Networks and Telecommunications Basics

A

Introduction

Change is everywhere in the information technology domain, but nowhere is change more evident and more dramatic than the realm of telecommunications and networking. Most 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 networked systems 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, data exchange, and resource-sharing system created by linking two or more computers and establishing standards, or protocols, so that they can work together. 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 with more than 350 million host computers in over 200 countries around the world. Telecommunication systems and networks are traditionally complicated and historically inefficient. However, businesses can benefit from today's modern network infrastructures that provide reliable global reach to employees and customers. Businesses around the world are moving to network infrastructure solutions that allow greater choice in how they go to market—solutions with global reach. These alternatives include wireless, voice-over internet protocol (VoIP), and radio-frequency identification (RFID). This appendix takes a detailed look at key telecommunication, network, and wireless technologies being integrated into businesses around the world.

LEARNING OUTCOMES

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

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

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

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

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

A.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. Music is the hot product line at coffee retailer Starbucks. In Starbucks stores, customers can shop for music wirelessly through iTunes free, thanks to the company's own increasingly sophisticated in-store network.

Today's corporate digital networks include a combination of local area networks and the Internet. 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 A.1 highlights the three different types of networks, and Figure A.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 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 e-commerce (now referred to as e-business) 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 A.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.

figure A.2

LAN, WAN, and MAN

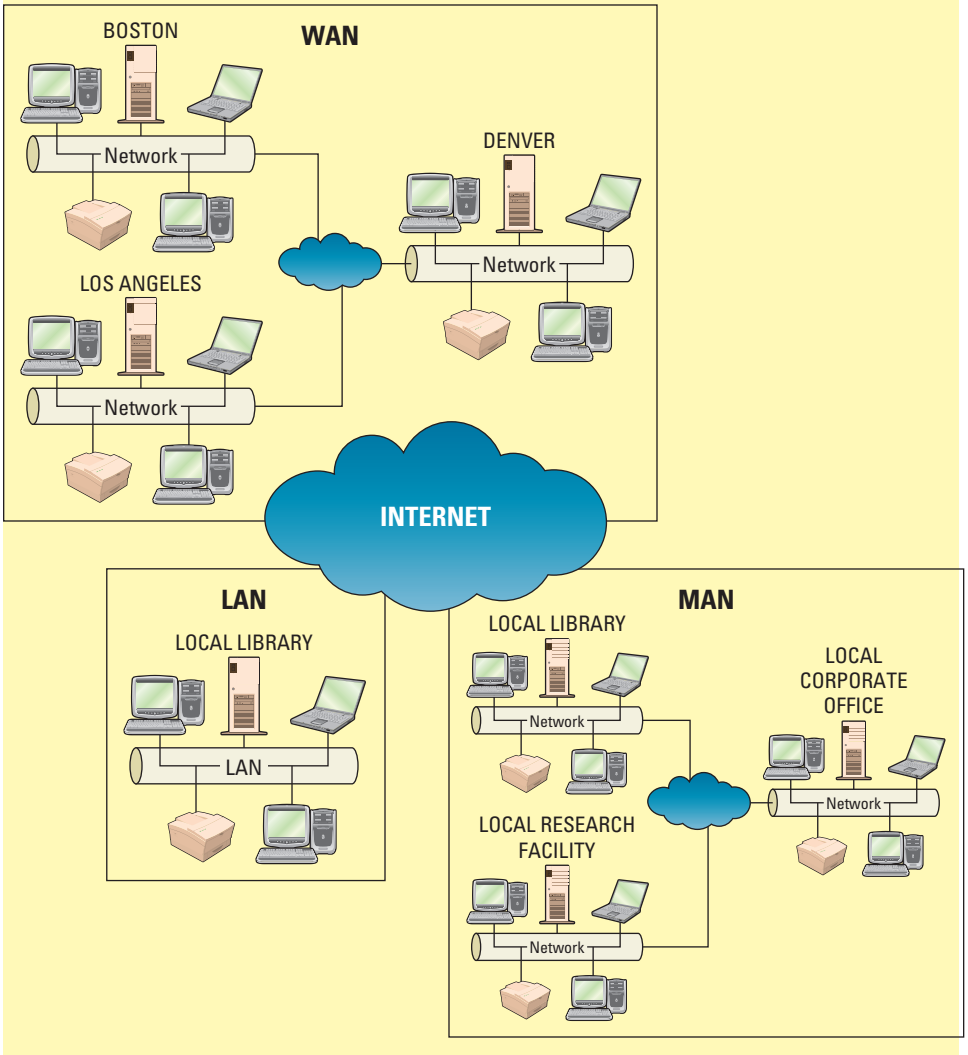
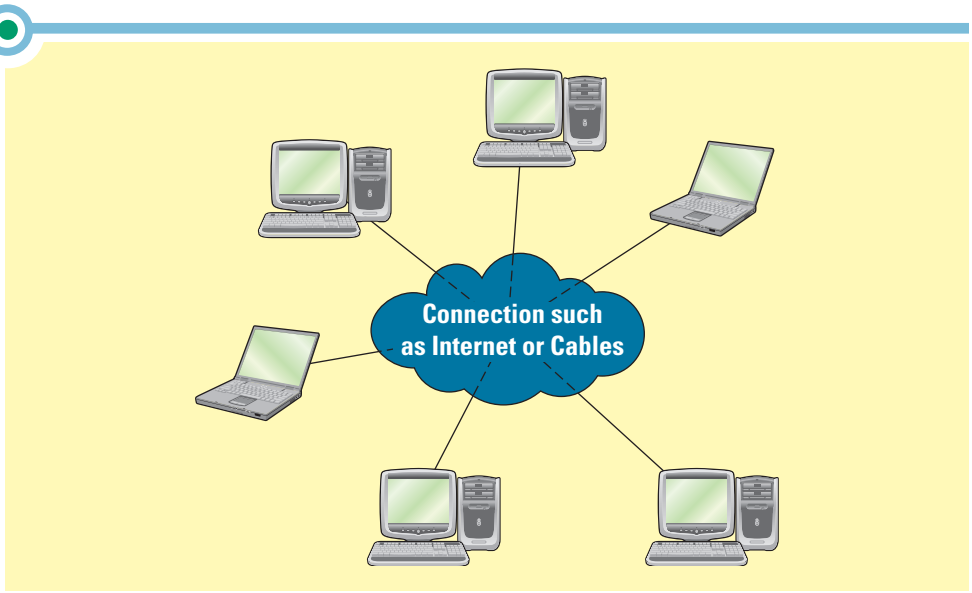


