Networks and Telecommunications

B

Introduction

Change is everywhere in the information technology domain, but nowhere is change more evident and more dramatic than the realm of networks and telecommunications. Most management information systems today rely on digital networks to communicate information in the form of data, graphics, video, and voice. Companies large and small from all over the world are using networks and the Internet to locate suppliers and buyers, to negotiate contracts with them, and to provide bigger, better, and faster services than ever before. ***Telecommunication systems*** enable the transmission of data over public or private networks. A ***network*** is a communications system created by linking two or more devices and establishing a standard methodology by which they can communicate. The world's largest and most widely used network is the Internet. The Internet is a global "network of networks" that uses universal standards to connect millions of different networks around the world. Telecommunication systems and networks are traditionally complicated and historically inefficient. However, businesses can benefit from today's network infrastructures that provide reliable global reach to employees and customers.

LEARNING OUTCOMES

B.1. Compare LANs, WANs, and MANs.

B.2. List and describe the four components that differentiate networks.

B.3. Compare the two types of network architectures.

B.4. Explain topology and the different types found in networks.

B.5. Describe TCP/IP along with its primary purpose.

B.6. Identify the different media types found in networks.

Network Basics

Networks range from small two-computer networks to the biggest network of all, the Internet. A network provides two principle benefits: the ability to communicate and the ability to share.

Today's corporate digital networks include a combination of local area networks, wide area networks, and metropolitan area networks. A ***local area network (LAN)*** is designed to connect a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games, or other applications. A LAN in turn often connects to other LANs, and to the Internet or wide area networks. A ***wide area network (WAN)*** spans a large geographic area, such as a state, province or country. WANs often connect multiple smaller networks, such as local area networks or metropolitan area networks. The world's most popular WAN is the Internet. A ***metropolitan area network (MAN)*** is a large computer network usually spanning a city. Figure B.1 highlights the three different types of networks, and Figure B.2 illustrates each network type.

Direct data communication links between a company and its suppliers or customers, or both, have been successfully used to give the company a strategic advantage. The SABRE airline reservation system is a classic example of a strategic management information system that depends upon communication provided through a network. SABRE Airline Solutions pioneered technological advances for the industry in areas such as revenue management, pricing, flight scheduling, cargo, flight operations, and crew scheduling. In addition, not only did SABRE help invent ecommerce for the travel industry, the company holds claim to progressive solutions that defined—and continue to revolutionize—the travel and transportation marketplace.

A network typically includes four things (besides the computers themselves):

1. **Protocol**—a set of communication rules to make sure that everyone speaks the same language.
2. **Network interface card (NIC)**—card that plugs into the back (or side) of your computers and lets them send and receive messages from other computers.
3. **Cable**—the medium to connect all of the computers together.
4. **Hub (switch or router)**—hardware to perform traffic control.

We will continue to define many of these terms and concepts in the sections that follow.

