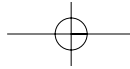


CHAPTER 2

Communications Networks

After reading this chapter you will be able to:

- Understand the benefits of networking
- Understand what telephony networking is
- Identify the layers of the OSI reference model and know what part each one plays in networking
- Discuss how the Internet communicates
- Understand the basics of ATM networks
- Apply knowledge of different networking components
- Explain how network topologies influence planning decisions



In today's complex world, most companies have networks. In fact, most companies have a Web presence as well. A network can range from simply two computers that are linked together to the complexity of computers that can access data across continents. Networks are used to improve communication between departments, foster customer relationships, and share data throughout the world.

As a network administrator, it is your job to manage the network. To do this, you must understand the fundamental networking principles. Having this knowledge will help develop your planning and troubleshooting skills. This chapter provides you with those fundamental principles on which you will build knowledge and experience. It also focuses on the concept of a network, what makes it possible for devices to communicate, and what types of medium are used for communication.

2.1 Introducing Networking

A **network** is a group of computers that can communicate with each other to share information. This can range, in its simplest form, from two computers in a home that are connected by one cable to the most complex network that includes many computers, cables, and devices spanning across continents. Before we can explore larger complex networks, we must look at what allows computers to talk to each other.

When computers can communicate with each other, they can share **resources**. These resources can be data (such as documents or spreadsheets), applications (such as Microsoft Word or Microsoft Excel), or hardware (such as modems or printers). What if you want to share a file with a friend who lives down the street? Each of you has your own computer, and neither computer is hooked up to any other computer or the Internet. Each of the computers is considered a **stand-alone computer**. See Figure 2.1.

The two of you can share files by transferring them onto a floppy disk and loading them onto each computer. This is also known as a **sneakernet**. It stems from the fact that you have to physically walk the files on disk back and forth to transfer them. This was the primary method of file transfer before networks became popular. An example of a sneakernet is shown in Figure 2.2.

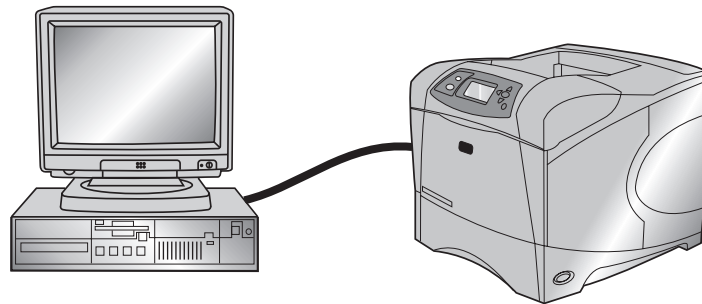


Figure 2.1
A stand-alone computer
attached to a printer

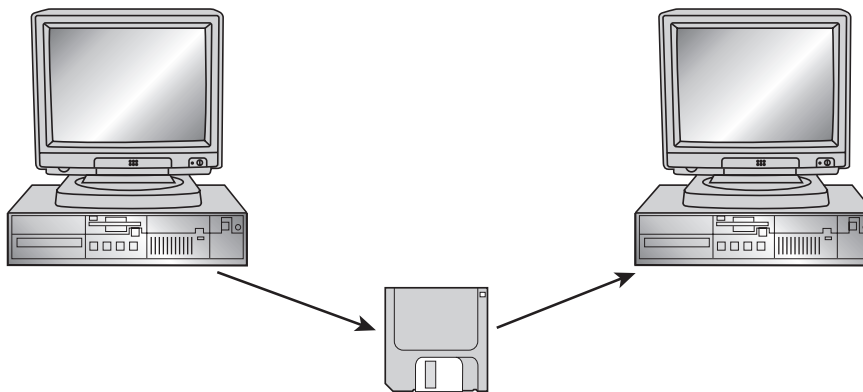


Figure 2.2
Sneakernet

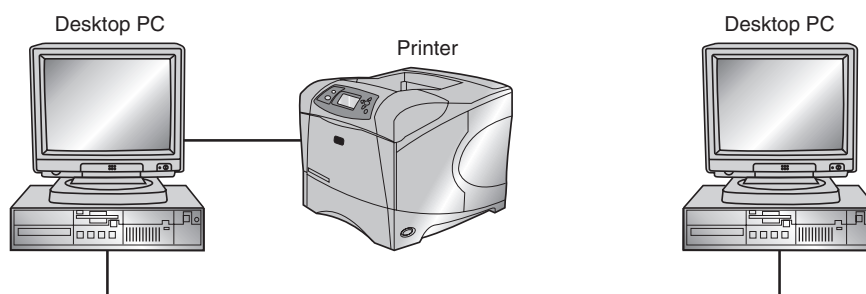


Figure 2.3
A simple network

You can connect two computers together with a cable, which results in a simple network. Figure 2.3 illustrates a simple network. In this example, two computers can share information and the same printer.

Before we discuss how computers can talk to each other, we will explore the different types of computers that make up a network. Many times you may hear administrators talk about servers and clients. What exactly are these?

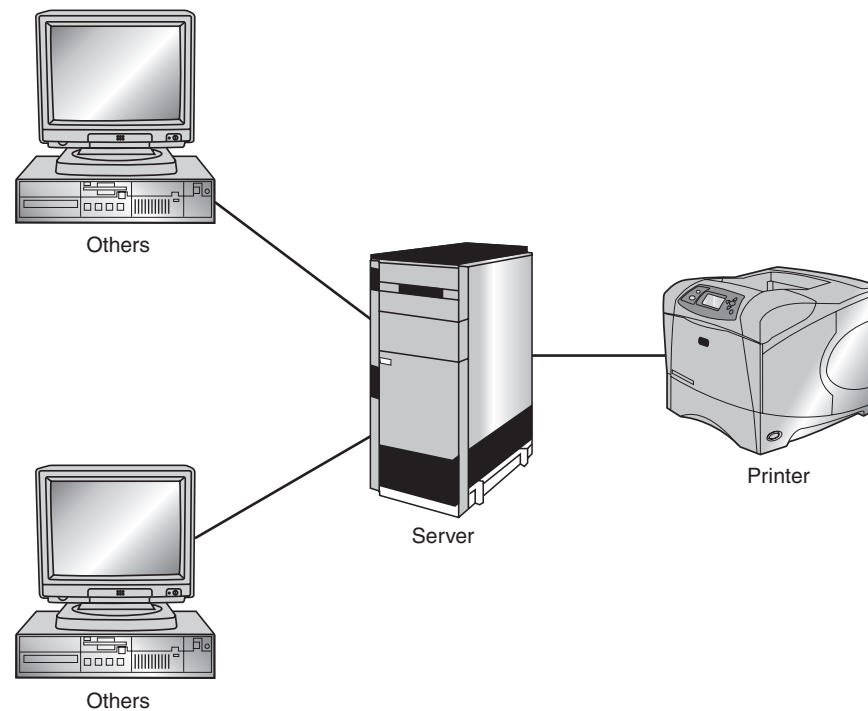


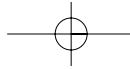
Figure 2.4
A server network

A **server** is a computer that allows its resources to be used by other computers on the network. A **client** is a computer that uses the resources of the server. Figure 2.4 depicts a network with a server and clients.

As we discussed earlier in this section, resources come in many different forms. Resources are the files, applications, and hardware shared by the server for the client to access. When a server provides a resource for a client to access, this is referred to as a *shared resource*. Shared resources are accessed across the network.

An important concept to remember is that of shared resources. Sharing allows for access across the network. If I share with you, you can use my resources by traversing the network. Shared resources will come into play further in Chapter 12 when the management of access and accounts is discussed.

Technology is advancing rapidly, and most networks tie into some type of telephone system, whether it is a single analog line used to connect a home computer to the Internet or a high-speed digital connection used in most businesses. In Chapter 1 we explained analog and digital signaling. Now



that we've introduced what a network is, it's time to look at how analog and digital signaling are used in the communication of a network.

2.2 Telephony Networks

The telecommunications (Telecom), or Private Branch Exchange (PBX), system is a vital part of an organization's infrastructure. A PBX is a telephone system within an organization that switches calls between users on local lines yet allows all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office. The PBX is owned and operated by the organization rather than the telephone company. Originally, private branch exchanges used analog technology, but most now use digital technology. Digital signals are converted to analog for outside calls on the local loop using plain old traditional telephone service. A PBX includes telephone trunk lines, a computer with memory that manages the calls, a network of lines within the PBX, and a console or switchboard. In essence, users of the PBX share a certain number of outside lines for making telephone calls. Most medium-sized or large companies use a PBX because it's much less expensive than connecting an external telephone line to every telephone in the organization. In addition, it's easier to call someone within a PBX because you simply dial a 3- or 4-digit extension. An example of this is a company with one published phone number yet the employees can answer up to five lines at a time. When a call comes in, the receptionist answers the phone and then transfers it to the requested party by dialing their 3-digit extension.

Not long ago the Internet ran on phone systems, but now many phone systems are running on the Internet. For years, companies carried data traffic on voice networks. During the mid-1990s, advances in technology made it possible to use existing network resources to reduce or eliminate telephony costs. Many companies have moved to **Voice over IP (VoIP)** to integrate computer telephony, videoconferencing, and document sharing. See Figure 2.5.

In analog connectivity, a **plain old telephone system (POTS)** is used. This is also referred to as a **public switched telephone network (PSTN)**. A modem converts the signals from digital to analog to be used over the phone lines and then back to digital for the computer to understand. For example, you and a friend install modems in your computers so that you

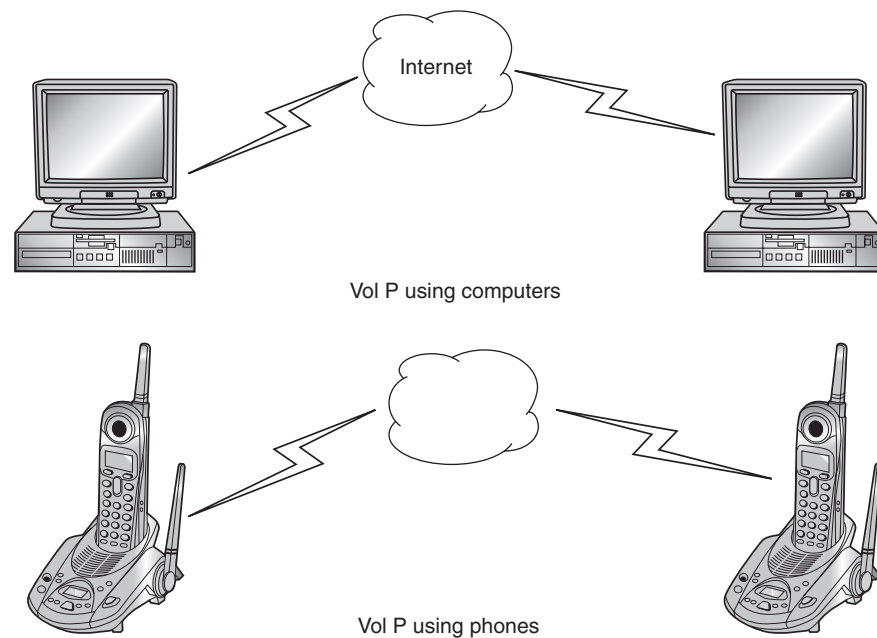


Figure 2.5
Voice over IP

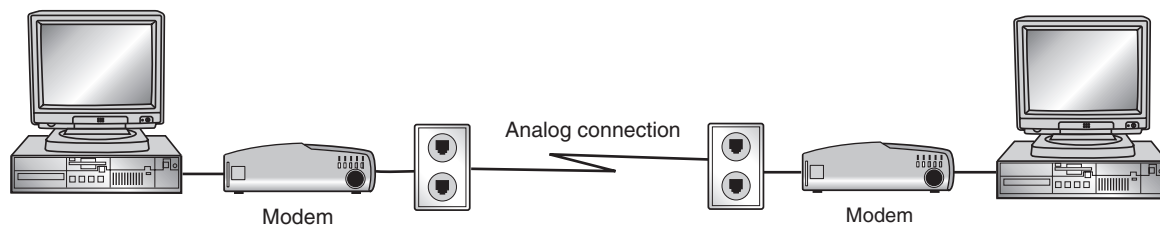


Figure 2.6
A PSTN connection between two computers

can share files without having to use the sneakernet method. You plug a phone line into each modem and use the PSTN to communicate between the computers. Each computer communicates in digital signals. The modem connected to your machine converts the digital signal to analog to travel from your house to your friend's house. Your friend's modem then converts the analog signal to digital for his computer to understand. Figure 2.6 shows an example of communication between modems.

Data networks are based on a technology called packet switching, whereas telephony networks use circuit switching. Because packet switching and

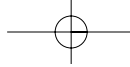
circuit switching and discussed in further detail in Chapter 5, we'll just go over some basics.

Here's how circuit switching works: When a call is made, a dedicated connection is opened and maintained between the parties for the duration of the call. No other calls can use those resources until the call is terminated. In contrast, packet switching does not require a dedicated circuit. Data packets are routed over any circuit that is available at any given point, and they don't travel over a fixed path. In other words, numerous users share the same circuit simultaneously because the circuits are available to all users.

A good example of packet switching would be similar to sending an e-mail. You compose an e-mail message and send it to your friend. The message you send is broken down into small pieces called **packets** or frames. This is done because large packets take up a lot of bandwidth, preventing other computers from communicating. After the packets hit the network, they are forwarded from computer to computer until they reach their final destination. All the packets can travel the same route or each can take a different route depending on how busy the network is. When the packets reach their final destination, they are assembled back into the original message and your friend reads it.

Integrating voice and data communications can be very cost effective. Let's look at an example of this. If you install a modem and use POTS to connect to a machine in New York, you are charged for a long distance phone call. If you use the Internet to make the connection, you connect via a local number and then use that connection to make contact with the machine in New York, saving the cost of a long-distance phone number.

Because IP telephony networks make better use of available bandwidth, a VoIP network carries voice traffic for less cost than a switched circuit telephone network does. In a public-switched telephone network, a dedicated end-to-end circuit is allocated for each call. In a VoIP network, data is much more compressed and carried in packets. Using the same bandwidth, a VoIP network can carry many times the number of voice calls as a switched circuit network and with better voice quality. Now that we have learned how analog and digital communications affect networking, we will go one step further and look at what allows devices to communicate over the network.



