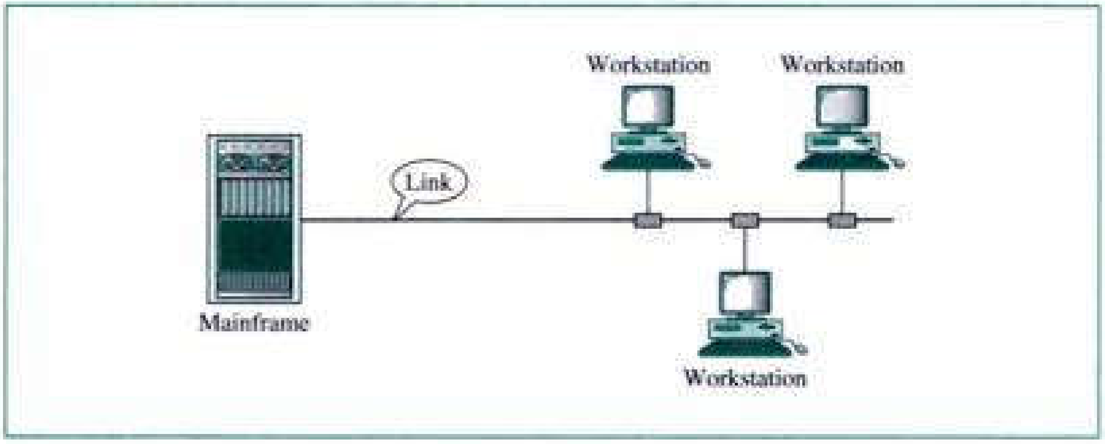
Figure 1.5 *Point-to-point connection*



Multipoint A **multipoint** (also called **multidrop**) connection is one in which more than two specific devices share a single link (see Fig. 1.6).

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshare* connection.

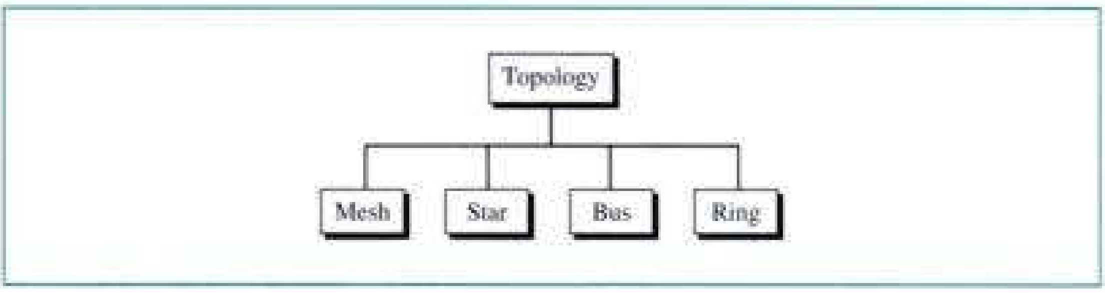
Figure 1.6 *Multipoint connection*



Physical Topology

The term **physical topology** refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and

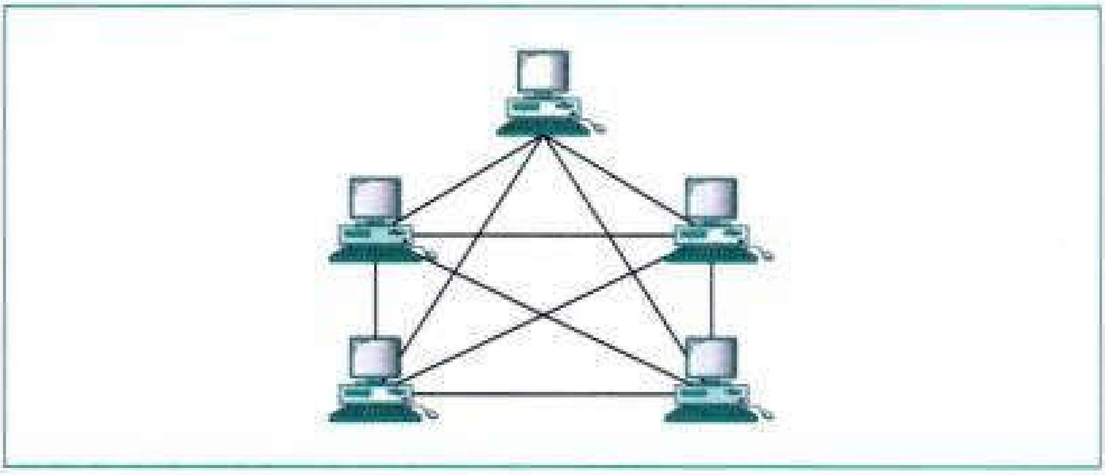
Figure 1.7 *Categories of topology*



linking devices (usually called **nodes**) to one another. There are four basic topologies possible: mesh, star, bus, and ring (see Fig. 1.7).