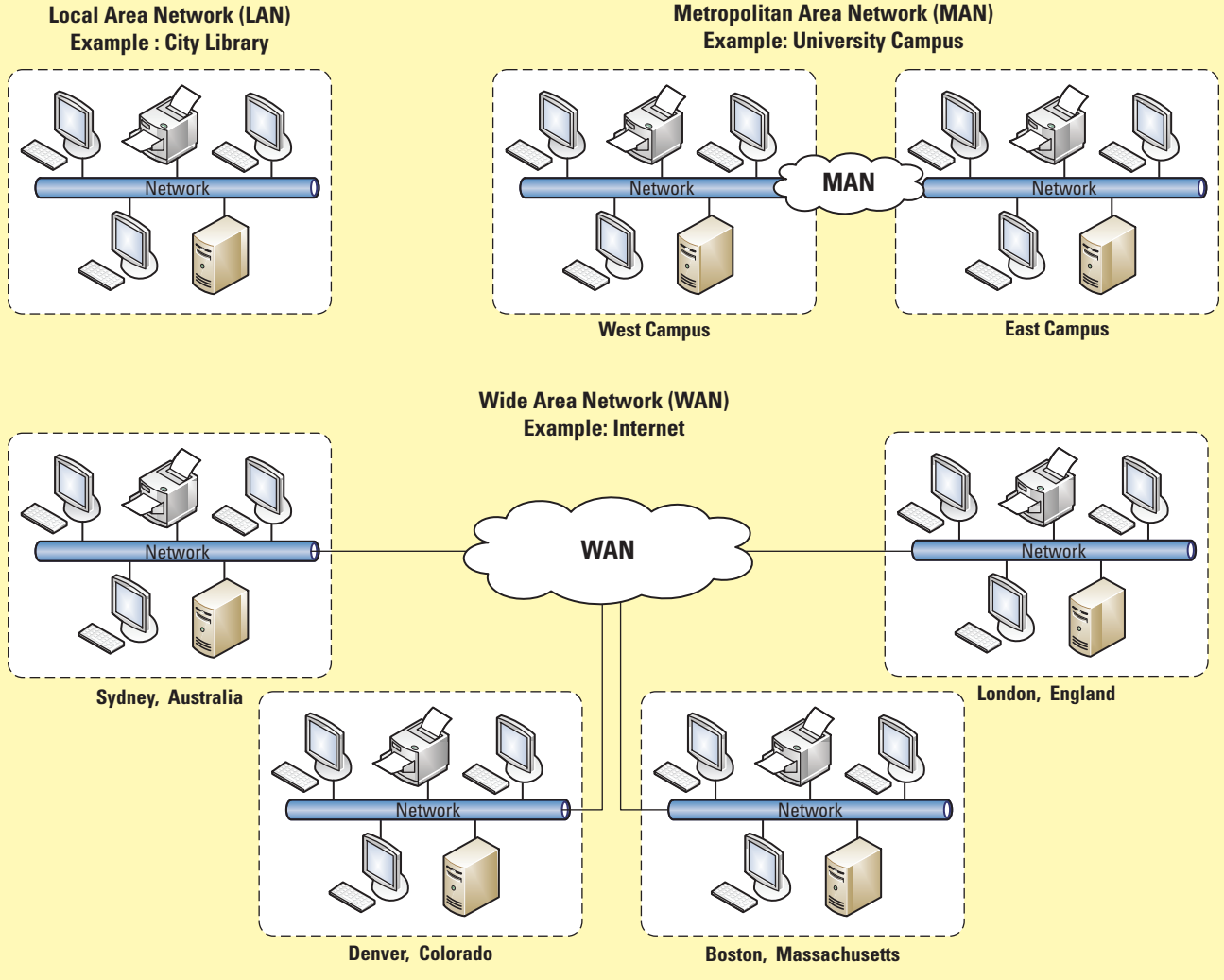
Networks are differentiated by the following:

- Architecture—peer-to-peer, client/server.
- Topology—bus, star, ring, hybrid, wireless.
- Protocols—Ethernet, transmission control protocol/Internet protocol (TCP/IP).
- Media—coaxial, twisted-pair, fiber-optic.

figure B.1
Network Types

Network Types	
Local area network (LAN)	Designed to connect a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games, or other applications. A LAN in turn often connects to other LANs, and to the Internet or wide area networks.
Wide area network (WAN)	Spans a large geographic area, such as a state, province, or country. WANs often connect multiple smaller networks, such as local area networks (LANs) or metropolitan area networks (MANs).
Metropolitan area network (MAN)	A large computer network usually spanning a city. Most colleges, universities, and large companies that span a campus use an infrastructure supported by a MAN.

figure B.2 LAN, WAN, and MAN



Architecture

The two primary types of network architectures are peer-to-peer networks and client/server networks.

PEER-TO-PEER NETWORKS

A ***peer-to-peer network (P2P)*** is a computer network that relies on the computing power and bandwidth of the participants in the network rather than a centralized server, as illustrated in Figure B.3. Each networked computer can allow other computers to access its files and use connected printers while it is in use as a workstation without the aid of a server.

While Napster may be the most widely known example of a P2P implementation, it may also be one of the most narrowly focused since the Napster model takes advantage of only one of the many capabilities of P2P computing: file sharing. The technology has far broader capabilities, including the sharing of processing, memory, and storage, and the supporting of collaboration among vast numbers of distributed computers such as grid computing described in Chapter 5. Peer-to-peer computing enables immediate interaction among people and computer systems.[1]

CLIENT/SERVER NETWORKS

A ***client*** is a computer designed to request information from a server. A ***server*** is a computer dedicated to providing information in response to requests. A ***client/server network*** is a model for applications in which the bulk of the back-end processing, such as performing a physical search of a database, takes place on a server, while the front-end processing, which involves communicating with the users, is handled by the clients (see Figure B.4). A ***network operating system (NOS)*** is the operating system that runs a network, steering information between computers and managing security and users. The client/server model has become one of the central ideas of network computing. Most business applications written today use the client/server model.