2.3 The OSI Reference Model

As networking became the norm for businesses, the need arose for businesses to be able to connect with each other even though their equipment and systems were different. In 1978, the **International Organization for Standardization (ISO)** developed an architecture that would allow the devices of different manufacturers to work together to communicate with different operating systems. In 1984, the ISO architecture became an international standard known as the **Open Systems Interconnection (OSI) reference model**. This architecture determines how hardware, software, topologies, and protocols exist and operate on a network. The OSI model is based on seven layers, as shown in Figure 2.7. Each layer adds functionality to the previous layer and communicates with the layers directly above and below it. Because each layer of the OSI model handles a different part of the

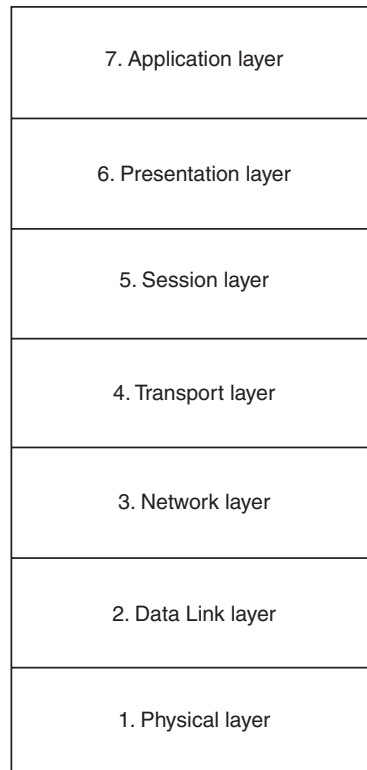


Figure 2.7
The OSI reference model

communications process, it makes the troubleshooting process a little easier because it provides specifications on how components should function.

The main idea behind the OSI model is that exchanging of data between two end points in a network can be divided into layers, with each layer adding its own set of special functions. Each communicating application is at a computer equipped with these layers. In an exchange between users, there will be a flow of data through each layer at one end down through the layers in that computer; and when the message arrives at its destination, there will be another flow of data up through the layers in the receiving computer that ultimately ends up at the application. The actual programming and hardware that furnishes these layers is usually a combination of applications, the computer operating system, transport and network protocols, and the software and hardware that enable you to put a signal on one of the lines attached to your computer.

We will go through each layer and discuss what each does as well as what devices function at that layer. The devices mentioned will be discussed in further detail later in this chapter or in the next one. Remember that the OSI model is a communications model. It is used in the telecommunications industry as well as in networking industry.

It is imperative that you grasp the information about the OSI model. Network architecture and devices all operate within the layers of the OSI model.

**NOTE**

Before we get into the layers of the OSI model, having some background information will help better understand how it works. We'll just cover the basics because much of this is explained in greater detail in later chapters, and some of it has already been explained in Chapter One. We will go over protocols, control information, error correction and flow control.

The OSI model provides a conceptual framework for communication between computers but in itself is not a method of communication. Actual communication is made possible by using communication **protocols**. A protocol is a set of rules and conventions that governs how computers exchange information over a **network medium**. Network medium refers to the cable (metallic or fiber-optic) that links computers on a network. Because wireless

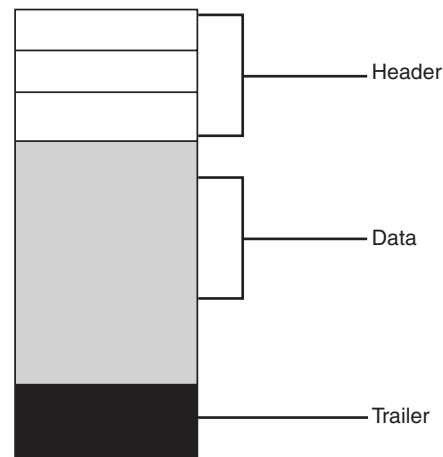
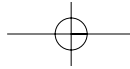


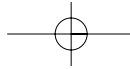
Figure 2.8
The structure of a packet

networking is possible, network medium can also describe the type of wireless communications used to permit computers to exchange data via some wireless transmission frequency. A protocol implements the functions of one or more of the OSI layers. A wide variety of communication protocols exist, and many of them rely on others for operation. This concept of building upon the layers already in existence is the foundation of the OSI model.

The OSI layers use various forms of control information to communicate with their equal layers in other computer systems. This information consists of specific requests and instructions that are exchanged between equal OSI layers. The data to be exchanged is broken down into packets. We briefly mentioned packets earlier in this chapter; let's now look at the parts of a packet. All packets consist of a header, data and a trailer. (See Figure 2.8.) The header contains the source and destination addresses, clocking information, and an alert signal. The data section contains the actual data or payload. The trailer contains information to verify that the contents of the packet are valid.

Control information is then added to the packets. Control information typically takes one of two forms: headers and trailers. Header and trailer information is added or removed as the data passes from layer to layer. An OSI layer may or may not attach a header or a trailer to data from upper layers.

Error checking determines whether transmitted data has become corrupt or damaged while traveling from the source to the destination. Error check-



ing is implemented at several of the OSI layers. A common error-checking method is the cyclic redundancy check (CRC) that detects and discards corrupted data. A CRC value is generated by a calculation that is performed at the source device. The destination device compares this value to its own calculation to determine whether errors occurred during transmission. If the values are equal, the packet is considered valid. If the values are unequal, the packet contains errors and is discarded.

Flow control prevents network congestion by ensuring that transmitting devices do not flood receiving devices with data. A high-speed modem may generate traffic faster than the phone lines can transfer it, or faster than the destination modem can receive and process it. The three commonly used methods for handling network congestion are windowing, buffering, and transmitting source-quench messages.

Windowing is a flow-control scheme in which the source device requires an acknowledgment from the destination after a certain number of packets have been transmitted. If the destination does not receive one or more of the packets for some reason, it does not receive enough packets to send an acknowledgment. The source then retransmits the packets at a reduced transmission rate. Buffering is used to temporarily store bursts of excess data in memory by network devices until they can be processed. Receiving devices use source-quench messages to help prevent their buffers from overflowing.

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers. The upper layers of the OSI model deal with application issues and generally are implemented only in software. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. Now we are ready to delve into the different layers and the devices that operate at those layers.

2.3.1 Physical Layer

The **Physical layer** (Layer 1) handles the mechanical and electrical communications. In other words, it translates bits (1s and 0s) into data that can be transmitted. Layer 1 specifications determine the shape, size, and pin-out of connectors; what voltages and currents are used; and how the physical media and electrical components work together.

Devices that operate at the Physical layer include network interface cards, hubs, repeaters, multistation access units, media filters, and transceivers.

2.3.2 Data Link Layer

The **Data Link layer** (Layer 2) provides flow, error control, and synchronization for the Physical layer. It takes information from the Network layer and sends it to the intended device through the Physical layer on the same network. The specifications defined at this layer are network and protocol characteristics. This includes physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing defines how devices are addressed. Network topology determines the specifications that define how devices are to be physically connected. Error notification alerts upper-layer protocols that a transmission error has occurred, and sequencing reorders frames that are transmitted out of order. Flow control monitors the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The **Institute of Electrical and Electronic Engineers (IEEE)**, a professional organization that defines networking and other standards, further defined the lower layers of the OSI model. The IEEE began this project in February of 1980 and named the project according to the year and the month it came into being. Hence, it became known as the 802 project. The results of this are 12 different specifications that define network connections, topologies, and interface cards. These versions and standards will be discussed in further detail in later chapters, but the standards, along with a brief description, will be listed at the end of the discussion on the OSI model because they work hand in hand. The IEEE 802.2 specification has divided the Data Link layer into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. Both layers are shown in Figure 2.9.

The **Logical Link Control (LLC) layer** manages communications between devices over a single link. This includes checking for errors and flow control. The LLC supports both connectionless and connection-oriented services used by higher-layer protocols. Connection-oriented and connectionless communications are discussed in the “Transport Layer” section. The **Media Access Control (MAC) sublayer** of the Data Link layer manages protocol access to the physical network medium. In other words, the MAC layer controls access and network adapter card drivers. **MAC**

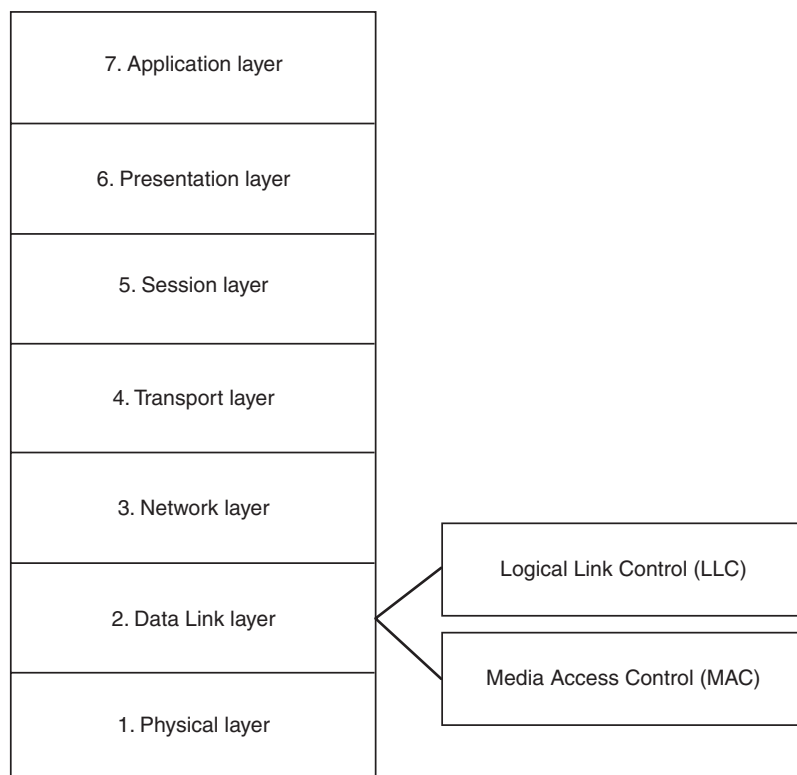


Figure 2.9
The sublayers of the Data Link layer

addresses enable multiple devices to uniquely identify one another. These unique addresses are assigned at the manufacturer. Because it only understands the MAC address, this layer cannot route to other networks—it can only pass on packets in its own segment. Devices that operate at this layer are bridges, switches, and routers.

2.3.3 Network Layer

The **Network layer** (Layer 3) manages the routing of packets that are to be forwarded on to different networks. The Network layer relies on the use of routable protocols to deliver packets to distant networks. The Network layer defines the network address, which is different from the MAC address. The MAC address is considered the physical address, and the network address is considered the logical address. Because this layer defines the logical network layout, routers can use it to determine how to forward

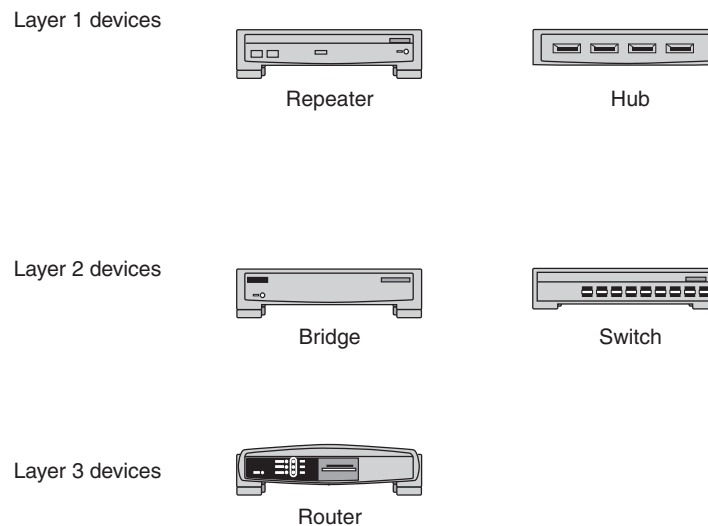
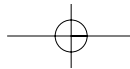


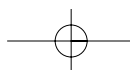
Figure 2.10
Devices that operate in the various lower levels of the OSI model

packets. Because routers function at this layer, much of the design and configuration of a network is done here. See Figure 2.10 for examples of the devices that operate on the first three layers of the OSI model.

2.3.4 Transport Layer

The **Transport layer** (Layer 4) manages the connection between the source and the destination to ensure that the data has reliable delivery. The Transport layer accepts data and segments it for transport across the network. Generally, the Transport layer is responsible for making sure that the data is delivered error free and in the proper sequence. Flow control generally occurs at the Transport layer. Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Reliable delivery involves error checking and recovery. Error checking involves detecting transmission errors, while error recovery involves acting to resolve any errors that occur.

Transport protocols can be characterized as being either connection-oriented or connectionless. Connection-oriented services must first establish a connection with the desired service before passing any data. A connectionless service can send the data without any need to establish a connec-



tion first. In general, connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not.

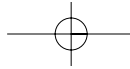
Connection-oriented service involves three phases: establishing the connection, transferring the data, and terminating the connection. The protocol is also responsible for putting the packets in the correct sequence before passing on the data. Connection-oriented network services have more overhead than connectionless ones. Connection-oriented services must negotiate a connection, transfer data, and tear down the connection, whereas a connectionless transfer can simply send the data without the added overhead of creating and tearing down a connection. An example of this is similar to the difference between regular mail and certified mail. Using regular mail delivery, you mail a letter and assume it will get there. Using certified mail delivery, the Post Office contacts the recipient, gives them the mail, and makes them sign for it.

2.3.5 Session Layer

The **Session layer** (Layer 5) manages the communication between the applications after a connection is made. It sets up the session, manages the information exchanges, and then breaks it down when the session ends. The Session layer establishes, manages, and terminates communication sessions. These sessions consist of service requests and responses that occur between applications located in different network devices. The sessions are coordinated by protocols implemented at this layer. It also monitors the identification of the session participants to be sure that only nodes that are authorized can participate in the session. An example of this would be a conference call. To connect, you need a participant number. The call is usually run by a moderator who decides who can talk and for how long. The call ends when the moderator disconnects.