figure A.3
Peer-to-Peer (P2P) Networks



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 (P2P) network*** is any network without a central file server and in which all computers in the network have access to the public files located on all other workstations, as illustrated in Figure A.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.

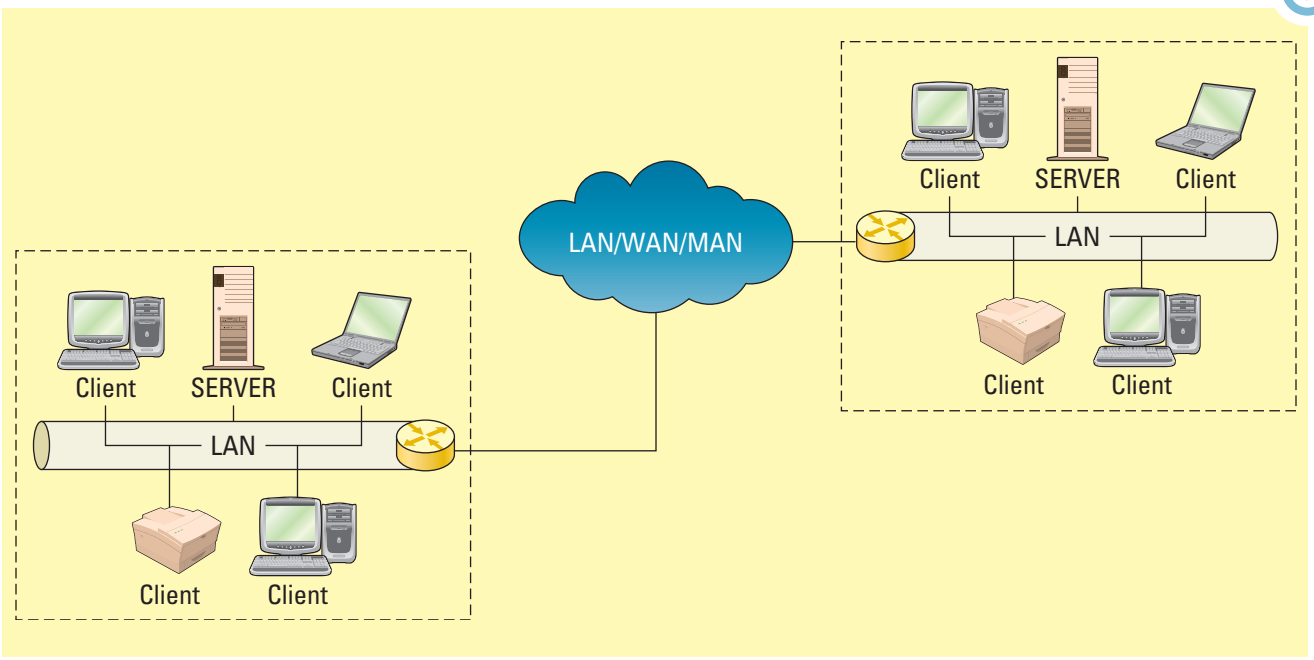
While Napster may be the most widely known example of a P2P implementation, it may also be one of the most narrowly focused since the Napster model takes advantage of only one of the many capabilities of P2P computing: file sharing. The technology has far broader capabilities, including the sharing of processing, memory, and storage, and the supporting of collaboration among vast numbers of distributed computers such as grid computing described in Chapter 11. Peer-to-peer computing enables immediate interaction among people and computer systems.[1]