A fundamental part of client/server architecture is packet-switching. ***Packet-switching*** occurs when the sending computer divides a message into a number of efficiently sized units of data called packets, each of which contains the address of the destination computer. Each packet is sent on the network and intercepted by routers. A ***router*** is an intelligent connecting device that examines each packet of data it receives and then decides which way to send it onward toward its destination. The packets arrive at their intended destination, although some may have actually traveled by different physical paths, and the receiving computer assembles the packets and delivers the message to the appropriate application.

figure B.3
Peer-to-Peer Networks

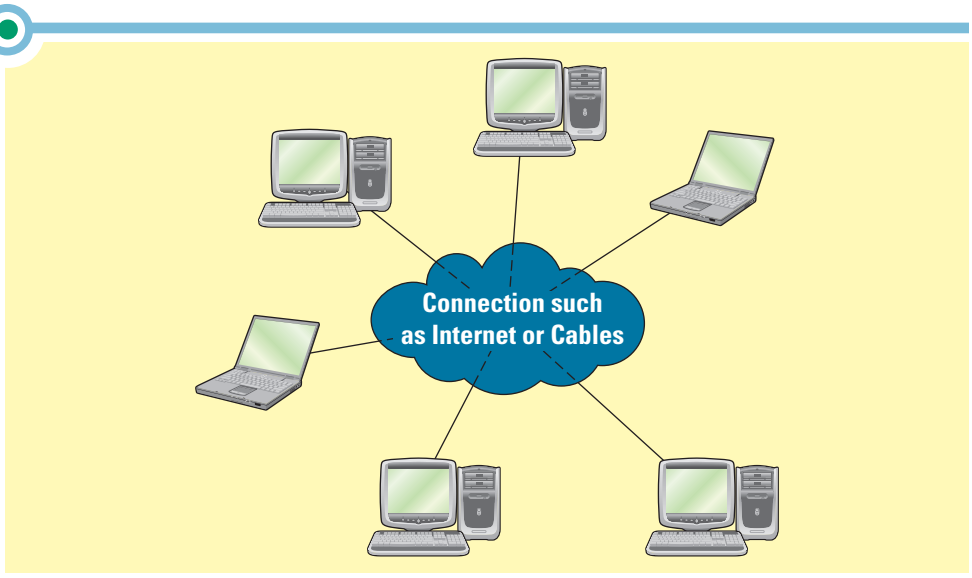
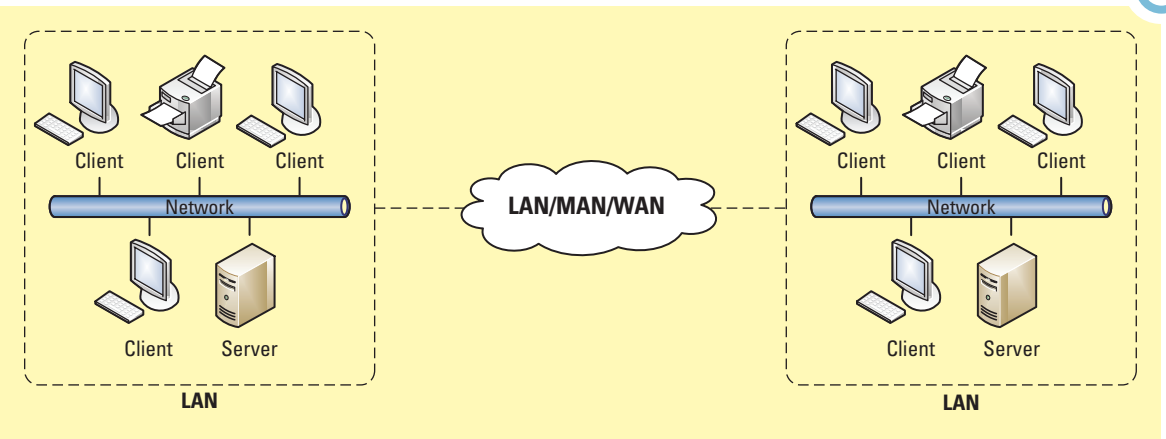


figure B.4 Client/Server Network



Topology

Networks are assembled according to certain rules. Cables, for example, have to be a certain length; each cable strand can support only a certain amount of network traffic. A ***network topology*** refers to the geometric arrangement of the actual physical organization of the computers (and other network devices) in a network. Topologies vary depending on cost and functionality. Figure B.5 highlights the five common topologies used in networks, and Figure B.6 displays each topology.