2.3.6 Presentation Layer

The **Presentation layer** (Layer 6) formats the data for exchange between the Application layer and the Session layer. Data compression and encryption also occur at this layer. This layer converts incoming and outgoing data from one presentation format to another through the use of standard image, sound, and video formats; standard data compression schemes; and standard data encryption schemes. Presentation layer implementations are



not typically associated with a particular protocol stack. Some well-known standards include Motion Picture Experts Group (MPEG), Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF).

2.3.7 Application Layer

The **Application layer** (Layer 7) provides the user interface for communication. The Application layer is the OSI layer closest to the end user, which means that both the OSI Application layer and the user interact directly with the software application. This layer interacts with software applications. Application layer functions typically include file transfer, file management, message handling, and database query functions. The Application layer also determines the availability of an application with data to transmit, and decides whether sufficient network resources for the communication exist. The Application layer is not application itself that is communicating. It is a service layer that provides these services. Some examples of Application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

Let's summarize what we have learned. Each layer of the OSI model performs a particular function. This type of organization allows each layer to communicate only with its surrounding layers within a given host. Applications use layers 5 through 7 to communicate with another machine using the same protocol. Layers 3 and 4 define how data delivery is set up and defined on computers that use the same protocol. Layers 1 and 2 define the physical and electrical signal characteristics. Between hosts, each layer communicates with its corresponding layer on the other machine, but only through the lower layers on both machines. Information being transferred from a software application in one computer system to a software application in another must pass through all of the OSI layers. For example, if a software application in your system has information to pass to a software application in a coworker's system, the application program in your system will pass its information to the Application layer. The Application layer then passes the information to the Presentation layer, which relays the data to the Session layer, and so on, until it reaches the Physical layer. At the Physical layer, the information is placed on the physical network medium and is sent across the medium to the coworker's system. The Physical layer

of that system removes the information from the physical medium, and then its physical information is passed up to the Data Link layer, which passes it to the Network layer, and so on, until it reaches the Application layer. The Application layer of the system then passes the information to the application program to complete the communication process. See Figure 2.11 for an overview of data flowing through the OSI model layers.

The OSI reference model is only a guideline. An actual protocol or device may or may not assume all responsibilities of one particular OSI layer. It may also take on functions that span several layers. However, we use the OSI model to help us understand and classify the functions that make up a particular implementation.

There are several ways to remember the layers of the OSI model. You can make up a sentence of your own but two common ones are, "Please Do Not Throw Sausage Pizza Away" and from the top down, "All People Seem To Need Data Processing."



The ISO created the OSI model and the IEEE further defined the lower layers of the OSI model. Table 2.1 lists those specifications.

2.4 The Internet

The Internet can be considered the largest network in the world. This network is made up of computers used by many different types of businesses, educational institutions, governments, and individuals located around the world. Each network operates independently but can connect to other networks through routers, which are covered in the "Routers" section later in this chapter. Before we discuss how the Internet works, we will go over some of the history behind the Internet.

The name "Internet" refers to the global interconnection of networks made possible by the protocols devised in the 1970s that are still in use today. The Internet was originally called ARPANET (short for Advanced Research Project Agency). It was developed by the Department of Defense to provide a way to connect networks. The ARPANET grew from four nodes in 1969 to about a hundred by 1975. By mid-1975, it was determined that the ARPANET was stable enough to be turned over to a separate agency for

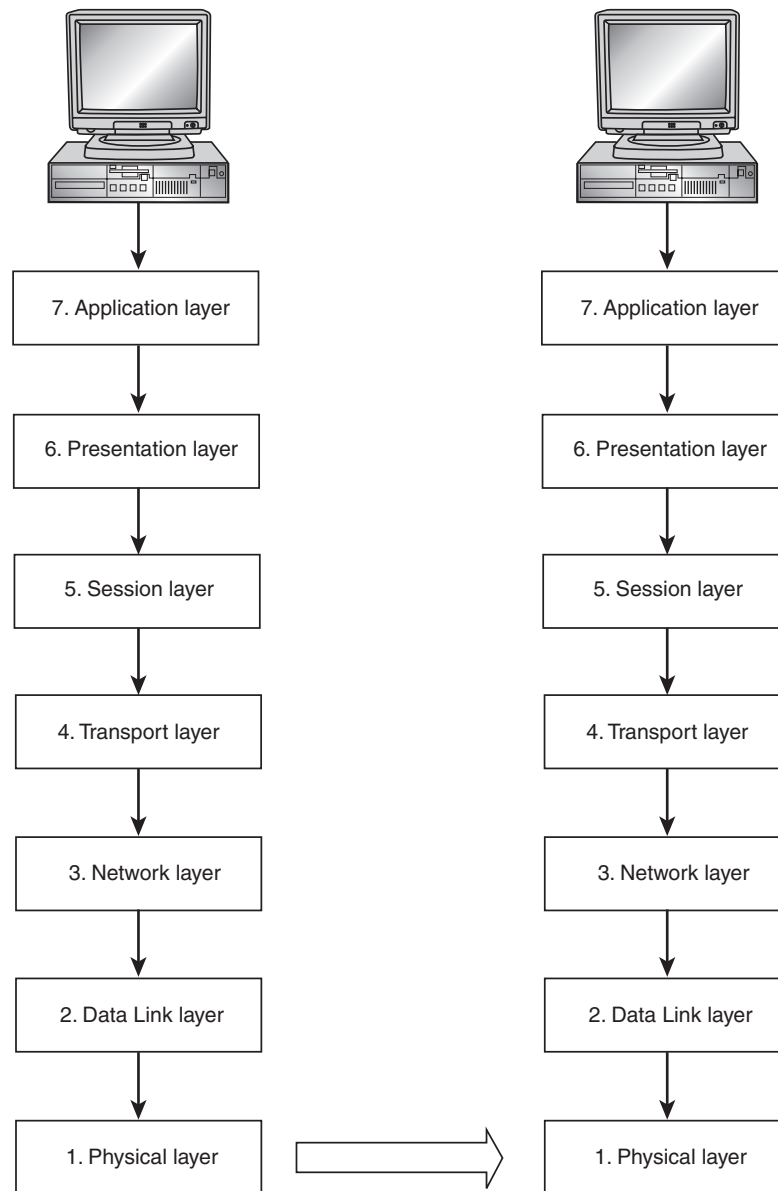


Figure 2.11
Path of an application
transmitting data through
the layers of the OSI
reference model

TABLE 2.1 IEEE 802 Standards

Standard	Name	Description
802.1	Internetworking	Defines internetworking communications, routing, bridging, and switching
802.2	Logical Link Control	Provides addressing, error checking, and flow control for data frames
802.3	Ethernet LAN	Defines all forms of Ethernet interfaces and media
802.4	Token Bus LAN	Defines all forms of Token Bus interfaces and media
802.5	Token Ring LAN	Defines all forms of Token Ring interfaces and media
802.6	Metropolitan Area Network (MAN)	Defines MAN services, technologies, and addressing
802.7	Broadband Technical Advisory Group	Specifies physical, electrical, and mechanical features of broadband cable
802.8	Fiber-Optic Technical Advisory Group	Provides technical direction for the use of fiber-optic technology and media
802.9	Integrated Voice/Data Networks	Defines integration of voice, video, and data on IEEE LANs
802.10	Network Security Technology Advisory Group	Develops a security model for diverse networks that covers authentication and encryption
802.11	Wireless Networks	Defines standards for wireless networks that cover a wide range of frequencies
802.12	Demand Priority	Defines the demand priority access method for 100VG-AnyLAN
802.14	Cable Modems	Creates standards for transmission of data over cable television networks

operational management, so responsibility was transferred to the Defense Communications Agency.

In 1973, the Defense Advanced Research Projects Agency (DARPA) began a series of research programs to extend packet switching to ground mobile units and ships at sea through the use of ground mobile packet radio and synchronous satellites. This process became known as *Internetting*. It was intended to

solve the problem of linking different kinds of packet networks together without requiring the users or their computers to know much about how packets traveled. About the same time, DARPA provided additional funding for a research project that began in the late 1960s to explore the use of radio for a packet-switched network. This effort, at the University of Hawaii, led to new mobile packet radio ideas and to the design of what is now Ethernet. The Ethernet concept arose when a researcher realized that the random-access radio system could be operated on a coaxial (coax) cable at data rates thousands of times faster than could then be supported over the air. These efforts came together in 1977 when a four-network demonstration was conducted.

Also in the early 1970s, researchers at Stanford began to design a new set of computer communication protocols that would allow multiple packet networks to be interconnected in a flexible and dynamic way. The first phase of this work was successfully completed in July 1977. This success led to an effort to implement robust versions of the two main Internet protocols—**Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**. By 1980 a serious effort was mounted to require all computers on the ARPANET to adopt the **Transmission Control Protocol /Internet Protocol (TCP/IP)** suite. This was accomplished in January 1983.

As DARPA was preparing to convert the organizations they supported to TCP/IP, the National Science Foundation started an effort to interconnect the nation's computer science departments through the use of dial-up connections. The result was "phone-mail," the capability for electronic mail exchange among computers that were not on ARPANET, which pioneered the use of TCP/IP over the X.25 protocol standard. NSF's interest in high bandwidth was heightened in 1986 through its sponsorship of NSFNET, which eventually replaced ARPANET when it was retired in 1990. Among the most monumental decisions that the NSF made was to support the creation of regional networks that would take the demand from the nation's universities and funnel it to the NSFNET backbone. The backbone was initially implemented using gateways and links operating at the speed of 56K bps. Because of rapidly increasing demand, a cooperative agreement was made with MCI and IBM to develop a 1.5M bps backbone. IBM developed the routers and MCI supplied 1.5M bps circuits. The result was a backbone with about 30 times the bandwidth of its predecessor.

Regional networks became the primary means by which universities and other research institutions linked to the backbone. By the mid-1980s there was sufficient interest in the use of the Internet in the research, educational, and defense communities, so businesses started making equipment for Internet implementation. In 1988, in an effort to test Federal policy on commercial use of the Internet, the Corporation for National Research Initiatives approached the Federal Networking Council for permission to experiment with the interconnection of MCI Mail with the Internet. An experimental electronic mail relay was built and put into operation in 1989.

NSFNET backbone traffic more than doubled annually, from a terabyte per month in March 1991 to eighteen terabytes a month in November 1994. The number of host computers increased from 200 to 5 million in the 12 years between 1983 and 1995. One of the major forces behind the exponential growth of the Internet was a variety of new capabilities, especially directory, indexing, and searching services that helped users find information more readily. Enhancing these services was the arrival of a “killer ap” for the Internet, the World Wide Web.

The World Wide Web was first used in experimental form in 1989. Around 1992 it came to the attention of a programming team at the National Center for Supercomputing Applications (NCSA). This team developed a graphical browser for the Web, called Mosaic. This software was made widely available on the Internet for free. Between 1992 and 1995 a number of commercial versions of Web browsers and servers emerged.

The Internet and the World Wide Web should not be used interchangeably. The World Wide Web is a method to navigate the Internet. They operate at different layers of the OSI model.



The Internet’s different services have evolved as technology has. Today some of the more popular Internet services are chat and instant messaging, e-mail, File Transfer Protocol (FTP), newsgroups, telnet, and the World Wide Web. Now that we know how the Internet and browsers were developed, let’s explore how the Internet communicates.

As stated earlier, the Internet is a network of interconnected, yet independent networks. Each host is directly connected to some particular network. Two hosts on the same network communicate with each other using the

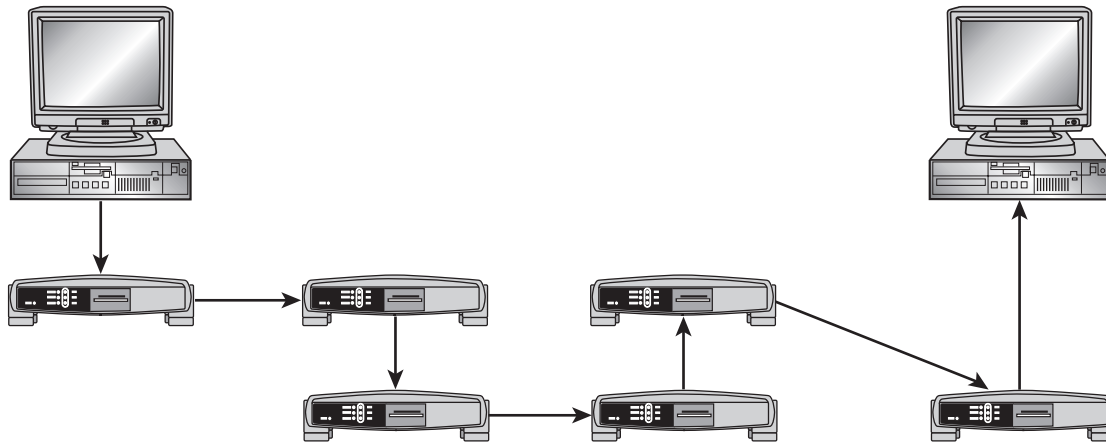
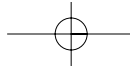
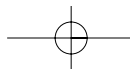
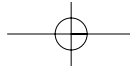


Figure 2.12
Path of a packet traveling through the Internet

same set of protocols that then would be used to communicate with hosts on distant networks. The language of the Internet is Transmission Control Protocol/ Internet Protocol (TCP/IP). This protocol calls for data to be broken into packets. These packets are designed to have a header for IP as well as TCP header followed by the data. The headers enable packets to be routed across many networks to arrive at their destination. (TCP/IP is described in finer detail in Chapter 6.) Packets are passed across the networks by devices called routers, which read the headers to determine whether the packet belongs to its network or should be passed on. (See Figure 2.12.) This is like sending a letter through the U.S. mail. The zip code is the ultimate destination for the letter. For example, when you send a letter from California to New York, it may be transported to various other post offices before it actually arrives in New York. If the zip code on the letter does not match a zip code for the area it arrives in, the letter is forwarded on until it reaches its final destination.