Mesh In a **mesh topology,** every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. A fully connected mesh network therefore has $n(n-1)/2$ physical channels to link n devices. To accommodate that many links, every device on the network must have $n-1$ input/output (I/O) ports (see Fig. 1.8).

Figure 1.8 *Fully connected mesh topology (for five devices)*

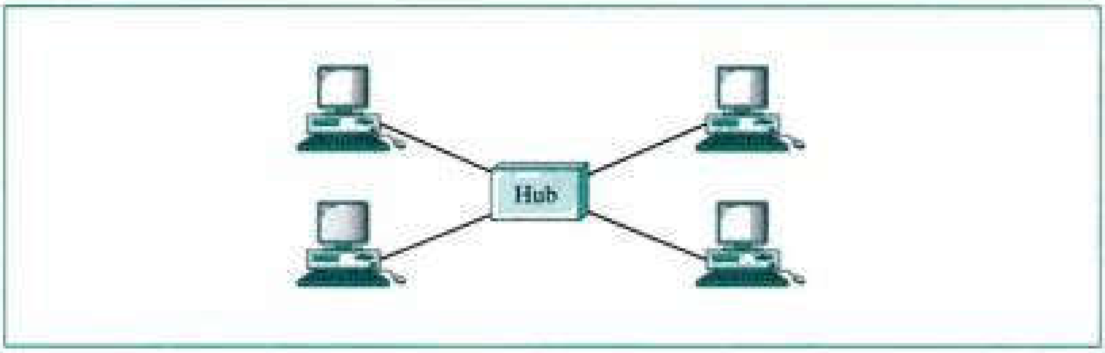


A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Another advantage is privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion—for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

Star In a **star topology,** each device has a dedicated point-to-point link only to a central controller, usually called a **hub.** The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Fig. 1.9).

Figure 1.9 *Star topology*



A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

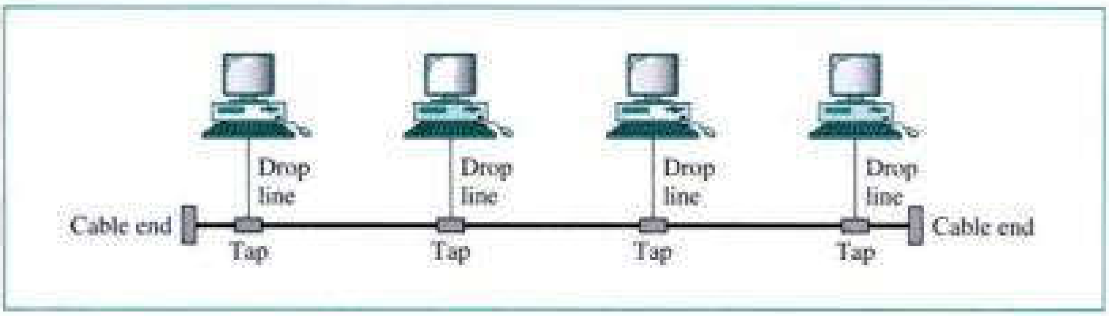
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

However, although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network (see Fig. 1.10).