Protocols

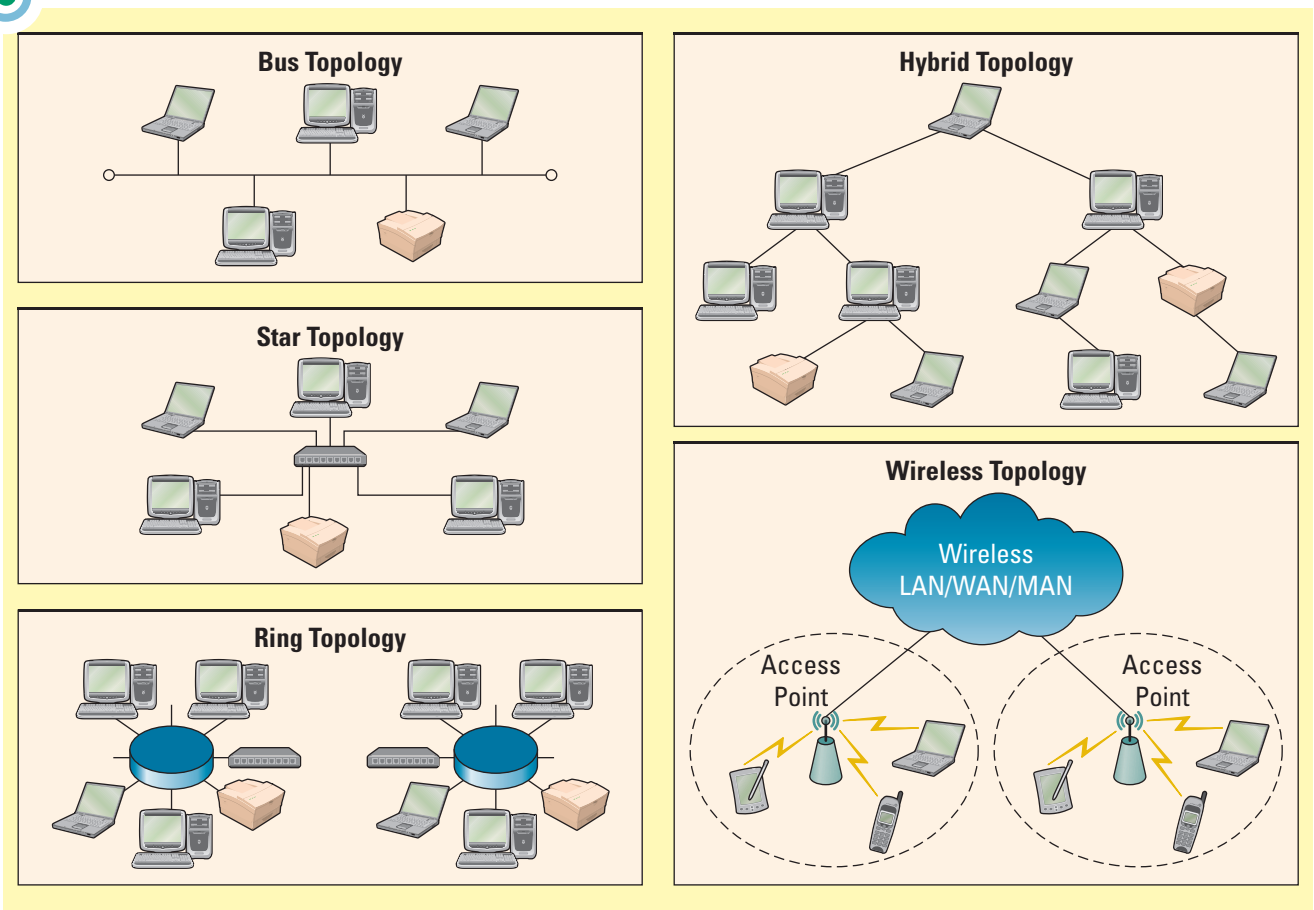
A ***protocol*** is a standard that specifies the format of data as well as the rules to be followed during transmission. Simply put, for one computer (or computer program) to talk to another computer (or computer program) they must both be talking the same language, and this language is called a protocol.

A protocol is based on an agreed-upon and established standard, and this way all manufacturers of hardware and software that are using the protocol do so in a similar fashion to allow for interoperability. ***Interoperability*** is the capability of two or more computer systems to share data and resources, even though they are made by different

figure B.5
Five Network Topologies

Network Topologies	
Bus	All devices are connected to a central cable, called the bus or backbone. Bus networks are relatively inexpensive and easy to install for small networks.
Star	All devices are connected to a central device, called a hub. Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through a hub.
Ring	All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. Ring topologies are relatively expensive and difficult to install, but they offer high speed and can span large distances.
Hybrid	Groups of star-configured workstations are connected to a linear bus backbone cable, combining the characteristics of the bus and star topologies.
Wireless	Devices are connected by signals between access points and wireless transmitters within a limited range.

figure B.6 Network Topologies



manufacturers. The most popular network protocols used are Ethernet and transmission control protocol/Internet protocol (TCP/IP).