For the packets to reach the Internet, there must be some type of connection between the PC and the Internet. The connection is supplied by a company called an **Internet service provider (ISP)**. An ISP provides a gateway to the Internet, along with other online services, primarily as a paid service. The two most common ways to connect to an ISP are dial-up lines using modems and cable modem or digital subscriber lines. ISPs own





2.5 Asynchronous Transfer Mode (ATM) Networks

blocks of addresses that they assign to their customers to give them identity on the network. These addresses are called Internet protocol addresses, or IP addresses. Each address is unique. IP addressing will be covered in Chapter 7. Because IP addresses are numbers and are difficult to remember, hosts are usually found by their domain name. This allows easier navigation on the Internet. All domain names are mapped to IP addresses. This structure behind domain naming and other Internet services is covered in Chapter 9.

The advent of backbones and network infrastructure created the need for high-speed technology. Now it's time to look a high-speed technology that allows networks like the Internet to function.

2.5 Asynchronous Transfer Mode (ATM) Networks

Before there was a need to share resources and communicate, telephone companies built an international network to carry multiple telephone calls using copper cable. Soon the bandwidth limitations of copper cable became apparent, and carriers began looking into upgrading their copper cable to fiber cable. To address these concerns, the **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)**, formerly called the Committee for International Telegraph and Telephone (CCITT), and other standards groups started work to establish a series of recommendations to implement a fiber-based network that could solve current limitations and allow networks to efficiently carry services of the future.

To deliver new services such as video conferencing and video on demand, as well as provide more bandwidth for the increasing volume of traditional data, the communications industry introduced a technology that provided a common format for services with different bandwidth requirements. This technology is **Asynchronous Transfer Mode (ATM)**. As ATM developed, it became instrumental in how companies deliver, manage, and maintain their goods and services. It was first developed at Bell Labs in 1983, but it took several years to have the specifications agreed upon by the standards organizations. ATM emerged commercially in the early 1990s. However, then few applications could utilize the features of ATM. The ATM Forum was established in October, 1991, and it issued its first specifications eight months later. The ATM Forum was formed to accelerate the use of ATM products and services.

ATM uses connection-oriented switches to permit senders and receivers to communicate by establishing a dedicated circuit. In this environment, data travels in fixed 53-byte cells. Five bytes are used for header information and 48 bytes are used for data. The data transfer rate can reach up to 9,953 Mbps.

NOTE The cells in ATM are a fixed length of 53 bytes. If the data takes up less space than that, the cells are padded with empty payload.

The use of fixed length cells enables ATM to work at extremely high speeds. ATM relies on circuit switching, which is done at the data link layer of the OSI model. Switches determine the most efficient route between the sender and the receiver, and then establishes this path before any data is transmitted. ATM was designed to guarantee a specific **quality of service (QoS)**. QoS is a standard specifying that data will be delivered within a particular time frame after transmission. It is best suited for long distance, high-bandwidth applications. ATM bandwidths are rated in terms of an optical carrier level. Table 2.2 lists the various rates for optical carrier signaling.

TABLE 2.2 Signaling Rates for Optical Carrier Levels

Optical Carrier Level	Signaling Rate
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-9	466.56 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-36	1.866 Gbps
OC-48	2.488 Gbps
OC-96	4.976 Gbps
OC-192	9.953 Gbps
OC-255	13.271 Gbps
OC-768	39.813 Gbps

Now it's time to look at the devices that make it possible to transmit data via telephony networks, the Internet, and ATM networks. We will discuss the different types of components that a network is comprised of, what layer of the OSI model they operate at, and their limitations.

2.6 Networking Components

Computers must share media to communicate successfully. Network media can be a physical cable or it can be wireless. Regardless of the media type, its main function is to carry data from one device to the next. To access the network or communicate with other computers, a network interface card (NIC) is needed. These come in a variety of specifications, and depending on the network setup may not be interchangeable in all machines. See Figure 2.13 for an example of a NIC.

You will often hear the term NIC; remember that the C stands for card. Many times the acronym is misused and you will hear "NIC card." This is redundant.



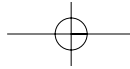
After the network card is installed, it is connected to the media. In the next section we will describe the various methods of connecting to a network.

2.6.1 Media: Cables and Wireless

Media can be divided into two categories, wired and wireless. We will first look at wired or cabled medium and then look at wireless technology.



Figure 2.13
A network interface card



Cabling is an important component of any network, because unless the network is wireless, this is how the data will travel from machine to machine. Before we discuss the different types of cable, let's look at the methods of sending signals across these cables. There are two primary methods to do this, baseband and broadband.

Baseband uses a digital transmission pulse at a single fixed frequency. This means that the entire bandwidth of the cable is used to transmit one data signal. It also limits any cable strand to either half duplex or full duplex. **Half-duplex** transmission means that data can be transmitted in both directions on a cable but not at the same time. **Full-duplex** transmission means that data can be transmitted in both directions on the cable at the same time. Because baseband uses a single fixed frequency, as the signal travels further down the cable, its strength decreases and can distort. For this reason, special devices called **repeaters** are used. A repeater refreshes the signal so that it is restored to its original strength and quality.

Broadband uses analog transmission over a continuous range of values. It travels one way only in optical waves. It is necessary to have two channels, one for receiving and one for sending data. If the cabling supports enough bandwidth, more than one transmission can operate on a single cable. If this happens, you will need a tuner to pick up the correct signal. As with baseband, if the signal travels too far, it needs to be strengthened. The device used to do this is called an amplifier. An amplifier detects weak signals, strengthens them, and then rebroadcasts them.

Cabling Media

Several types of network cabling are available. The three main types are coaxial, twisted pair, and fiber optic. They all share certain characteristics, which include grade, bandwidth rating, maximum segment length, maximum number of segments per network, maximum number of devices per segment, and interference susceptibility. Besides these factors, you should also take into consideration the cost of the cable and the installation costs.

Coaxial cable was the first type of cable used to network computers and was instrumental in forming the basis of the Ethernet standard. Coaxial cables are made of a thick copper core with an outer metallic shield used to reduce external interference. External interference can be in the form of electromagnetic interference (EMI), which comes from devices in the surrounding environment, or radio frequency interference (RFI), which

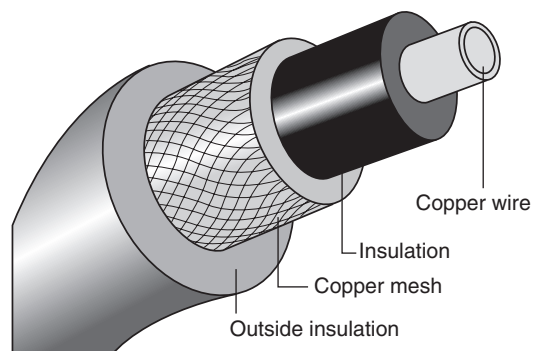


Figure 2.14
Coaxial cable

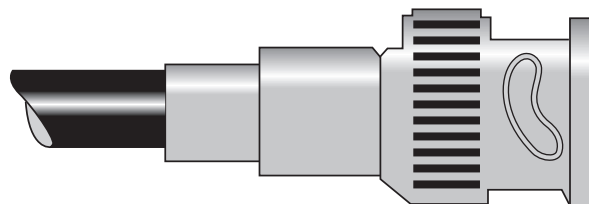


Figure 2.15
A BNC connector

comes from other broadcast signals. Often, the shield is made of woven copper mesh or aluminum. The cable is then surrounded by a plastic covering, called a sheath. See Figure 2.14.


Although coaxial cables are no longer deployed, they still may be found in legacy environments. The two main types of coaxial cables used are 10Base2 and 10Base5.

10Base2, also known as Thinnet, has a communication speed of 10 Mbps, uses baseband signaling, and is limited in length to 185 meters per segment. 10Base2 uses BNC connectors to attach segments to each other. See Figure 2.15. Terminators are required at both ends of each segment to prevent signal echo.

10Base5, also known as Thicknet, it has a communication speed of 10 Mbps, uses baseband signaling, and is limited in length to 500 meters per segment. 10Base5 uses **attachment unit interface (AUI)** external transceivers connected to each NIC by a vampire tap that allows access to the network by piercing the cable.

TABLE 2.3 Types of RG Cable

Specification	Type	Impedance	Description
RG-58/U	Thinnet	50 ohms	U stands for utility grade; solid copper core
RG-58 A/U	Thinnet	50 ohms	A/U indicates braided copper center with foam dielectric insulator; stranded copper core
RG-58 C/U	Thinnet	50 ohms	Solid dielectric insulation; Military version of RG-58 A/U
RG-59	CATV	75 ohms	Broadband cable used for television
RG-6	Broadband	75 ohms	A CATV drop cable with higher bandwidth and larger diameter than RG-59
RG-62	Baseband	93 ohms	Used for IBM 3270 terminals and ARCnet
RG-8	Thicknet	50 ohms	0.4" in diameter with a solid core
RG-11	Thicknet	75 ohms	A CATV trunk line; 0.4" in diameter with a stranded core

TIP  To remember 10Base2 and 10Base5, look at the makeup of the type: 10 is for the bandwidth, 10 Mbps per second; base is for the signaling, baseband; and the 2 and 5 are the estimated segment lengths—200, which is rounded up from 185, and 500.

Coax belongs to a family of cable specifications called Radio Government (RG). Due to a joint effort between the U.S. military and cable manufacturers, the specification came into being. Table 2.3 lists the types of RG cable.

If using coaxial cable, keep in mind that the electric signal, conducted by a single core wire, can easily be tapped by piercing the sheath. Another concern of coax cable is reliability. Because there is no focal point involved, a faulty cable can bring the entire network down. Missing terminators or improperly functioning transceivers can cause poor network performance and transmission errors. If you are using coax cable, be sure to have proper cable testing equipment available and periodically scan the network.

Twisted-pair cable is used in most of today's network topologies. Twisted-pair cabling is either unshielded (UTP) or shielded (STP). Plenum cable is also available; this is a grade that complies with fire codes and is used for

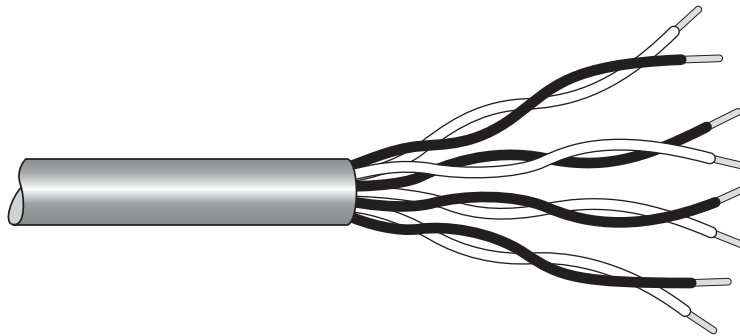


Figure 2.16
UTP cable

running cable either in the area above the ceiling or below the subflooring. The outer casing is more fire resistant than regular twisted-pair cable.

UTP is popular because it is inexpensive and easy to install. See Figure 2.16 for an example of UTP.

There are seven types of UTP cable, the most popular being Category 5 (Cat5). Before Cat5, Cat3 type cable was used on Ethernet networks, and some networks may still have it in place. Cat3 is the lowest category that meets standards for a 10BaseT network. The following are the speeds and cable lengths for the seven categories of unshielded pair cable:

- **Category 1 (Cat1):** Traditional telephone cable used prior to 1982 for voice only.
- **Category 2 (Cat2):** Cabling for bandwidth up to 4 Mbps, consisting of four pairs of wire.
- **Category 3 (Cat3):** Speed capability of 10 Mbps, with cable segments up to 100 meters. Consists of four pairs of wire.
- **Category 4 (Cat4):** The first data-grade cable. Certified for bandwidth up to 16 Mbps. Consists of four pairs of wire.
- **Category 5 (Cat5):** Speed capability of 1 Gbps, with cable segments up to 100 meters. Consists of four pairs of wire.
- **Category 6 (Cat6):** Consists of four pairs of wire wrapped in foil insulation. The insulation provides shielding against crosstalk and allows for support up to at least six times the throughput of Cat5.

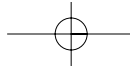
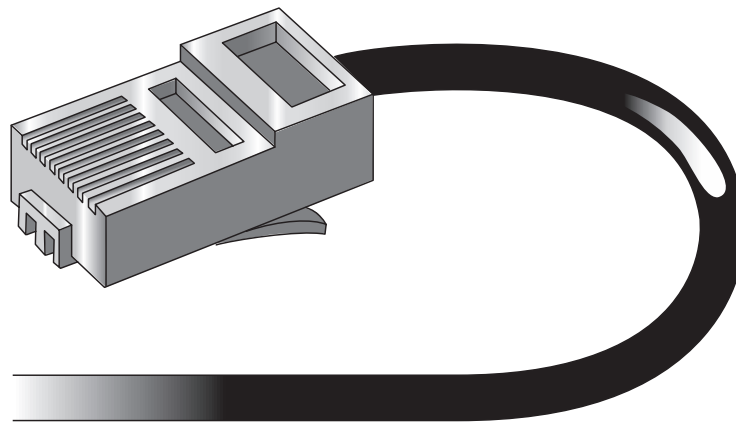


Figure 2.17
STP cable



Figure 2.18
RJ-45 connector



- **Category 7 (Cat7):** Speed capability of 1 Gbps, with two layers of shielding. Due to the additional shielding, special connectors are needed.

UTP is eight wires twisted into four pairs. The design cancels much of the overflow and interference from one wire to the next, but UTP is subject to interference from outside electromagnetic sources and is prone to RFI and EMI as well as crosstalk.

STP is different from UTP in that it has shielding surrounding the cable's wires. Some STP has shielding around the individual wires, which helps prevent crosstalk. STP is more resistant to EMI and is considered a bit more secure because the shielding makes wire-tapping more difficult. See Figure 2.17.

Both UTP and STP use an RJ-45 connector to plug into network devices such as NICs, hubs, and switches. See Figure 2.18.