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it has to travel farther

Figure 1.10 *Bus topology*



and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

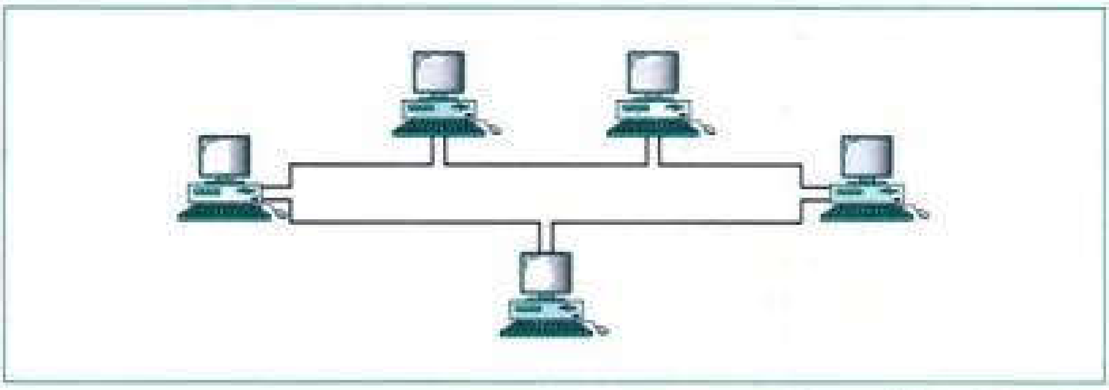
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring In a **ring topology,** each device has a dedicated point-to-point connection only with the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Fig. 1.11).

Figure 1.11 *Ring topology*



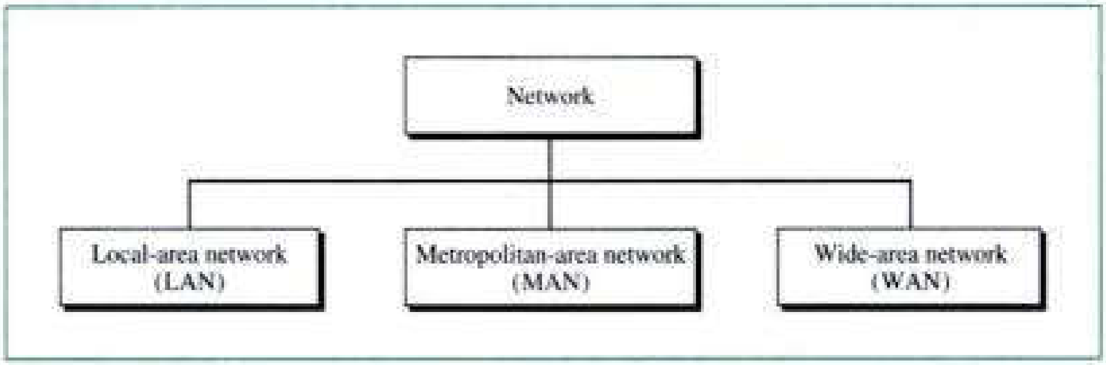
A ring is relatively easy to install and reconfigure. Each device is linked only to its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Categories of Networks

Today when we speak of networks, we are generally referring to three primary categories: local area networks, metropolitan area networks, and wide area networks. Into which category a network falls is determined by its size, its ownership, the distance it covers, and its physical architecture (see Fig. 1.12).

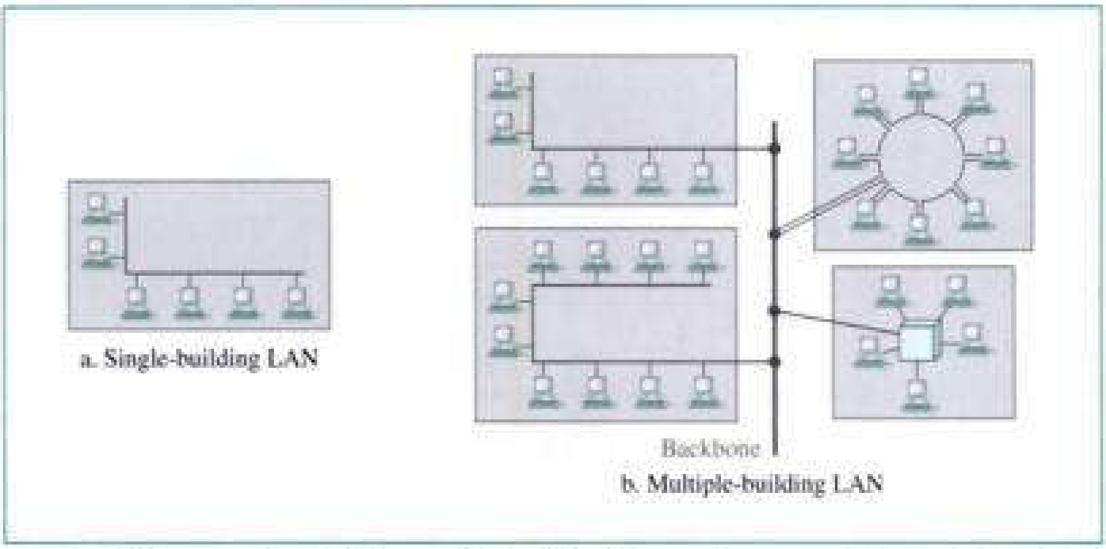
Figure 1.12 *Categories of networks*



Local Area Network (LAN) A **local area network (LAN)** is usually privately owned and links the devices in a single office, building, or campus (see Fig. 1.13). Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large-capacity disk drive and may become a server to the other clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