ETHERNET

Ethernet is a physical and data layer technology for LAN networking (see Figure B.7). Ethernet is the most widely installed LAN access method, originally developed by Xerox and then developed further by Xerox, Digital Equipment Corporation, and Intel. When it first began to be widely deployed in the 1980s, Ethernet supported a maximum theoretical data transfer rate of 10 megabits per second (Mbps). More recently, Fast Ethernet has extended traditional Ethernet technology to 100 Mbps peak, and Gigabit Ethernet technology extends performance up to 1,000 Mbps.

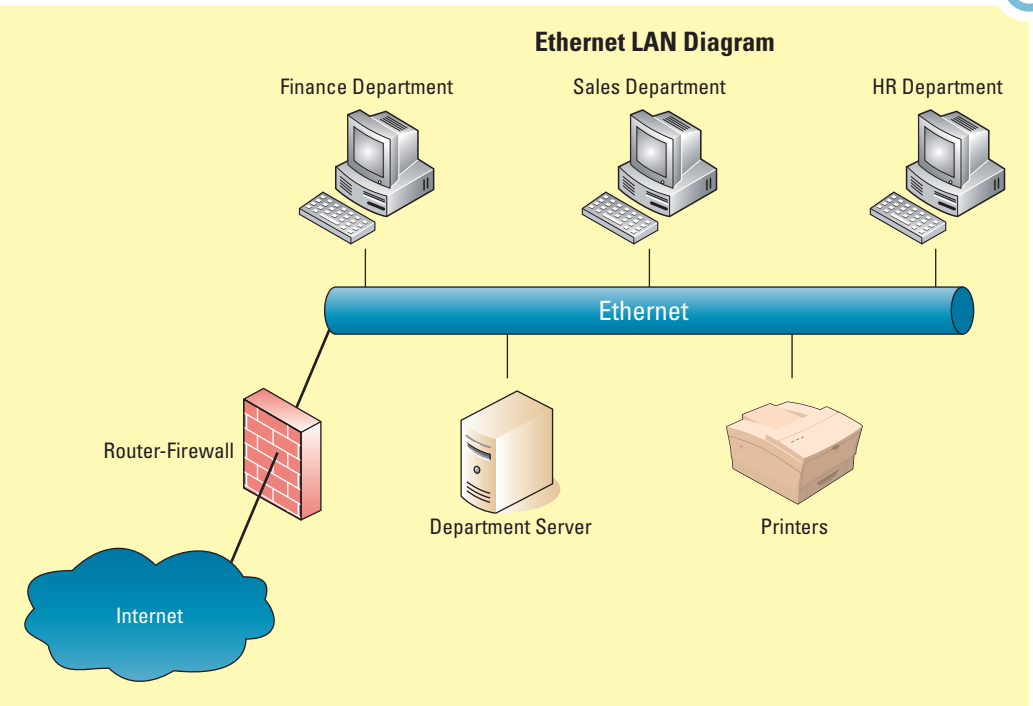
Ethernet is one of the most popular LAN technologies for the following reasons:

- Is easy to implement, manage, and maintain.
- Allows low-cost network implementations.
- Provides extensive flexibility for network installation.
- Guarantees interoperability of standards-compliant products, regardless of manufacturer.[2]

TRANSMISSION CONTROL PROTOCOL/ INTERNET PROTOCOL

The most common telecommunication protocol is transmission control protocol/ Internet protocol (TCP/IP), which was originally developed by the Department of Defense to connect a system of computer networks that became known as the Internet.