Equipment that is associated with STP and UTP cables includes punch-down blocks, patch panels, and wall plates. Punchdown blocks help organize cables and can be used for both network and telephone management. Patch panels allow the cables to be connected in an arrangement beneficial

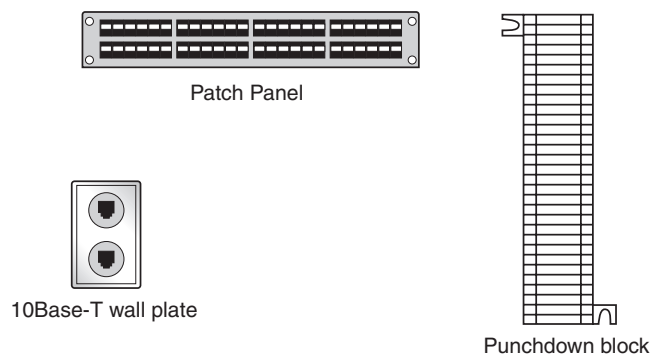


Figure 2.19
Punchdown block, patch panel, and wall plate

to the network design. Wall plates are used to make office wiring easier. Usually the cables will be connected on one end to the wall plate and on the other end to the patch panel. Then the RJ-45 connectors attach a patch cable from the wall plate to the computer and from the patch panel to a hub or switch. See Figure 2.19.

10BaseT is an Ethernet standard that replaces 10Base2 and 10Base5. Ethernet will be discussed in detail in Chapter 3. The “10” represents 10-Mbps throughput, “base” means that it uses baseband transmission, and “T” tells you that it uses twisted-pair wire. On this type of network, two pair of wires are used for transmission—one for sending and one for receiving. It also requires Cat3 or higher grade wire, and each segment can be up to 100 meters.

100BaseT is also known as Fast Ethernet. Based on what you have learned so far, it could be determined that this type of media has a throughput of 100Mbps, and uses baseband transmission and twisted-pair wire. This type of standard usually requires Cat5 or higher grade wire. There are two 100BaseT specifications, 100BaseTX and 100BaseT4. The difference between the two lies in how they achieve their transmission rates. 100BaseTX uses two pair of wires within a Cat5 cable, one pair for sending and one for receiving. 100BaseT4 uses all four pairs of wires and can use Cat3 cabling. It achieves its speed by breaking down the data into three 33 Mbps streams, and then using three pairs of wire to send it.

100BaseT4 and 100BaseTX are not interchangeable. You cannot mix devices on the same segment; in other words, you must pick one or the other.

! WARNING

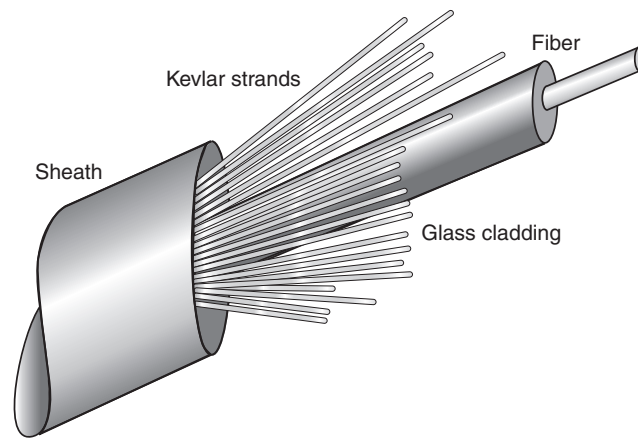
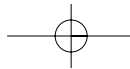


Figure 2.20
Fiber-optic cable

100BaseVG is an alternative to Ethernet technology. “VG” stands for voice grade. This is also known as 100VG-AnyLan. 100BaseVG is more efficient at processing and carrying audio and video, but it requires special NICs and connecting devices. It uses all four wire pairs, so it is slower than 100BaseT.

Fiber was designed for transmissions at higher speeds over longer distances. It uses light pulses for signal transmission, making it immune to RFI, EMI, and eavesdropping. Fiber optic has a plastic or glass center surrounded by another layer of plastic or glass, called cladding. To keep the cable from stretching, another layer of strands of polymer fiber, called Kevlar, is added. Finally, it all is surrounded with a protective outer coating called a sheath, as shown in Figure 2.20. Data transmission speed ranges from 100 Mbps to 10 Gbps and can be sent a distance of 100 kilometers.

Fiber-optic cable comes in two different types, single-mode fiber (SMF) and multimode fiber (MMF). Single-mode fiber uses a laser for transmission and is used mainly by industries that provide communications over large areas, such as telephone companies. Multimode fiber uses diode transmitters and is used mainly for network and college campuses up to a distance of 2 kilometers. Laser transmissions travel much farther than diode transmitters. There are a variety of connectors that can be used with fiber-optic cable. The two most popular are the ST- and SC-type connector. Figure 2.21 shows an example of

Figure 2.21
Fiber-optic cable
connectors

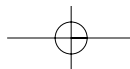
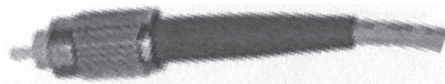


TABLE 2.4 Types of Network Cable

Standard	Type of Cable	Bandwidth	Maximum Length per Segment
10Base2	Coaxial	10 Mbps	185 meters
10Base5	Coaxial	10 Mbps	500 meters
10BaseT	UTP	10 Mbps	100 meters
100BaseT	UTP	100 Mbps	100 meters
100BaseT4	Four pairs, Cat3, Cat4, Cat5 UTP	100 Mbps	100 meters
100BaseTX	Two pairs, Cat5 UTP or Cat1 STP	100 Mbps, Fast Ethernet	100 meters
100BaseVG	UTP	100 Mbps, Fast Ethernet	100 meters
10BaseF	Fiber-optic	10 Mbps	2 kilometers
10BaseFX	Fiber-optic	100 Mbps, Fast Ethernet	2 kilometers

the ST-type connector. If you are using a patch cable to run from a router to a patch panel, you should purchase the cable with connectors already installed.

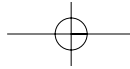
A suffix of “F” or “FX” means that the cable is suitable for an Ethernet environment. 10BaseF requires two strands of multimode cable and uses an ST-type connector. 100BaseFX also requires two strands of multimode cable but can use either the SC- or ST-type connector. The throughput for 10BaseF is only 10 Mbps, so due to the low output and high cost, it is seldom found in networks today.

On the down side, fiber is still quite expensive compared to more traditional cabling. It is also more difficult to install, and fixing breaks can be costly. Fiber can transmit data in only one direction at a time; therefore, each cable must have two strands, one for receiving and one for transmitting. Table 2.4 summarizes types of network cable.

Now that we have gone over all the cabling types, it’s time to look at wireless technology.

Wireless Technology

Wireless devices have become extremely popular because of the mobility they provide. The term *wireless network* refers to technology that allows two or more computers to communicate using standard network protocols,



without network cabling. They are most often referred to as wireless local area networks (WLANs). LANs and wireless technology will be explained in further detail in the next chapter. This technology has produced a number of affordable wireless solutions that are growing in popularity with businesses and schools, or where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Wireless networking hardware requires the use of technology that handles data transmission over radio frequencies. The most widely used standard is the IEEE 802.11 standard that defines all aspects of Radio Frequency Wireless networking. Currently, the IEEE standards for wireless are 802.11a and 802.11b. There are plans to implement 802.11e, f, g, and i in 2003. Because standards operate on radio frequencies, one of the issues with the current wireless technology is that it is a broadcast signal, so basically it advertises that it is out there, making it easy to pick up.

To connect a wireless network to a wired network, you will need some sort of bridge between the wireless and wired network. This can be done either with a hardware access point or a software access point. Hardware access points are available with various types of network interfaces, but typically require extra hardware to be purchased if your networking requirements change. A software access point does not limit the type or number of network interfaces you use; it is only limited by the number of slots or interfaces available in the computer. It may also allow considerable flexibility in providing access to different network types. A software access point may include additional features such as shared Internet access, web caching, and content filtering.

The 802.11b standard specifies a transfer rate of 11 Mbps, which is sufficient for most broadband connections. As the signal deteriorates, the transfer rate drops dramatically, to 5.5 Mbps, 2 Mbps, and then 1 Mbps, although actual throughput is about half these rates. Optical wireless transmission via a light beam is capable of transmitting data at speeds up to 622 Mbps.

There are two kinds of wireless networks, ad-hoc and access points. An ad-hoc, or peer-to-peer wireless network, consists of computers that are equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources.

A wireless network can also use an access point, or base station. In this type of network, the access point acts like a hub, providing connectivity for the wireless computers. It connects the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources. There are two subcategories of access points: hardware and software access points. Hardware access points offer comprehensive support of most wireless features, but all devices may not be compatible. Software access points run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network.

Each access point has a specific range in which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending upon the environment. When pushed to the limits of the range, the performance may drop because the quality of connection deteriorates and the system tries to compensate. Indoor ranges for wireless devices are 150 to 300 feet but may be shorter if the construction of the building interferes with radio transmissions. Although longer ranges are possible, performance will degrade with distance. Outdoor ranges are quoted up to 1000 feet, depending on the environment.

2.6.2 Hubs

A **hub** is a multiport repeater that retransmits a signal on all ports. When a packet arrives at one port, it is sent to the other ports so that all segments of the LAN can see it. Because it operates at layer one of the OSI model, it can connect segments or a network but cannot segment a network. Most hubs come with a minimum of 4 ports but can have as many as 48. There are two basic types of hubs: active and passive. Active hubs are the type described previously in this paragraph. A passive hub simply allows the signal to pass through without any amplification or regeneration. Intelligent or manageable hubs add features to active hubs that enable each port to be configured and the traffic passing through the hub to be monitored. A switching hub is a type of active hub that can read the destination address of packets and forward it to the correct port.

Most hubs require no configuration, and passive hubs do not even require power. And remember that the devices connected to hubs all share the same bandwidth. In other words, if you have a 10-Mbps hub and three devices are transmitting at the same time, each device gets one third of the bandwidth (see Figure 2.22).

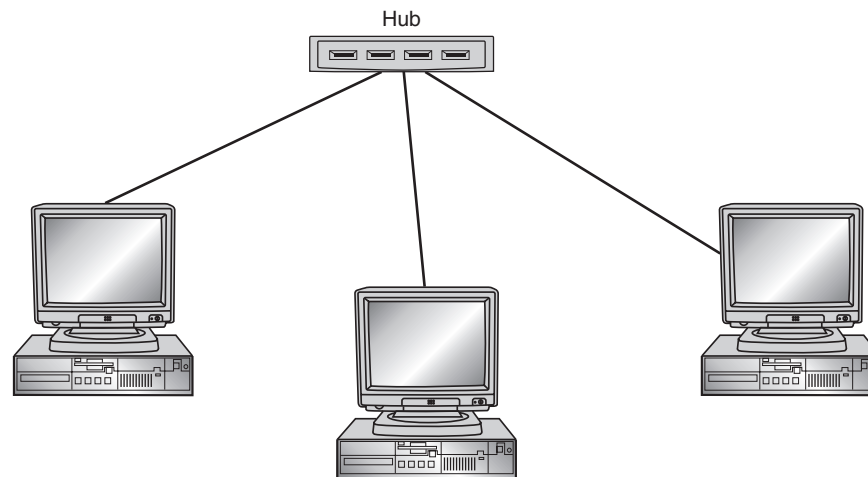
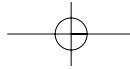


Figure 2.22
A hub connected to three devices

WARNING ! To connect two hubs you must use a crossover cable, or use the uplink port.

A stackable hub is designed to be connected and stacked on top of another hub, forming an expanding stack. This stackable approach allows equipment to be easily expanded as it grows in size and also reduces clutter.

2.6.3 Bridges

A **bridge** is a device that connects two or more segments of a network to make them one. It could be described as a device that determines whether a message from you to someone else is going to the local area network or to someone on the local area network in the next building. A bridge examines each message, passing on those known to be within the same LAN, and forwarding those known to be on the other connected LANs. It looks similar to a hub but functions at the next layer of the OSI model, the Data Link layer. Bridges have a single input and a single output port. It stores the MAC address for each device and then analyzes the incoming packets to determine what to do with them as they come through. Basically, it learns all the MAC addresses of the network to construct a database used for forwarding or filtering packets. A bridge can connect two different types of topologies because it does not understand anything above the Data Link layer. It doesn't matter whether one machine is using TCP/IP and another is using IPX/SPX because they are only concerned with the MAC addresses

and not the protocols. This allows them to move data more rapidly, but it takes longer to transmit because a bridge analyzes each packet.

2.6.4 Switches

Switches are rapidly becoming more popular than hubs when it comes to connecting desktops to the wiring closet. Switches operate at the Data Link layer of the OSI model. Their packet-forwarding decisions are based on MAC addresses. That is, a switch simply looks at each packet and determines from a physical address (the MAC address) which device a packet is intended for and then switches it out toward that device.

Switches allow LANs to be segmented, thereby increasing the amount of bandwidth that goes to each device. This means that, unlike a hub, each port on the switch is like a network segment itself. If you have a 10-Mbps switch with three devices connected to it, all three devices can use 10-Mbps of bandwidth. A switch repeats data only to the specified port, whereas a hub sends the data to all ports. In this context, it is said that each segment is a separate collision domain but all segments are in the same broadcast domain. Collision and broadcast domains are explained in Chapter 5. The basic functions of a switch include filtering and forwarding frames, learning media access control (MAC) addresses, and preventing loops.

In wide area networks such as the Internet, the destination address requires them to be looked up in a routing table by a device known as a router. Some newer switches also perform routing functions. These switches are sometimes called IP switches or layer-3 switches. Bridges and switches are covered in Chapter 5.

2.6.5 Routers

Routers operate at the Network layer of the OSI model. They forward information to its destination on the network or the Internet. Routers maintain tables that are checked each time a packet needs to be redirected from one interface to another. The routers may be added manually to the routing table or may be updated automatically using various protocols. Although routers are primarily used to segment traffic, they have some good features. One of the best is its ability to filter packets either by source

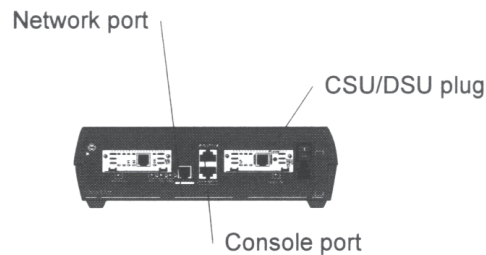
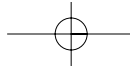


Figure 2.23
Router

address, destination address, protocol, or port. A router may create or maintain a table of the available routes and their conditions, and then use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. Routers can also be configured to use strong protocol authentication.

On the Internet, a router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any gateway, including each Internet point of presence. Many times the connection from a router to the Internet is through a device called a Channel Service Unit/Data Service Unit (CSU/DSU). The router is then internal, connected to a LAN port on a switch. See Figure 2.23 for an example of a router. Routing will be discussed further in Chapter 8.