Figure 1.13 *LAN*



a. Single-building LAN

b. Multiple-building LAN

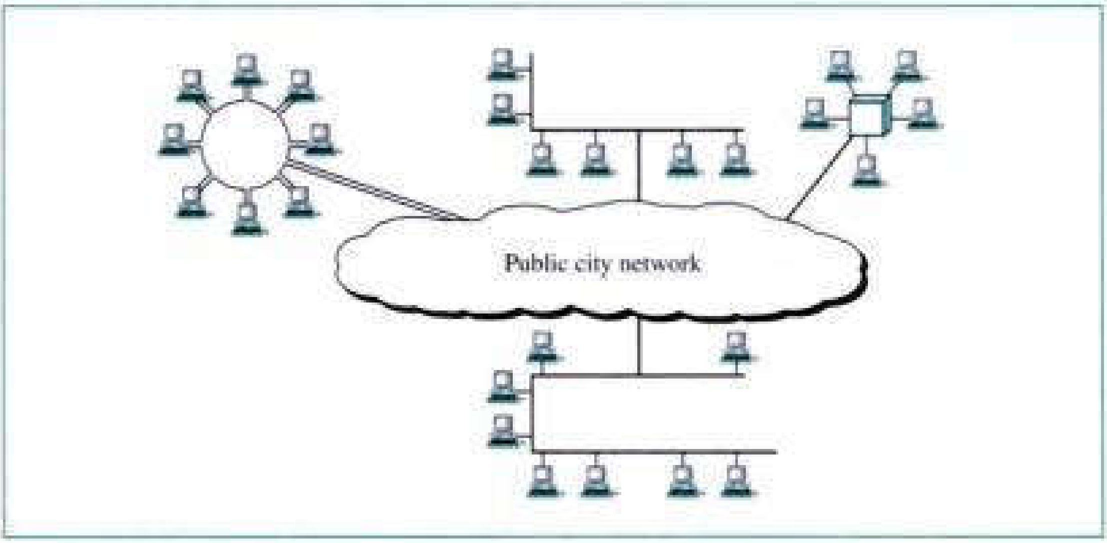
In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.

Traditionally, LANs have data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are increasing and can reach 100 Mbps with gigabit systems in development. LANs are discussed at length in Chapters 14, 15, and 16.

Metropolitan-Area Network (MAN) A **metropolitan-area network (MAN)** is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. For example, a company can use a MAN to connect the LANs in all its offices throughout a city (see Fig. 1.14).

A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company. Many

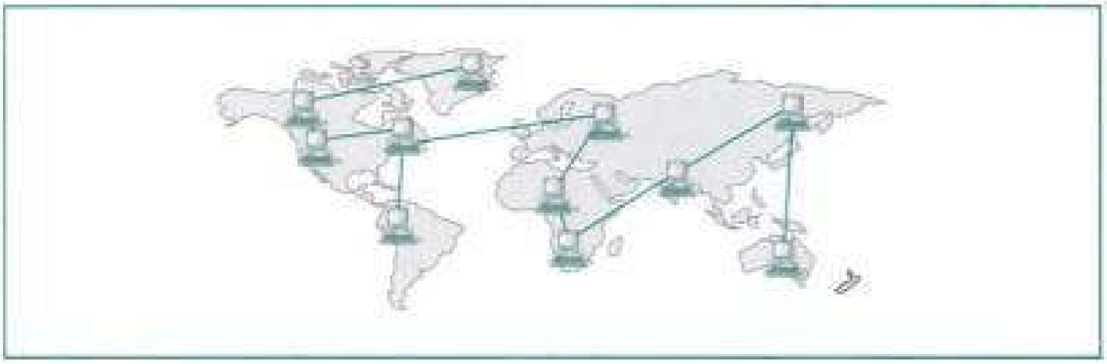
Figure 1.14 *MAN*



telephone companies provide a popular MAN service called Switched Multi-megabit Data Services (SMDS).