CLIENT/SERVER NETWORKS

A ***client*** is a computer that is designed to request information from a server. A ***server*** is a computer that is dedicated to providing information in response to external 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 A.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.

Federal Express (FedEx) is the world's largest express transportation company, providing fast and reliable services for important documents, packages and freight. The company delivers more than 2.3 million items in 192 countries each working day. It employs more than 108,000 people, operates 478 aircraft and more than 35,000 vehicles in its integrated system. It also happens to have one of the world's

figure A.4 Client/Server Network



largest client/server-based imaging systems. The system is designed to scan, recognize, and store images of nearly 1,000,000 airbills each day at FedEx's Memphis headquarters before transmitting them to several remote data entry service providers located throughout the United States. The data entry providers then convert the images into keyed data used for customer invoicing. In the past the paper airbills were delivered overnight to the vendors for data conversion. The new system improves FedEx's invoicing process by reducing keystrokes, eliminating paper handling, and increasing workers' productivity.

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.

Eva Chen, CIO at Trend Micro, built a router that helps prevent worms and viruses from entering networks. The problem with most existing antivirus software is that it starts working after a destructive sequence of code is identified, meaning it starts doing its job only after the virus or worm has been unleashed inside the network. Chen's router, the Network VirusWall, sits on the edge of a corporate network, scanning data packets and detaining those that might contain viruses or worms. Any suspicious packets are compared with up-to-the-second information from Trend Micro's virus-tracking command center. Viruses and worms are then deleted and refused entry to the network, allowing the company to perform a preemptive strike.[2]