Now that we have defined cabling and the devices that hook everything together, it's time to look at how to lay out the network. The actual geometric layout of the workstations is important because it will determine the type of cable, access, and protocols used.

2.7 Network Topologies

In this section you will get a good grasp of the ways that a network can be designed. The physical layout of a network is called the **topology**, which includes the method of communication. When designing a network, you

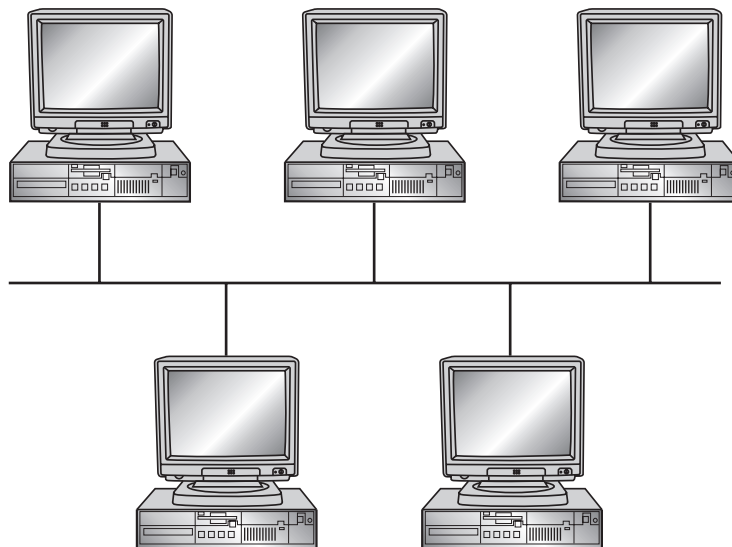


Figure 2.24
Bus topology network

should build in room for expansion. It is much easier to adapt a current network than to have to replace it because it was poorly designed.

2.7.1 Shared Medium

All machines “share” the network. This design as a shared media topology means that all devices on the network compete for access on a single shared piece of media. Only one device can transmit (talk) on the media at a time while all others must listen. When more than one device tries to talk simultaneously, the competition for access to the media results in a collision of information. Because the devices share the same media, limitations on total throughput and distance limitations of the cabling must be considered. Now we look at the two most common topologies where all devices share media, bus and star.

Bus

The **bus** topology consists of computers connected by a single cable called a **backbone**, as shown in Figure 2.24. All the computers on the bus share in its capacity. This is the simplest method for connecting computers. In a bus environment, 10Base2 or 10Base5 cable is used, and

Figure 2.25
Terminator

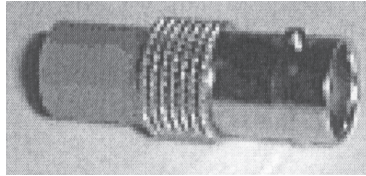


TABLE 2.5 Advantages and Disadvantages of the Bus Topology

Advantages	Disadvantages
Cable use is economical because all computers are in one line.	It is difficult to isolate problems because one break affects the entire network.
Cabling is easy to work with and extend, along with being cost-effective.	One break or bad termination brings down the entire network.
Layout is simple.	Heavy traffic can slow it down because all machines share the same bandwidth.

because all devices share the same bandwidth, the more devices the slower the network. In fact, it is probably not feasible for more than 10 workstations.

In a bus topology, the computers only listen for data being sent to them—they do not forward data. This is called a passive topology. A generated signal moves from one end of the bus to the other end. If it is not stopped, it will continue bouncing back and forth, preventing the computers from sending data. To prevent this, a terminator is located at each end of the cable. (See Figure 2.25.)

Because the computers are all connected by the same cable, if one segment has a problem the whole network is down. Table 2.5 lists the advantages and disadvantages of the bus topology.

TIP 

A bus topology can be likened to a transportation bus—if the bus breaks down, no one gets to where they're going.

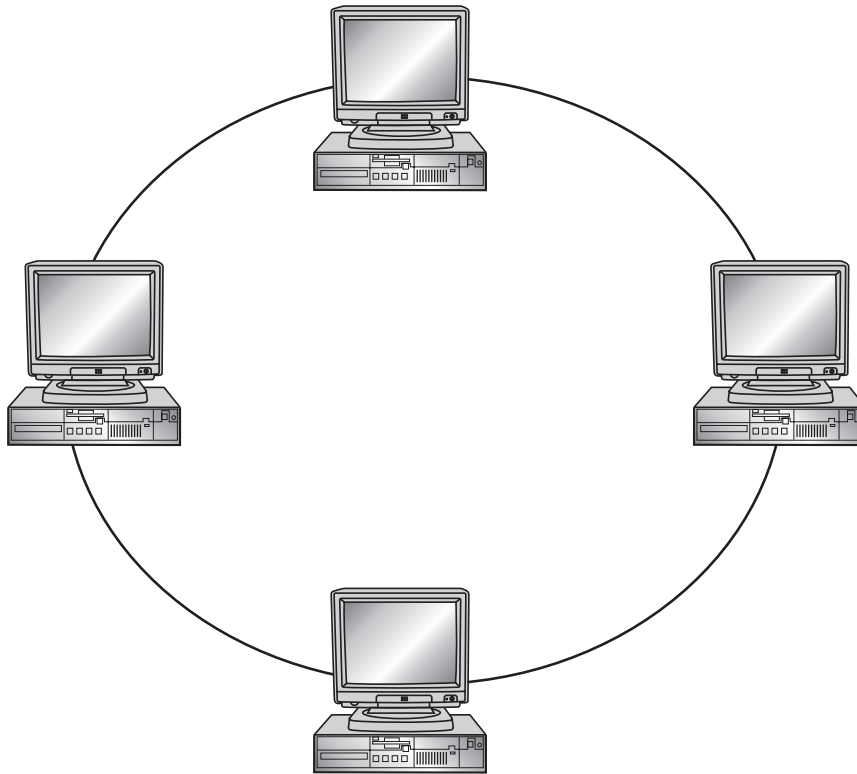


Figure 2.26
A ring topology

Ring

In a **ring** topology, each computer connects directly to the next one in line, forming a circle, as shown in Figure 2.26. Data travels in a clockwise direction, and each computer accepts the information intended for it and passes on the information for other computers. It uses a **token**, which is actually a small packet, to send information. Every computer in the ring is responsible for either passing the token or creating a new one. **Token passing** uses the token, or series of bits, to grant a device permission to transmit over the network. The computer with the token can pass data on the network. When a computer has information to send, it modifies the token and passes it on. After the token reaches its final destination, it lets the sender know it has arrived safely, the sender then makes a new token, and the process starts over. Most ring networks use fiber or twisted pair as the medium.

TABLE 2.6 Advantages and Disadvantages of the Ring Topology

Advantages	Disadvantages
Equal access is granted to all computers.	It is difficult to isolate problems because one break affects the entire network.
Network performance is consistent due to token passing.	If one computer fails, it brings down the entire network.
	The entire network is disrupted when adding or removing computers.

In a ring topology, if one computer fails, the network goes down. This is known as an active topology because each workstation is responsible for sending on the token. Currently, many ring networks implement a dual-ring network or use smart hubs to help alleviate this issue. In a dual ring, two rings are used for redundancy while smart hubs remove the failed computer from the ring. Table 2.6 lists the advantages and disadvantages of the ring topology.

2.7.2 Peer-to Peer

In a **peer-to-peer** network, all machines are equal. They each can act as a server and a client. There is no central control over shared resources; the individual users decide what to share and with whom. There is little control over who has access to what resources and who has what version of each file, so it is less secure than a server-based network. However, it is acceptable for small offices that do not require administration and is much cheaper to implement than a server-based solution. The two most common peer-to-peer networks are the star and mesh topologies.

Star

In a **star** topology, the computers are connected to a centralized hub by a cable segment. (See Figure 2.27.) They require more cabling than ring or bus topologies, but each computer is connected to the hub by its own cable. Therefore, if one computer connection goes down, it does not affect the rest of the network. Because each workstation has its own connection, it is much easier to move them around or connect them to other networks. 10BaseT-100BaseFX can be used with a star topology. A star topology can

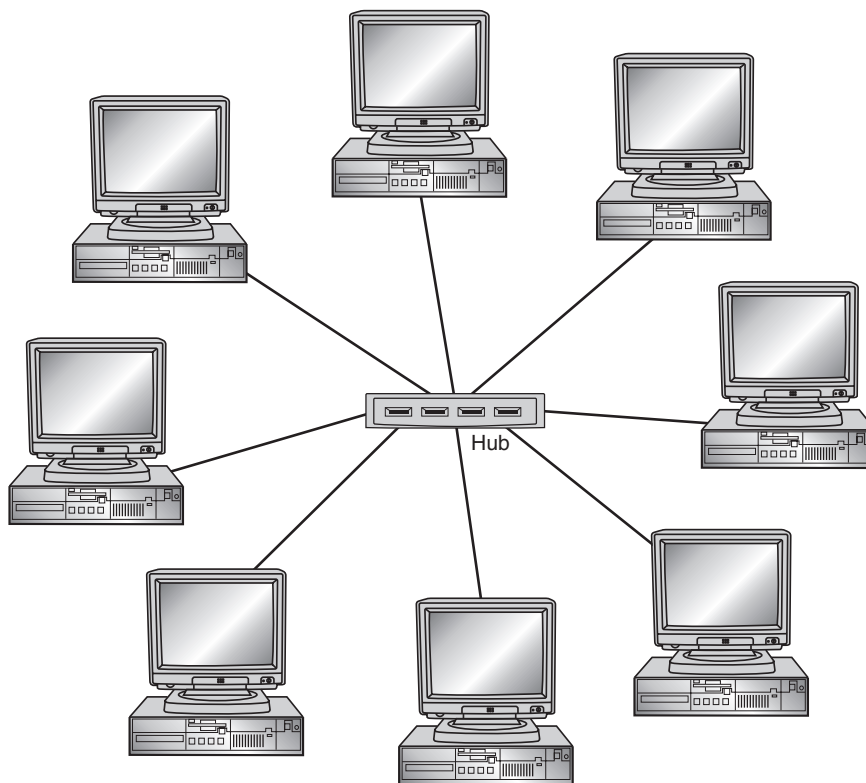


Figure 2.27
A star topology

support up to 1024 workstations, but it may not be feasible to connect them all to the same logical network. Table 2.7 lists the advantages and disadvantages of the star topology.

A star topology can be likened to a star in the night sky: If one star falls, the sky still stays lit.



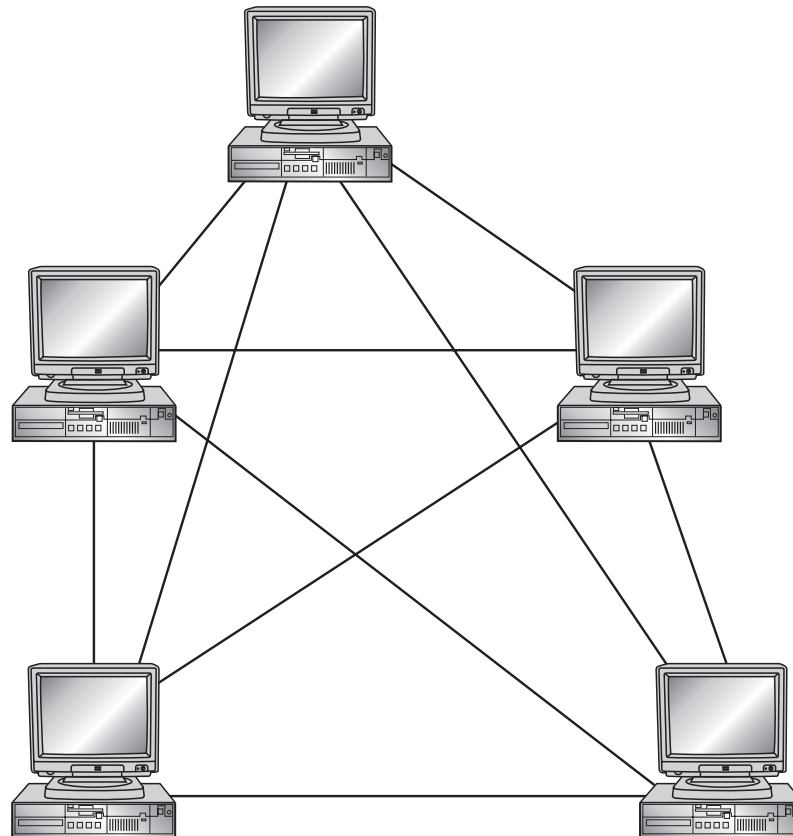
TIP

Mesh

In a **mesh** topology, all devices are connected to each other more than once to create fault tolerance. (See Figure 2.28.) A single device or cable failure will not affect the performance because the devices are connected by more than one means. This is more expensive as it requires more hardware and cabling. This type of topology can also be found in enterprise-wide networks with routers connected to other routers for fault tolerance.

TABLE 2.7 Advantages and Disadvantages of the Star Topology

Advantages	Disadvantages
The entire network is not disrupted when adding or removing computers.	It requires more cabling because each machine needs a separate connection to the central hub.
If one computer fails, it doesn't affect the rest of the network.	If the central hub fails, it brings down the entire network.
It is easy to manage and monitor.	N/A

**Figure 2.28**
A mesh topology

2.7.3 Hybrid networks

In a **star bus** topology, computers are connected to hubs in a star formation, and then the hubs are connected via bus topology. (See Figure 2.29.) Although it is more expensive to implement, longer distances can be covered, and networks can be isolated more easily.

In a **star ring** topology, data is sent in a circular motion around the star. (See Figure 2.30.) This eliminates the single point of failure that happens in a ring topology. It uses **token passing** data transmission with the physical layout of a star.

Large networks typically are organized as hierarchies. A hierarchical organization provides advantages such as ease of management, flexibility, and a reduction in unnecessary traffic. In a hierarchical network structure, a high-speed backbone usually connects the servers. Fiber or ATM are the usual choices for these high-speed backbones. The types of large networks and their technologies will be discussed in the next chapter.