Wide Area Network (WAN) A **wide area network (WAN)** provides long-distance transmission of data, voice, image, and video information over large geographic areas that may comprise a country, a continent, or even the whole world (see Fig. 1.15).

Figure 1.15 *WAN*



In contrast to LANs (which depend on their own hardware for transmission), WANs may utilize public, leased, or private communication equipment, usually in combinations, and can therefore span an unlimited number of miles.

A WAN that is wholly owned and used by a single company is often referred to as an *enterprise network*. WANs are discussed in Chapters 17 and 18.

Internetworks When two or more networks are connected, they become an **internetwork,** or **internet.**

1.3 THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (email) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule—all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow Trekker, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

The Internet is a structured, organized system. We begin with a brief history of the Internet. We follow with a description of the Internet today.

A Brief History

A **network** is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the **Internet** (uppercase letter I), a collaboration of more than hundreds of thousands interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for **ARPANET,** a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in turn, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

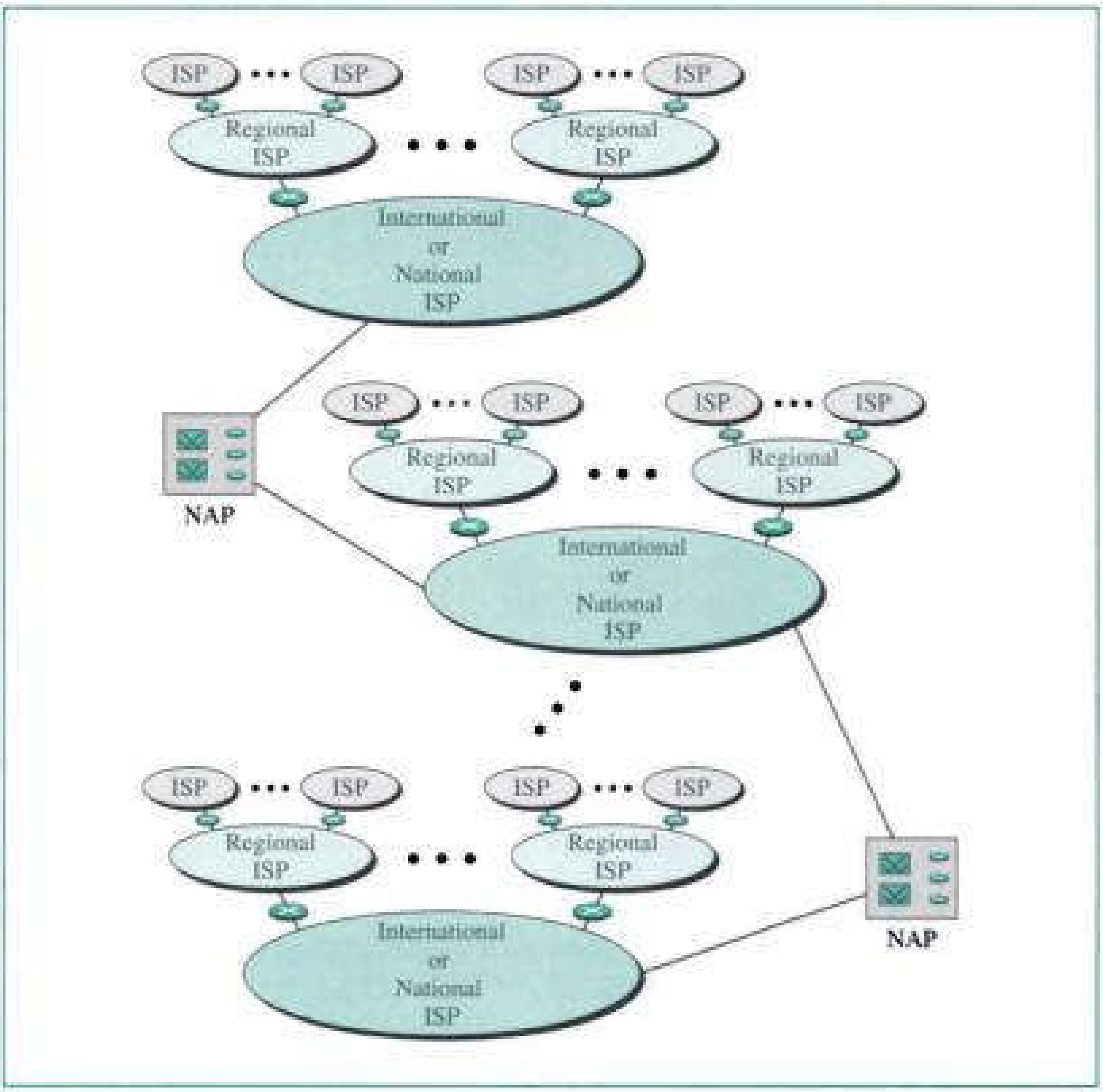
In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Project*. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internetworking Protocol (IP).** IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCP/IP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continuously changing—new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.16 shows a conceptual (not geographic) view of the Internet.