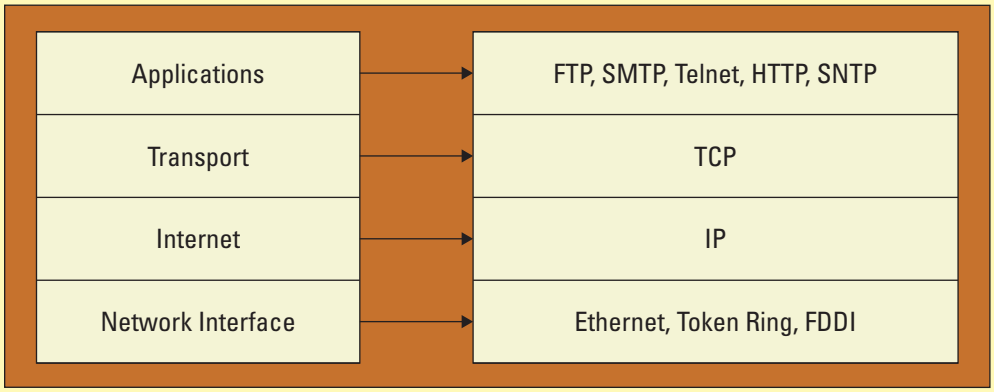
figure B.7 Ethernet Protocols



Transmission control protocol/Internet protocol (TCP/IP) provides the technical foundation for the public Internet as well as for large numbers of private networks. The key achievement of TCP/IP is its flexibility with respect to lower-level protocols. TCP/IP uses a special transmission method that maximizes data transfer and automatically adjusts to slower devices and other delays encountered on a network. Although more than 100 protocols make up the entire TCP/IP protocol suite, the two most important of these are TCP and IP. **TCP** provides transport functions, ensuring, among other things, that the amount of data received is the same as the amount transmitted. **IP** provides the addressing and routing mechanism that acts as a postmaster. Figure B.8 displays TCP/IP's four-layer reference model:

- Application layer—serves as the window for users and application processes to access network services.
- Transport layer—handles end-to-end packet transportation.

figure B.8 TCP/IP Four-Layer Reference Model



- Internet layer—formats the data into packets, adds a header containing the packet sequence and the address of the receiving device, and specifies the services required from the network.
- Network interface layer—places data packets on the network for transmission.[3]

For a computer to communicate with other computers and Web servers on the Internet, it must have a unique numeric IP address. IP provides the addressing and routing mechanism that acts as a postmaster. An IP address is a unique 32-bit number that identifies the location of a computer on a network. It works like a street address—as a way to find out exactly where to deliver information.

When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have 4,294,967,296 unique addresses. The actual number of available addresses is smaller (somewhere between 3.2 and 3.3 billion) due to the way that the addresses are separated into classes, and some addresses are set aside for multicasting, testing, or other special uses.[4]

With the explosion of the Internet and the increase in home networks and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the address format to allow for more possible addresses. ***Internet protocol version 6 (IPv6)*** is the "next generation" protocol designed to replace the current version Internet protocol, IP version 4 (IPv4). However, IPv6 will take several years to implement because it requires modification of the entire infrastructure of the Internet. The main change brought by IPv6 is a much larger address space that allows greater flexibility in assigning addresses. IPv6 uses a 128-bit addressing scheme that produces 3.4×10^{38} addresses.[5]

The TCP/IP suite of applications includes five protocols—file transfer, simple mail transfer, telnet, hypertext transfer, and simple network management (see Figures B.9 and B.10).[6]

figure B.9
TCP/IP Applications

TCP/IP Applications	
File Transfer Protocol (FTP)	Allows files containing text, programs, graphics, numerical data, and so on to be downloaded off or uploaded onto a network.
Simple Mail Transfer Protocol (SMTP)	TCP/IP's own messaging system for email.
Telnet Protocol	Provides terminal emulation that allows a personal computer or workstation to act as a terminal, or access device, for a server.
Hypertext Transfer Protocol (HTTP)	Allows Web browsers and servers to send and receive Web pages.
Simple Network Management Protocol (SNMP)	Allows the management of networked nodes to be managed from a single point.

figure B.10
Open System Interconnection Model

OSI Model
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Media

Network transmission media refers to the various types of media used to carry the signal between computers. When information is sent across the network, it is converted into electrical signals. These signals are generated as electromagnetic waves (analog signaling) or as a sequence of voltage pulses (digital signaling). To be sent from one location to another, a signal must travel along a physical path. The physical path that is used to carry a signal between a signal transmitter and a signal receiver is called the transmission media. The two types of transmission media are wire (guided) and wireless (unguided).

WIRE MEDIA

Wire media are transmission material manufactured so that signals will be confined to a narrow path and will behave predictably. The three most commonly used types of guided media are (see Figure B.11):

- Twisted-pair cable
- Coaxial cable
- Fiber-optic cable

Twisted-Pair Cable ***Twisted-pair cable*** refers to a type of cable composed of four (or more) copper wires twisted around each other within a plastic sheath. The wires are twisted to reduce outside electrical interference. Twisted-pair cables come in shielded and unshielded varieties. Shielded cables have a metal shield encasing the wires that acts as a ground for electromagnetic interference. Unshielded twisted-pair (UTP) is the most popular and is generally the best option for LAN networks. The quality of UTP may vary from telephone-grade wire to high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The connectors (called RF-45) on twisted-pair cables resemble large telephone connectors.[7]