2.8 Chapter Summary

- A network is a group of computers that can communicate with each other to share information, and when they can communicate with each other they can also share resources. When a server provides a resource for a client to access, this is referred to as a shared resource. Shared resources are accessed across the network.
- Because IP telephony networks make better use of available bandwidth, a VoIP network carries voice traffic cheaper than a switched circuit telephone network. In a PSTN, a dedicated end-to-end circuit is allocated for each call. In a VoIP network, data is much more compressed and is carried in packets.
- The ISO developed an architecture that allowed the devices of different manufacturers to work together to communicate with different operating systems. In 1984, it became an international standard known as the OSI reference model. This architecture determines how hardware, software, topologies, and protocols exist on the network and how they operate. The OSI model is based on seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

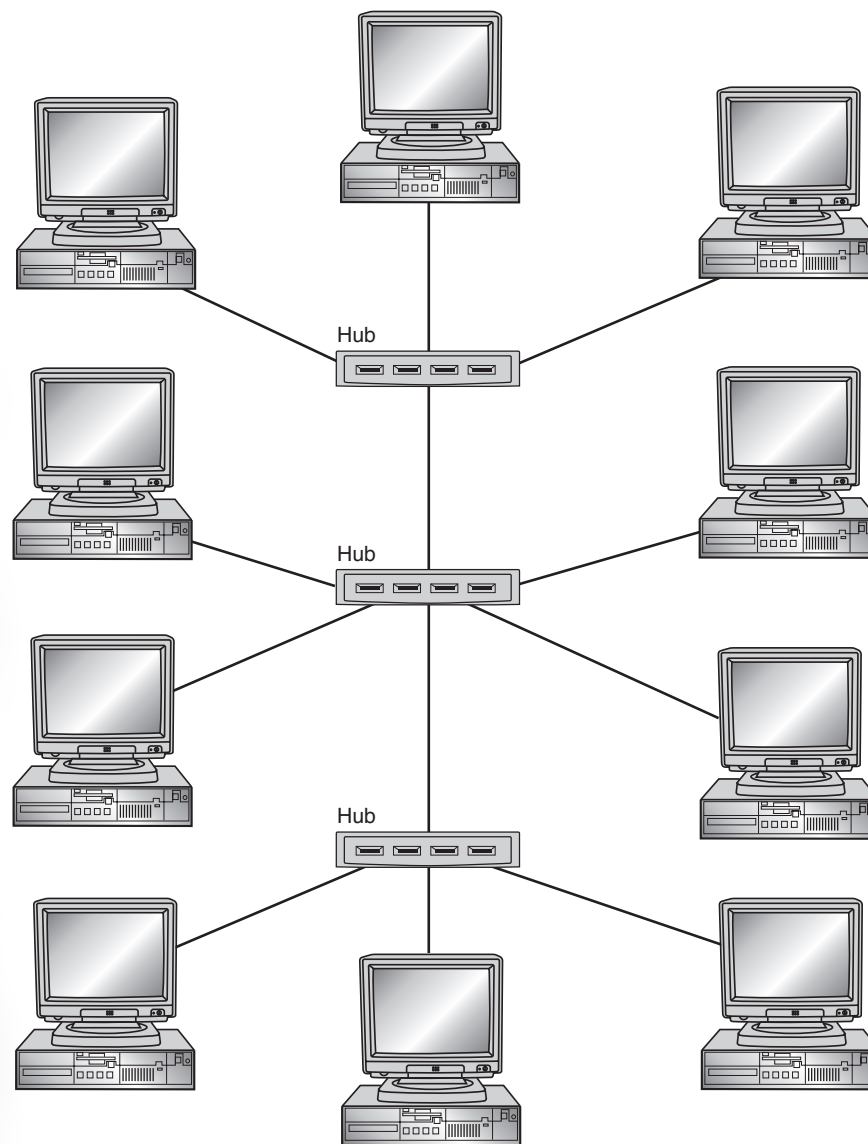


Figure 2.29
A star bus topology

- The Internet was originally called ARPANET. It was developed by the Department of Defense to provide a way to connect networks. The Internet is a network of interconnected, yet independent networks. Each host is directly connected to some particular network. Two hosts on the same network communicate with each other using the same set of protocols that then would be used to communicate with hosts on distant networks. The language of the Internet is TCP/IP.

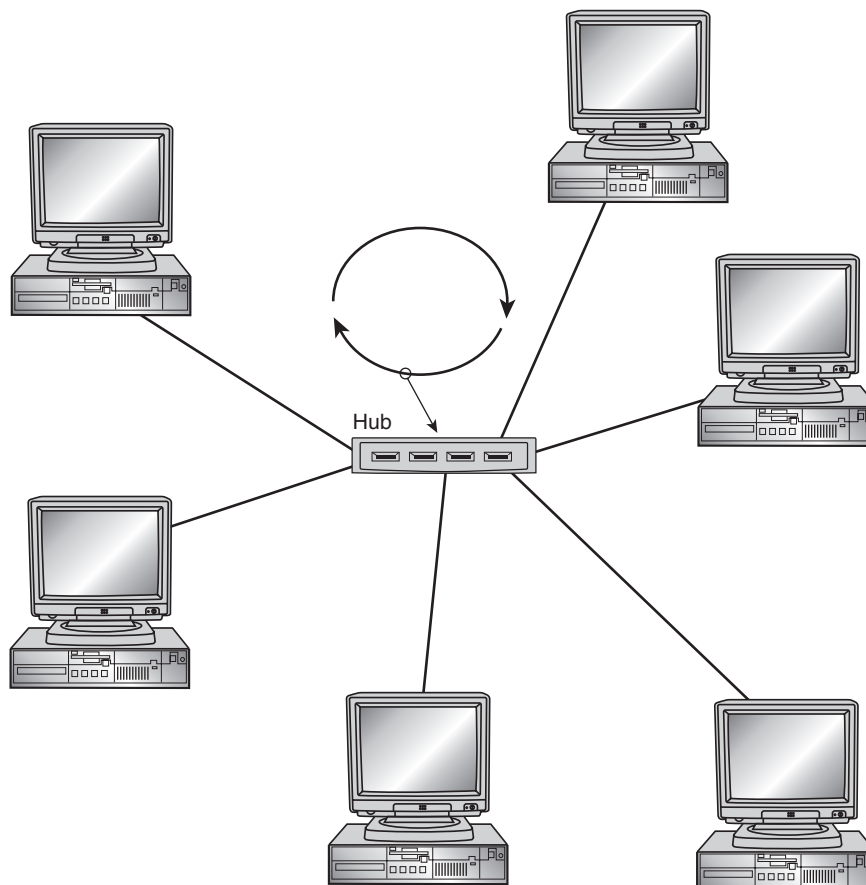


Figure 2.30
A star ring topology

- To deliver new services such as video conferencing and video on demand, as well as to provide more bandwidth for the increasing volume of traditional data, the communications industry introduced ATM technology to provide a common format for services with different bandwidth requirements. ATM uses connection-oriented switches to permit senders and receivers to communicate by establishing a dedicated circuit. In this environment, data travels in fixed 53-byte cells. Five bytes are used for header information, and 48 bytes are used for data. The data transfer rate can reach up to 9953 Mbps.
- Baseband uses a digital transmission pulse at a single fixed frequency. This means that the entire bandwidth of the cable is used to transmit one data signal. It also limits any cable strand to either

half duplex or full duplex. Half duplex means that one transmission takes up the entire bandwidth of the cable. Full duplex uses two strands of cable and two network interfaces: one for sending and the other one for receiving data. Because baseband uses a single fixed frequency, as the signal travels further down the cable, its strength decreases and can distort. Broadband uses analog transmission over a continuous range of values. It travels one way only, in optical waves. It is necessary to have two channels, one for receiving and one for sending data. If the cabling supports enough bandwidth, more than one transmission can operate on a single cable. If this happens, you will need a tuner to pick up the correct signal.

- Coaxial cable was the first type of cable used to network computers and was instrumental in forming the basis of the Ethernet standard. Coaxial cables are made of a thick copper core with an outer metallic shield to reduce external interference. Twisted-pair cable is used in most of today's network topologies. Twisted-pair cabling is either unshielded (UTP) or shielded (STP). Twisted-pair cable comes in seven different categories. Fiber was designed for transmissions at higher speeds over longer distances. It uses light pulses for signal transmission, making it immune to RFI, EMI, and eavesdropping.
- The term *wireless network* refers to technology that allows two or more computers to communicate using standard network protocols, but without network cabling. They are most often referred to as wireless local area networks (WLANs). Wireless networking hardware requires the use of technology that handles data transmission over radio frequencies. The most widely used standard is the IEEE 802.11 standard that defines all aspects of Radio Frequency Wireless networking. Currently, the IEEE standards for wireless are 802.11a and 802.11b.
- A hub is a multiport repeater that retransmits a signal on all ports. When a packet arrives at one port, it is sent to the other ports so that all segments of the LAN can see it. Because it operates at Layer 1 of the OSI model, it can connect segments or a network, but cannot segment a network. A bridge can connect two different types of topologies because it does not understand anything above the Data Link layer. This allows them to move data more rapidly, but it takes longer to transmit because a bridge analyzes each packet. Switches operate at the Data Link layer of the OSI model. Their packet-for-

warding decisions are based on MAC addresses. It looks at each packet and determines from a physical address (MAC address) which device a packet is intended for and switches it out toward that device. Routers operate at the Network layer of the OSI model. They forward information to its destination on the network or the Internet. Routers maintain tables that are checked each time a packet needs to be redirected from one interface to another.

- The physical layout of a network is called the topology, which includes the method of communication. Some of the most common topologies are star, ring, bus, and mesh.

2.9 Key Terms

Application layer: Layer 7 of the OSI reference model. This layer provides services to application processes to ensure that effective communication with other application programs is possible.

Asynchronous Transfer Mode (ATM): A communications services technology that provides a common format for services with high bandwidth requirements, such as video conferencing and video on demand. ATM supports transmission rates up to 9953 Mbps.

attachment unit interface (AUI): A transceiver cable between the medium access unit (MAU) and the data terminal equipment.

backbone: A single cable segment used in a bus topology to connect computers in a straight line.

bus: A major network topology in which the computers connect to a backbone cable segment to form a straight line.

bridge: A device that connects two or more segments of a network to make them one.

client: A computer on a network that requests resources or services from some other computer.

Data Link layer: Layer 2 of the OSI reference model. This layer packages raw bits from the Physical layer into logical, structured data packets.

full-duplex: A transmission method whereby data can be transmitted in both directions on a cable at the same time.

half-duplex: A transmission method whereby data can be transmitted in both directions on a cable but not at the same time.

hub: A multiport repeater that retransmits a signal on all ports.

International Organization for Standardization (ISO): An international standards organization responsible for developing a wide range of standards, including many that are relevant to networking such as the OSI reference model and the OSI protocol suite.

International Telecommunication Union-Telecommunication Standardization Sector (ITU-T): An international organization that develops communication standards. The ITU-T developed X.25 and other communications standards.

Internet Protocol (IP): The Network layer protocol that is part of the TCP/IP suite.

Internet service provider (ISP): An organization that provides Internet access to customers, primarily as a paid service.

Institute of Electrical and Electronic Engineers (IEEE): A professional engineering organization that defines standards for networking devices, which include network interfaces, cabling, and connectors.

Logical Link Control (LLC) layer: A sublayer of the Data Link layer that manages communications between devices over a single link. This layer includes error checking and flow control.

Media Access Control (MAC) layer: A sublayer of the Data Link layer that manages protocol access to the physical network medium.

MAC address: The unique hardware or physical address of a hardware device. Manufacturers assign MAC addresses to hardware devices.

mesh: A hybrid network topology used for fault tolerance in which all computers connect to each other.

network: A group of computers that can communicate with each other so that they can share information.

Network layer: Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two systems. This is the layer at which routing occurs.

network medium: Refers to the cable (metallic or fiber-optic) that links computers on a network. Because wireless networking is possible, it can also describe the type of wireless communications used to permit computers to exchange data via some wireless transmission frequency.

Open Systems Interconnection (OSI) reference model: A hierarchical, seven-layer abstract structure of communications between application processes running in computer systems.

peer-to-peer: A type of networking in which each computer can be a client to other computers and act as a server as well.

Physical layer: Layer 1 of the OSI reference model. It defines mechanical, functional, procedural, and electrical aspects of networking. It includes connectors, circuits, voltage levels, and grounding.

plain old telephone system (POTS): The public telephone system, also known as PSTN.

Presentation layer: Layer 6 of the OSI reference model. It translates data from the Application layer into an intermediary format and provides services such as data encryption, and compresses data.

protocol: A set of rules and conventions that specifically governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.

public switched telephone network (PSTN): See plain old telephone system (POTS).

quality of service (QoS): A standard that specifies the time frame in which data will be delivered after transmission. QoS helps control jitter, latency, and loss for long-distance, high-bandwidth applications.

repeater: A device that regenerates electronic signals so that they can travel a greater distance or accommodate additional computers on a network segment.

resources: The files, applications, and hardware that are shared by the server for the client to access.

ring: Topology consisting of computers connected in a circle, forming a closed ring.

routers: A device that passes data on from one network to another.

server: A computer whose job is to respond to requests for services or resources from clients elsewhere on a network.

Session layer: Layer 5 of the OSI reference model. It allows two applications on different computers to establish dialog control, regulates which side transmits, and determines the time and length of the transmission.

star: A topology in which the computers connect via a central connecting point, usually a hub.

star bus: A network topology that combines the star and bus topologies.

star ring: A network topology wired like a star that handles traffic like a ring.

switch: A special networking device that manages networked connections between any pair of star-wired devices on a network.

terminator: A device used to absorb signals as they reach the end of a bus, thus freeing the network for new communications.

token: A packet used in some ring topology networks to ensure fair communications between all computers.

token passing: A method of passing data around a ring network.

topology: The basic physical layout of a network.

Transmission Control Protocol (TCP): The Transport layer protocol that's part of the TCP/IP suite.

Transmission Control Protocol/Internet Protocol (TCP/IP): The language of the Internet. This is a suite of protocols that enables packets to be routed across many networks to arrive at their destination.