Topology

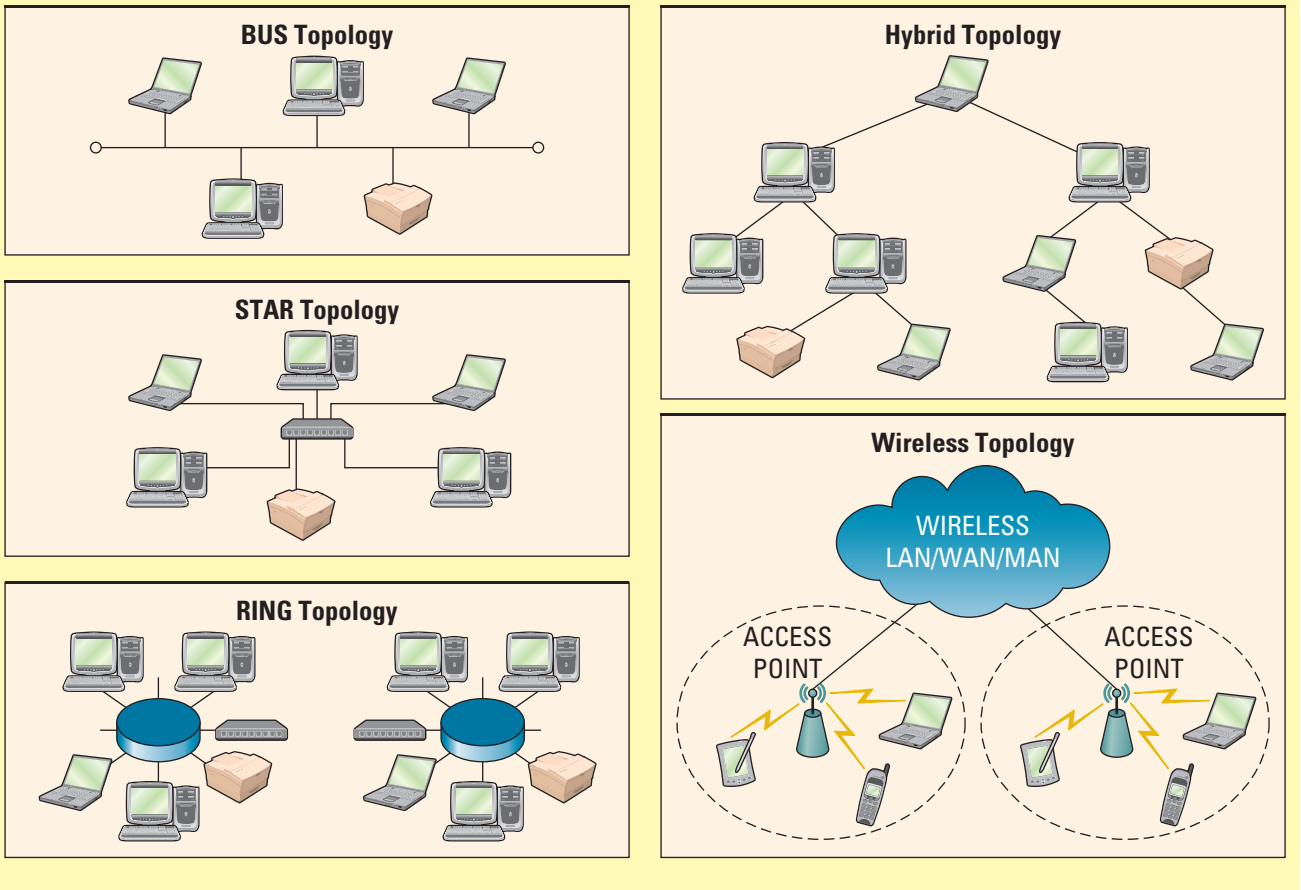
Networks are assembled according to certain rules. Cables, for example, have to be a certain length; each cable strand can support only a certain amount of network traffic. A ***network topology*** refers to the geometric arrangement of the actual

figure A.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 the 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 bandwidth 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 a receiver/transmitter to a special network interface card that transmits signals between a computer and a server, all within an acceptable transmission range.

figure A.6 Network Topologies



physical organization of the computers (and other network devices) in a network. Topologies vary depending on cost and functionality. Figure A.5 highlights the five common topologies used in networks, and Figure A.6 displays each topology.[3]

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 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 A.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 has survived as the major LAN technology—it is currently used for approximately 85 percent of the world's LAN-connected PCs and workstations due to the following characteristics:

- Is easy to understand, implement, manage, and maintain.
- Allows low-cost network implementations.
- Provides extensive flexibility for network installation.
- Guarantees successful interconnection and operation of standards-compliant products, regardless of manufacturer.