Coaxial Cable ***Coaxial cable*** is cable that can carry a wide range of frequencies with low signal loss. It consists of a metallic shield with a single wire placed along the center of a shield and isolated from the shield by an insulator. Coaxial cable is similar to that used for cable television. This type of cable is referred to as coaxial because it contains one copper wire (or physical data channel) that carries the signal and is surrounded by another concentric physical channel consisting of a wire mesh. The outer channel serves as a ground for electrical interference. Because of this grounding feature, several coaxial cables can be placed within a single conduit or sheath without significant loss of data integrity.[8]

Fiber-Optic Cable ***Fiber optic*** (or ***optical fiber***) refers to the technology associated with the transmission of information as light impulses along a glass wire or fiber. Fiber-optic cable is the same type used by most telephone companies for long-distance service. Fiber-optic cable can transmit data over long distances with little loss in data integrity. In addition, because data are transferred as a pulse of light, fiber optical is not subject to interference. The light pulses travel through a glass wire or fiber encased in an insulating sheath.[9]

Fiber optic's increased maximum effective distance comes at a price. Optical fiber is more fragile than wire, difficult to split, and labor intensive to install. For these reasons, fiber optics is used primarily to transmit data over extended distances where the hardware required to relay the data signal on less expensive media would exceed the cost of fiber-optic installation. It is also used where large amounts of data need to be transmitted on a regular basis.

WIRELESS MEDIA

Wireless media are natural parts of the Earth's environment that can be used as physical paths to carry electrical signals. The atmosphere and outer space are examples of wireless media that are commonly used to carry these signals. Today, technologies for

figure B.11 Twisted-Pair, Coaxial Cable, and Fiber-Optic

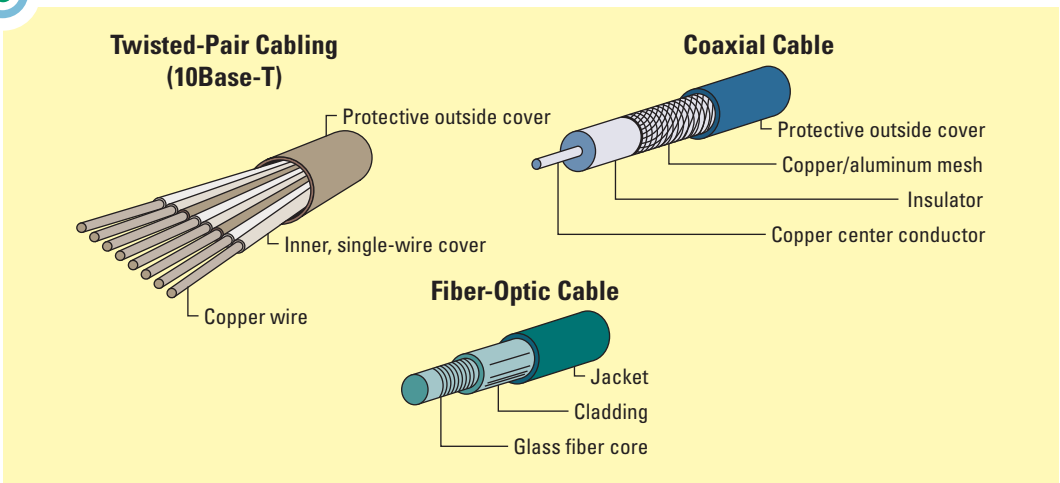
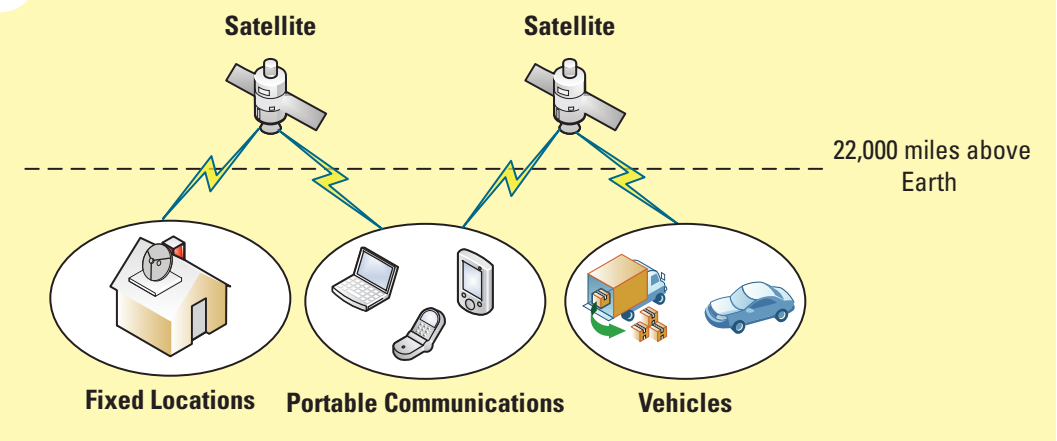


figure B.12 Communication Satellite Example



wireless data transmission include microwave transmission, communication satellites, (see Figure B.12) mobile phones, personal digital assistants (PDAs), personal computers (e.g., laptops), and mobile data networks.