Figure 1.16 *Internet today*



International Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

National Service Providers (NSPs)

National service providers (NSPs) are backbone networks created and maintained by specialized companies. There are many NSPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet MCI. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party), called **network access points (NAPs).** Some NSP networks are also connected to one another by private switching stations called *peering points*. NSPs normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers

Regional internet service providers or **regional ISPs** are smaller ISPs that are connected to one or more NSPs. They are at the third level of hierarchy with a lesser data rate.

Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to NSPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

1.4 PROTOCOLS AND STANDARDS

In this section, we define two widely used terms: protocols and standards. First, we define *protocol,* which is synonymous with *rule.* Then we discuss *standards,* which are agreed-upon rules.

Protocols

In computer networks, communication occurs between entities in different systems. An **entity** is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A **protocol** is a set of rules that governs data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.** Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics.** Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** Timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. They provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

- **De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.** De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology.
- **De jure.** Those that have been legislated by an officially recognized body are **de jure standards.**

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- **International Organization for Standardization (ISO).** The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- **International Telecommunication Union—Telecommunication Standards Sector (ITU-T).** By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the **Consultative Committee for International Telegraphy and Telephony (CCITT).** This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union—Telecommunication Standards Sector (ITU-T).
- **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
- **Institute of Electrical and Electronics Engineers (IEEE).** The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

- **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

Forums

Telecommunications technology development is moving faster than the ability of standards committees to ratify standards. Standards committees are procedural bodies and by nature slow-moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed *forums* made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the **Federal Communications Commission (FCC)** in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and international commerce as it relates to communications.

Internet Standards

An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An **Internet draft** is a working document (a work in progress) with no official status and a 6-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC).** Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

1.5 KEY TERMS

Advanced Research Projects Agency (ARPA)

American National Standards Institute (ANSI)

ARPANET

audio

backbone

bus topology

code

Consultative Committee for International Telegraphy and Telephony (CCITT)

CSNET

data

data communications

de facto standards

de jure standards
distributed processing
Electronic Industries Association (EIA)
entity
Federal Communications Commission (FCC)
forum
full-duplex mode
half-duplex mode
hub
image
Institute of Electrical and Electronics Engineers (IEEE)
International Organization for Standardization (ISO)
International Telecommunication Union–Telecommunication Standards Sector (ITU-T)
Internet
Internet draft
Internet service provider (ISP)
Internet standard
internetwork (internet)
local area network (LAN)
local Internet service providers
maturity levels
mesh topology
message
metropolitan area network (MAN)
multipoint connection
national service provider (NSP)
network
node
performance
physical topology
point-to-point connection
protocol
receiver
regional ISPs
reliability
Request for Comment (RFC)
ring topology
security
semantics
sender
simplex mode
star topology
syntax
telecommunications
timing
Transmission Control Protocol/Internetworking Protocol (TCP/IP)
transmission medium
video
wide area network (WAN)

1.6 SUMMARY

- ❑ Data communication is the transfer of data from one device to another via some form of transmission medium.
- ❑ A data communications system must transmit data to the correct destination in an accurate and timely manner.
- ❑ The five components that make up a data communications system are the message, sender, receiver, medium, and protocol.
- ❑ Text, numbers, images, audio, and video are different forms of information.
- ❑ Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.
- ❑ A network is a set of communication devices connected by media links.
- ❑ In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link.