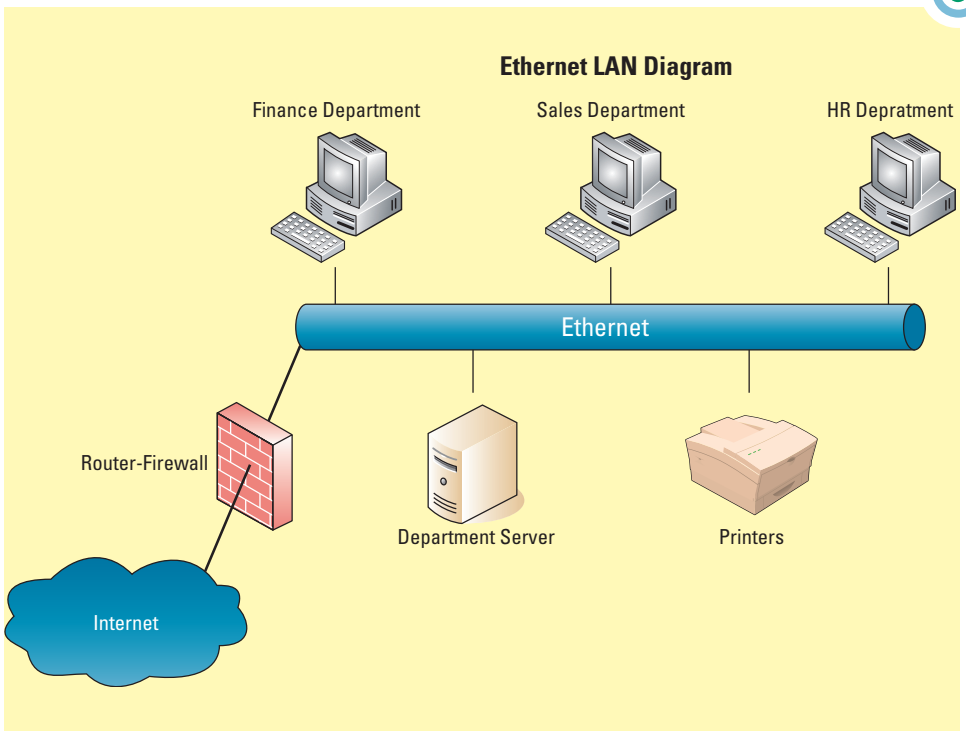
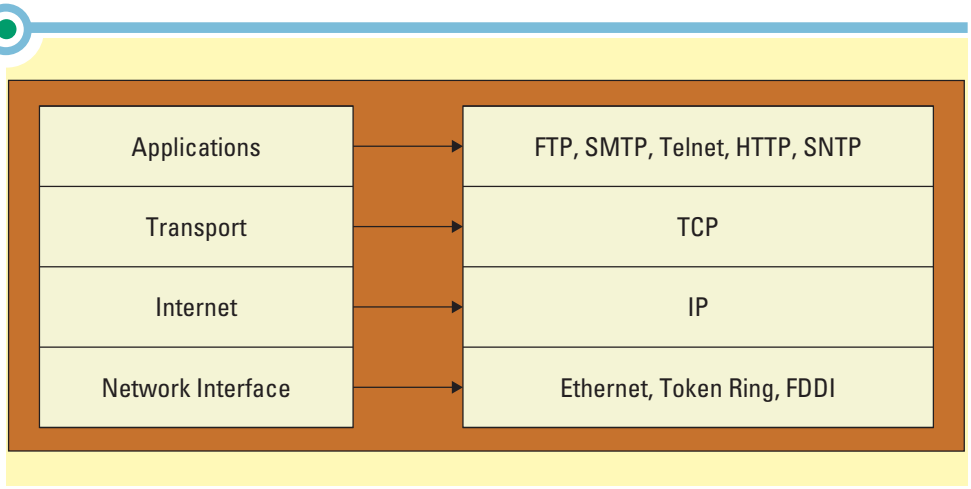


figure A.7
Ethernet Protocols

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



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. ***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 A.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.
- 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.

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.

figure A.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 personalcomputer 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 A.10
Open System Interconnection Model

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

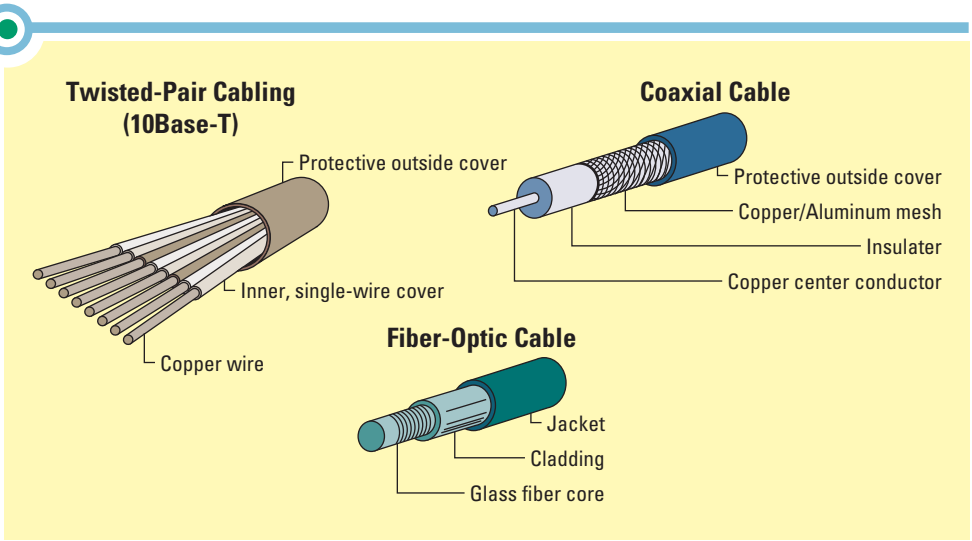
With the explosion of the Internet and the increase in home networks and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the address format to allow for more possible addresses. ***Internet Protocol version 6 (IPv6)*** is the "next generation" 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.