Network signals are transmitted through all media as a type of waveform. When transmitted through wire and cable, the signal is an electrical waveform. When transmitted through fiber-optic cable, the signal is a light wave, either visible or infrared light. When transmitted through the Earth's atmosphere, the signal can take the form of waves in the radio spectrum, including microwaves, infrared, or visible light.

Key Terms

Client B.4
Client/server network B.4
Coaxial cable B.9
Ethernet B.6
Fiber optic (or optical fiber) B.9
Internet protocol version 6 (IPv6) B.8
Interoperability B.5
Local area network (LAN) B.2
Metropolitan area network (MAN) B.2
Network B.1
Network operating system (NOS) B.4
Network topology B.5
Network transmission media B.9
Packet-switching B.4
Peer-to-peer (P2P) network B.4
Protocol B.5
Router B.4
Server B.4
Telecommunication system B.1
Transmission control protocol/Internet protocol (TCP/IP) B.7
Twisted-pair cable B.9
Wide area network (WAN) B.2
Wire media B.9
Wireless media B.9

Apply Your Knowledge

1. Network Analysis

Global Manufacturing is considering a new technology application. The company wants to process orders in a central location and then assign production to different plants. Each plant will operate its own production scheduling and control system. Data on work in process and completed assemblies will be transmitted back to the central location that processes orders. At each plant, Global uses personal computers that perform routine tasks such as payroll and accounting. The production scheduling and control systems will be a package program running on a new computer dedicated to this application.

The MIS personnel at Global have retained you as a consultant to help with further analysis. What kind of network configuration seems most appropriate? How much bandwidth is needed? What data should be collected? Prepare a plan showing the information Global must develop to establish this network system. Should Global use a private network or can it accomplish its objectives through the Internet?

2. Secure Access

Organizations that have traditionally maintained private, closed systems have begun to look at the potential of the Internet as a ready-made network resource. The Internet is inexpensive and globally pervasive: Every phone jack is a potential connection. However, the Internet lacks security. What obstacles must organizations overcome to allow secure network connections?

3. Telecommunications Options

Research the telecommunications options that currently exist for you to link to the Internet from where you live. Prepare a list of criteria on which to compare the different technologies, such as price (is there tiered pricing depending on speed and amount you can download?), start-up cost (do you need to buy a special modem, or is there an installation fee), maximum data transfer rate, and so on. Compare your responses with several classmates, and then develop a summary of all telecommunications options that you identified, including the criteria and your group comparison based on the criteria.

4. Frying Your Brains?

Radio waves, microwaves, and infrared all belong to the electromagnetic radiation spectrum used. These terms reference ranges of radiation frequencies we use every day in our wireless networking environments. However, the very word *radiation* strikes fear in many people. Cell towers have sprouted from fields all along highways. Tall rooftops harbor many more cell stations in cities. Millions of cell phone users place microwave transmitters/receivers next to their heads each time they make a call. With all this radiation zapping around, should we be concerned? Research the Internet to find out what the World Health Organization (WHO) has had to say about this.

5. Home Network Experience

If you maintain a home computer network (or have set one up in the past), create a document that describes the benefits that the network provides along with the difficulties that you have experienced. Include in your document a network topology, a detailed description of the type of network you have and the equipment you use. If you have no experience with home networking, interview someone who does, and write up his or her comments. Compare this with several classmates, and discuss the benefits and challenges.

6. The Internet Is Almost Full

IPv4 has given us a little more than 4 billion possible IP addresses. Although 4 billion may sound like a lot, the number of devices connecting to the Internet is exploding! Internet access is now built into smart phones, tablets, televisions, DVD players, video game consoles, utility meters, thermostats, appliances, and more. There is another problem—large masses of existing addresses were not allocated efficiently, and these cannot be easily reclaimed from the corporations, universities, and other organizations that initially received them. This means that we are running out of IP addresses.

Research the Internet to identify just when IPv6 will roll out. Who is leading the charge for IPv6 roll-out? What are the main issues for deploying IPv6? Is it backward-compatible with IPv4?