- ❑ Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.
- ❑ A network can be categorized as a local area network (LAN), a metropolitan-area network (MAN), or a wide area network (WAN).
- ❑ A LAN is a data communication system within a building, plant, or campus, or between nearby buildings.
- ❑ A MAN is a data communication system covering an area the size of a town or city.
- ❑ A WAN is a data communication system spanning states, countries, or the whole world.
- ❑ An internet is a network of networks.
- ❑ The Internet is a collection of many separate networks.
- ❑ TCP/IP is the protocol suite for the Internet.
- ❑ There are local, regional, national, and international Internet service providers (ISPs).
- ❑ A protocol is a set of rules that governs data communication; the key elements of a protocol are syntax, semantics, and timing.
- ❑ Standards are necessary to ensure that products from different manufacturers can work together as expected.
- ❑ The ISO, ITU-T, ANSI, IEEE, and EIA are some of the organizations involved in standards creation.
- ❑ Forums are special-interest groups that quickly evaluate and standardize new technologies.
- ❑ A Request for Comment (RFC) is an idea or concept that is a precursor to an Internet standard.

1.7 PRACTICE SET

Review Questions

1. Identify the five components of a data communications system.
2. What are the advantages of distributed processing?
3. What are the three criteria necessary for an effective and efficient network?
4. What are the advantages of a multipoint connection over a point-to-point connection?
5. What are the two types of line configuration?
6. Categorize the four basic topologies in terms of line configuration.
7. What is the difference between half-duplex and full-duplex transmission modes?
8. Name the four basic network topologies, and give an advantage for each type.
9. For *n* devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?
10. What are some of the factors that determine whether a communication system is a LAN, MAN, or WAN?
11. What is an internet? What is the Internet?

12. Why are protocols needed?
13. Why are standards needed?

Multiple-Choice Questions

14. The _______ is the physical path over which a message travels.
    a. Protocol
    b. Medium
    c. Signal
    d. All the above
15. The information to be communicated in a data communications system is the _______.
    a. Medium
    b. Protocol
    c. Message
    d. Transmission
16. Frequency of failure and network recovery time after a failure are measures of the _______ of a network.
    a. Performance
    b. Reliability
    c. Security
    d. Feasibility
17. An unauthorized user is a network _______ issue.
    a. Performance
    b. Reliability
    c. Security
    d. All the above
18. Which topology requires a central controller or hub?
    a. Mesh
    b. Star
    c. Bus
    d. Ring
19. Which topology requires a multipoint connection?
    a. Mesh
    b. Star
    c. Bus
    d. Ring
20. Communication between a computer and a keyboard involves _____________ transmission.
    a. Simplex
    b. Half-duplex
    c. Full-duplex
    d. Automatic

21. In a network with 25 computers, which topology would require the most extensive cabling?
    a. Mesh
    b. Star
    c. Bus
    d. Ring
22. A television broadcast is an example of _______ transmission.
    a. Simplex
    b. Half-duplex
    c. Full-duplex
    d. Automatic
23. A _______ connection provides a dedicated link between two devices.
    a. Point-to-point
    b. Multipoint
    c. Primary
    d. Secondary
24. In a _______ connection, more than two devices can share a single link.
    a. Point-to-point
    b. Multipoint
    c. Primary
    d. Secondary
25. In _______ transmission, the channel capacity is shared by both communicating devices at all times.
    a. Simplex
    b. Half-duplex
    c. Full-duplex
    d. Half-simplex
26. A cable break in a _______ topology stops all transmission.
    a. Mesh
    b. Bus
    c. Star
    d. Primary
27. Which organization has authority over interstate and international commerce in the communications field?
    a. ITU-T
    b. IEEE
    c. FCC
    d. ISO

Exercises

28. Assume six devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?
29. For each of the following four networks, discuss the consequences if a connection fails.
    a. Five devices arranged in a mesh topology
    b. Five devices arranged in a star topology (not counting the hub)
    c. Five devices arranged in a bus topology
    d. Five devices arranged in a ring topology
30. Draw a hybrid topology with a star backbone and three ring networks.
31. Draw a hybrid topology with a ring backbone and two bus networks.
32. Draw a hybrid topology with a bus backbone connecting two ring backbones. Each ring backbone connects three star networks.
33. Draw a hybrid topology with a star backbone connecting two bus backbones. Each bus backbone connects three ring networks.
34. Find three standards defined by ISO.
35. Find three standards defined by ITU-T.
36. Find three standards defined by ANSI.
37. Find three standards defined by IEEE.
38. Find three standards defined by EIA.
39. Give two instances of how networks are a part of your life today.
40. When a party makes a local telephone call to another party, is this a point-to-point or multipoint connection? Explain your answer.