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

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).

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



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 A.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.

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.

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. The 10Base-FL and 100Base-FX fiber optic cable are the same types of cable 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.

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 signals. Today, common technologies for wireless data transmission include microwave transmission, communication satellites, pagers, cellular telephones and personal communication services (PCS), personal digital assistants (PDAs), smart phones, 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.

Recent advances in radio hardware technology have produced significant advancements in wireless networking devices: the cellular telephone, wireless modems, and wireless LANs. These devices use technology that in some cases has been around for decades but until recently was too impractical or expensive for widespread use.[4]

Retailer REI reports that one-third of all customers who buy online and pick up at the store make another purchase while there, with a spending average of $90. From a technology perspective, in-store pick up needs to have some level of inventory integration to work effectively. The integration of data is critical in being able to display to the consumer the availability of products at their closest geographic store.

Key Terms

Client A.4
Client/server network A.4
Coaxial cable A.10
Ethernet A.7
Fiber optic (or optical fiber) A.10
Internet protocol version 6 (IPv6) A.9
Interoperability A.7
Local area network (LAN) A.2
Metropolitan area network (MAN) A.2
Network A.1
Network operating system (NOS) A.4
Network topology A.5
Network transmission media A.9
Packet-switching A.5
Peer-to-peer (P2P) network A.4
Protocol A.2, A.7
Router A.5
Server A.4
Telecommunication system A.1
Transmission Control Protocol/Internet Protocol (TCP/IP) A.8
Twisted-pair cable A.10
Wide area network (WAN) A.2
Wire media A.10
Wireless media A.11

Making Business Decisions

1. Wireless fitness

Sandifer's Fitness Club is located in beautiful South Carolina. Rosie Sandifer has owned and operated the club for 20 years. The club has three outdoor pools, two indoor pools, 10 racquetball courts, 10 tennis courts, an indoor and outdoor track, along with a four-story exercise equipment and massage therapy building. Rosie has hired you as a summer intern specializing in information technology. The extent of Rosie's current technology includes a few PCs in the accounting department and two PCs with Internet access for the rest of the staff. Your first assignment is to create a report detailing networks

and wireless technologies. The report should explain how the club could gain a business advantage by implementing a wireless network. If Rosie likes your report, she will hire you as the full-time employee in charge of information technology. Be sure to include all of the different uses for wireless devices the club could implement to improve its operations.

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. Integrating wireless worlds

Tele-Messaging is a next-generation integrated Internet and wireless messaging service that offers services to ISPs, telecommunications carriers, and portal companies. According to Tele-Messaging's research, the primary reason that 90 percent of the people go online is for email. However, the challenge for Tele-Messaging is how to successfully attract and retain these customers. Customers want more than free calls to sign up and are looking for a host of additional services with whiz-bang technology to give them the information they want, when they want it, anywhere, and in the method most convenient to them. List the infrastructures needed to deliver the technology with the necessary reliability, availability, and scalability demanded by Tele-Messaging's customers.

4. Communicating with instant messages

You are working for a new start-up magazine, *Jabber Inc.,* developed for information professionals that provides articles, product reviews, case studies, evaluation, and informed opinions. You need to collaborate on news items and projects, and exchange data with a variety of colleagues inside and outside the *Jabber Inc.* walls. You know that many companies are now embracing the instant messaging technology. Prepare a brief report for the CIO that will explain the reasons IM is not just a teenage fad, but also a valuable communications tool that is central to everyday business.

Notes

1. Timothy Mullaney and Arlene Weintraub, "The Digital Hospital," *BusinessWeek,* March 28, 2005, and Michelle Delio, "How Secure Is Digital Hospital," *Wired,* March 28, 2001.
2. Eva Chen, "Shop Talk," *CIO Magazine,* October 15, 2004.
3. www.perrio.com, accessed November 2005.
4. Chris Murphy, "RIM Settles BlackBerry Suit," *InformationWeek,* March 6, 2006.