Transport layer: Layer 4 of the OSI reference model. It helps provide a virtual error-free, point to point connection so that communication between two hosts will arrive un-corrupted and in the correct order.

wireless network: XXX

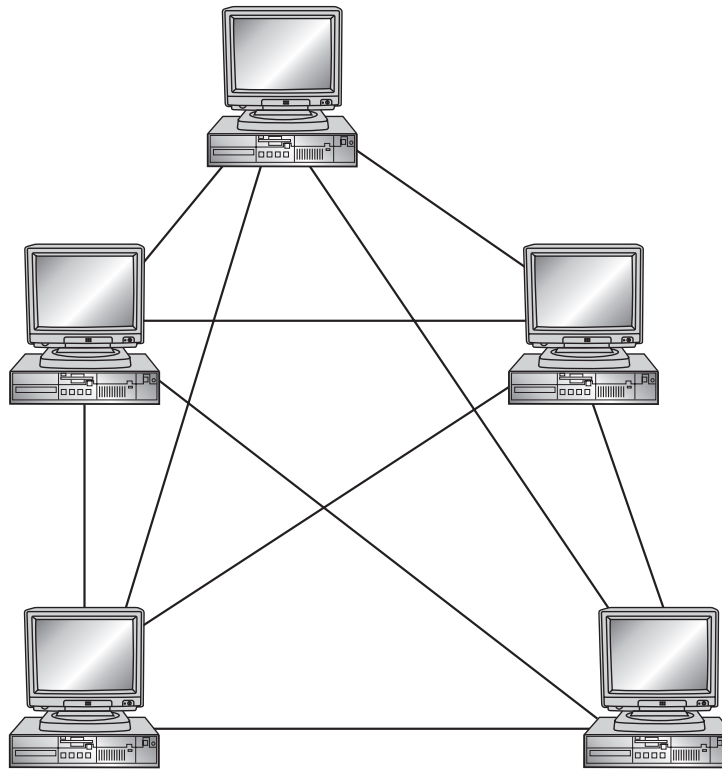
2.10 Challenge Questions

- 2.1 Match the layers of the OSI reference model with their appropriate function.
- Physical ___ Provides error-free packet delivery
 - Data Link ___ Establishes responses between applications
 - Networking ___ Deals with mechanical and electrical communications
 - Transport ___ Formats, encrypts, and compresses data

2.10 Challenge Questions

111

- e. Session ___ Determines routes and addressing
 - f. Presentation ___ Provides user access to the environment
 - g. Application ___ Packages bits into data
- 2.2 A(n) _____ accesses shared resources on a network.
- a. server
 - b. dumb terminal
 - c. client
 - d. server
- 2.3 ATM is based on _____.
- a. dynamic 64-byte packets
 - b. fixed 53-byte cells
 - c. fixed 64-bit cells
 - d. none of the above
- 2.4 Which of the following are considered an advantage of peer-to-peer networking? (Choose all that apply.)
- a. A network administrator is needed to install and configure a peer-to-peer network.
 - b. Peer-to-peer networking is inexpensive to purchase and operate.
 - c. Individual users control their own shared resources.
 - d. Individual machines depend on the presence of a dictated server.
- 2.5 Telephony networks are based on _____.
- a. packet switching
 - b. circuit switching
 - c. data switching
 - d. packet filtering
- 2.6 Which type of network topology is depicted in the following figure?



- a. Star bus
 - b. Star ring
 - c. Hybrid
 - d. Mesh
- 2.7 Which of the following is not an advantage of the ring topology?
- a. All computers have equal access to the rest of the network.
 - b. Even with many users, network performance is consistent.
 - c. A single computer failure can impact the entire network.
 - d. None of the above.
- 2.8 Which of the following is not an advantage of the bus topology?
- a. It is simple and reliable.
 - b. Its cabling is inexpensive and easier to work with.
 - c. Any cable can bring the network down.

2.11 Challenge Exercises

113

d. All computers are arranged in a line and use cables economically.

2.9 Which type of cable is depicted in the following figure?



- a. Coax
- b. Fiber
- c. UTP
- d. STP

2.10 The layout of a computer network is known as its _____.

2.11 A(n) _____ absorbs all signals that reach it, clearing the network for new communications.

2.12 A small packet, called a(n) _____, passes around the ring to each computer in turn.

2.13 Describe the purpose of a switch.

2.14 Describe the purpose of data sharing.

2.15 Describe the components that are necessary for two computers to communicate with one another.

2.11 Challenge Exercises

Challenge Exercise 2.1

In this exercise, you make a patch cable. You should know how to do this for several important reasons. You will better understand how cabling works, you will learn how to test cabling, and you will be able to make your own cables if you are ever in a bind. You need UTP cable, RJ-45 connectors, a crimper, scissors, and a cable tester.

To make a patch cable:

1. Cut the UTP cable to a desired length.
2. On one end of the cable, using the stripper on the crimper or a pair of scissors, strip about 1 inch of the outside plastic coating from the cable. Only strip the outside plastic coating from the

wire; do not strip the plastic coating off the inside wires. Network cabling is different than audio cabling. When stripping the coating, be careful not to cut through the copper wires. Sometimes it is better to use scissors than the stripper on the crimper because you have better control over the process.

3. Arrange the wires based on the color of the coating on the wires. Start at one end of the cable and arrange them in this sequence: orange/white, orange, green/white, blue, blue/white, green, brown/white, brown. Carefully trim the ends so they are even.
4. Insert an RJ-45 connector over the wires, pushing them to the end of the connector. Hold the connector such that you can see whether the ends of the wire are touching the top of the connector. It is important that the wires touch the top of the connector, otherwise the cable might not work.
5. Crimp the connector.
6. Repeat steps 1 through 5 on the opposite end of the UTP cable.

To test a patch cable:

Each cable tester has different settings to test a cable. Your instructor will help you make sure that the tester is set to the right specification. After this is completed, insert one end of the cable into the larger part of the tester and the other end of the cable into the smaller end of the tester. Check to be sure that all wires go straight through and that the cable is good.

Challenge Exercise 2.2

In this exercise, you make a crossover cable. You need UTP cable, RJ-45 connectors, a crimper, scissors, and a cable tester.

To make a crossover cable:

1. Follow steps 1 through 3 in Challenge Exercise 2.1.
2. Arrange the wires based on the color of the coating of the wires. Start at one end of the cable in this sequence: orange/white, orange, green/white, blue, blue/white, green, brown/white, brown. Carefully trim the ends so they are even.
3. Arrange the wires on the other end of the cable in this sequence: green/white, green, orange/white, blue, blue/white, orange, brown/white, brown. Carefully trim the ends so they are even.

4. Insert a RJ-45 connector over the wires, pushing them to the end of the connector. Hold the connector such that you can see whether the ends of the wire are touching the top of the connector. It is important that the wires touch the top of the connector, otherwise the cable might not work.
5. Crimp the connectors.

To test a crossover cable:

[INSERT G, missing]

5 lines

x

x

x

Challenge Exercise 2.3

In this exercise, you learn to punch down cable to a patch panel and a RJ-45 jack. You need Cat5 cable, a patch panel, a punchdown tool, and a RJ-45 jack.

1. Cut the UTP cable to a desired length.
2. On one end of the cable, using the stripper on the crimper or a pair of scissors, strip about 1 inch of the outside plastic coating from the cable. Only strip the outside plastic coating from the wire; do not strip the plastic coating off the inside wires.
3. Arrange the wires on one end of the cable in the sequence indicated in the specifications located on the back of the patch panel or in the documentation that accompanied the patch panel. Using the punchdown tool, carefully punch the ends into the panel.
4. Arrange the wires on the other end of the cable according to the specifications that accompany the jack. Using the punchdown tool, carefully punch the ends into the panel.

Challenge Exercise 2.4

In this exercise, you connect a computer to a patch panel with cables. You need two patch cables, a hub or switch, and a desktop PC or laptop with a NIC installed.

1. Attach one end of a patch cable to the NIC in the computer.
2. Take the other end of the patch cable and attach it to the RJ-45 jack.

3. Take the second patch cable and attach it to the patch panel.
4. Use the second end of the patch cable to attach to the patch panel.

Challenge Exercise 2.5

In this exercise, you tour an existing network and examine the components, such as topology, media, and hardware. Your instructor has arranged a tour of the school network or the network of a nearby business. During the tour, determine the following:

- What type of topology is used?
- What type of cabling is used?
- How many routers, switches, and hubs are used?
- How many computers are attached to the network?
- Is it a client/server or peer-to-peer network?
- How do users access the Internet?

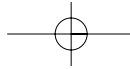
2.12 Challenge Scenarios

Challenge Scenario 2.1

Acorn Music company occupies four buildings in your city for administrative offices, a warehouse, a record shop, and a multimedia studio. Currently, Acorn has some stand-alone computers but no network. Over the next two months, Acorn plans to implement a network linking all the offices and has asked you to help design it. There are plans for a total of 50 computers at all four sites. Security is not an issue, and the users are fairly computer savvy. What type of network should be installed and why?

Challenge Scenario 2.2

Evergrow, a large, multinational company, is currently running a peer-to-peer network at each of its 60 sites. The sites are not currently connected, but Evergrow is planning to do so. To keep costs low, management would like to continue to use the peer-to-peer network. However, as the sites are linked together, data will be shared between the users, making security a high priority. Should the company continue to use peer-to-peer networking? Why or why not?



2.12 Challenge Scenarios

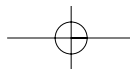
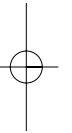
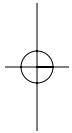
117

Challenge Scenario 2.3

There are 17 computers in Mr. Green's office. They are spread out over three floors of a single building. Each floor has a central telephone room with access to the other floors. You have been asked to connect the computers in a peer-to-peer network. What type of network topology should you implement?

Challenge Scenario 2.4

You are setting up a workgroup for your department, which has seven computers, two printers, and one scanner that need to be connected. All equipment is on one floor and located relatively close to each other. Costs must be kept at a minimum, and the network doesn't need to be especially fast. What type of cable would you recommend and why?



CHAPTER 2

Answer Key

Answers to Challenge Questions

1. Match the layers of the OSI reference model with their appropriate function:
 - a. Physical
 - b. Data Link
 - c. Networking
 - d. Transport
 - e. Session
 - f. Presentation
 - g. Application
 - d. Provides error-free packet delivery
 - e. Establishes responses between applications
 - a. Deals with the mechanical and electrical communications
 - f. Formats, encrypts, and compresses data
 - c. Determines routes and addressing
 - g. Provides user access to environment
 - b. Packages bits into data
2. c
3. b
4. b
5. d
6. d
7. c
8. c
9. d
10. topology
11. terminator
12. token

13. A switch allows a network to be segmented, thereby increasing the amount of bandwidth that goes to each device. As a result, computers can exchange data at the rated bandwidth for the medium in use rather than dividing it among the computers.
14. Data sharing allows resources such as data, applications, or hardware to be used by more than one person, providing corroboration and cost efficiency.
15. For computers to communicate, they need a network medium (such as cabling), a method of communicating, and a device for communication (such as a NIC).

Discussion of Challenge Exercises

Challenge Exercise 2.1

In this exercise, students work with media and learn the importance of proper pin-out and connectivity. This should be a fun exercise although some students might get frustrated because its not always easy to get the wires to stay straight as they put them into the connector, but it's worth it when they actually make a good cable.

Challenge Exercise 2.2

In this exercise, again, students work with media and learn the importance of proper pin-out and connectivity. This exercise can lead to questions from the students on how to network their home computers. Of course, they won't be able to do so until they learn about IP addresses, but it does get them thinking about it and asking questions. It also gives them a sense of accomplishment. They can now make a regular patch cable as well as a crossover cable.

Challenge Exercise 2.3

In this exercise, students work with common network equipment and learn the importance of wiring in network and phone connectivity. Some students might get frustrated when trying to get the wires to punch down correctly, and they actually have to map the wires to the color scheme.

Challenge Exercise 2.4

In this exercise, students learn how data gets from place to place in a network. This should prepare them for the scenarios. Many times, students get

lost when designing a network and do not think about how communication actually happens.

Challenge Exercise 2.5

Because the scenarios are about network planning, this exercise gives the students a chance to see how a running network is set up. It also allows them to see actual equipment rather than pictures in a book. It should reinforce what they learned in the previous exercises.

Option: If you cannot arrange a tour of the school network or a local business, see if you can arrange a guest speaker to come in and talk about their network.

Discussion of Challenge Scenarios

Challenge Scenario 2.1

There are two factors to consider:

1. How to link the buildings
2. How to link the computers inside each building

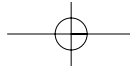
To link the buildings via the ground, fiber is recommended as the preferred media. It can go long distances and has high resistance to outside interference as well as good bandwidth.

To link the computers inside the offices, peer-to-peer would be recommended because security is not an issue and all the users are computer savvy so an administrator is not needed. The layout should be a star with UTP as the cabling choice.

Challenge Scenario 2.2

Currently, there are 60 sites, and as they grow they will become impossible to manage individually. As each site grows individually, they will outgrow the capability to keep the peer-to-peer networking. Security is an issue. In a peer-to-peer environment, everyone acts as an administrator. Therefore, little security or control exists.

The cost of switching to a server-based network would be less costly than not being able to operate properly because the current network structure has outgrown its limits.

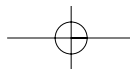
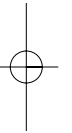


Challenge Scenario 2.3

Because each floor has a telephone room with access to the other floors, a star-bur type topology would work best. This allows each floor to have its own hub with the hubs then connected together. Depending on the bandwidth of the hubs, either 10Base2 or UTP could be used to connect the hubs, and UTP would be used to connect the computers to the hubs.

Challenge Scenario 2.4

Because all the devices are relatively close to each other and are on one floor, a bus with 10Base2 cabling would work. It would be inexpensive to implement and maintain.



0 F
1 A
2 9
3 G
4 0
5 A
6 3
7 2
8 K
9 V
0 8
1 7
2 A
3 D
4 9
5 0
6 1
7 N
8 A
9 D
0 F
1 8
2 9
3 7
4 L
5 K
6 1
7 8
8 7
9 0
0 9
1 8
2 8
3 2
4 4
5 F
6 7
7 6
8 A
9 S
0 D
1 0
2 9
3 8
4 7
5 F
6 1
7 2
8 K
9 9
0 2
1 A
2 S
3 F

