part III

Networking Fundamentals

Back in the twentieth century, networking was a highly technical endeavor that most users happily let their network administrator perform for them. The rollout of digital television and the growing popularity of media center PCs are creating a new perspective on networking. Circuit City, Radio Shack, Best Buy, Sears, and Wal-Mart sell Ethernet hubs and wireless media center devices at mass market prices. Because of the mass market appeal of local area networking, end users want to network digital media devices throughout the home. This retail market makes all the more relevant this book's third and final part, which is devoted to networking. The hands-on exercises provide skills that you can use not only in the workplace, but also on digital devices throughout the home.

Students who are preparing for the CIW Foundations exam need not worry that this part of the book is all fun and games. To the contrary, all of the CIW objectives are covered, and the end-of-chapter materials contain practice tests that will help you prepare for the exam.

After covering general networking principles in Chapter 10 and Internetworking in Chapter 11, Chapter 12 contains a tutorial on providing database access over a network. Then Chapter 13 rounds things out by covering network security. The book concludes by stepping you through the process of publishing a Web site securely and providing access only to authorized users.

chapter 10

Introduction to Networking

"This is the power of the network. Now."

—*Cisco slogan from www.cisco.com*

In this chapter, you will learn how to:

- Define the term *networking* and list the three critical components that must be present in a network.
- Define the five networking topologies used in describing the physical layout or shape of a network.
- Define the seven layers in the OSI Reference Model and identify the networking protocol suites that follow it.
- Describe the difference between a local area network (LAN), metropolitan area network (MAN), and a wide area network (WAN).
- Define the physical network components that LANs, MANs, and WANs comprise.

NETWORKING has a fascinating history that chronicles the invention of the technologies that power the Internet. Back in the 1950s, for example, people did not have personal computers. To use a computer, you had to go to the computing center and wait your turn at the card reader to feed in a deck of cards upon which you had typed your script using a keyboarding device called a *keypunch*. Compare this early technology to today's network, over which wireless devices enable people to work productively almost everywhere they go. During the transition from punched cards to ubiquity, the field of computing evolved through four functional stages of networking. This chapter introduces networking by defining these four networking models, all of which are in use today.

Another way of defining networks is to classify the geographical shapes that form when you connect computers in different physical arrangements. So far, the field of computer networking has evolved five distinct geographical network topologies. This chapter defines, diagrams, and explains them.

For computers to exchange data meaningfully, they must use a communications protocol that defines how the data flows. Most of the world has adopted an international standard for networking that is called the **OSI Reference Model (OSI/RM)**. After describing how data flows across the network in packets created according to the OSI/RM, this chapter concludes by presenting the physical hardware devices and transmission media that create the local and wide area networks over which these packets flow.

Understanding Networks

A **network** is the connection of two or more digital devices for the purpose of communicating, transferring, or obtaining data. In order to have a network, you must have three things that are characteristic of all networks. First, there must be a physical connection through which the data will flow. Second, there must be a set of communication rules called *protocols* that the networked devices use to communicate. Third, there must be one or more network services that will receive these communications and respond by providing the informational resources that are the reason why you want to create a network in the first place.

The act of communicating over a network is called **networking**. Advances in microelectronics enable networking to encompass a wide range of devices. Figure 10-1 illustrates how these devices can include network-ready home appliances as well as more traditional computing equipment.

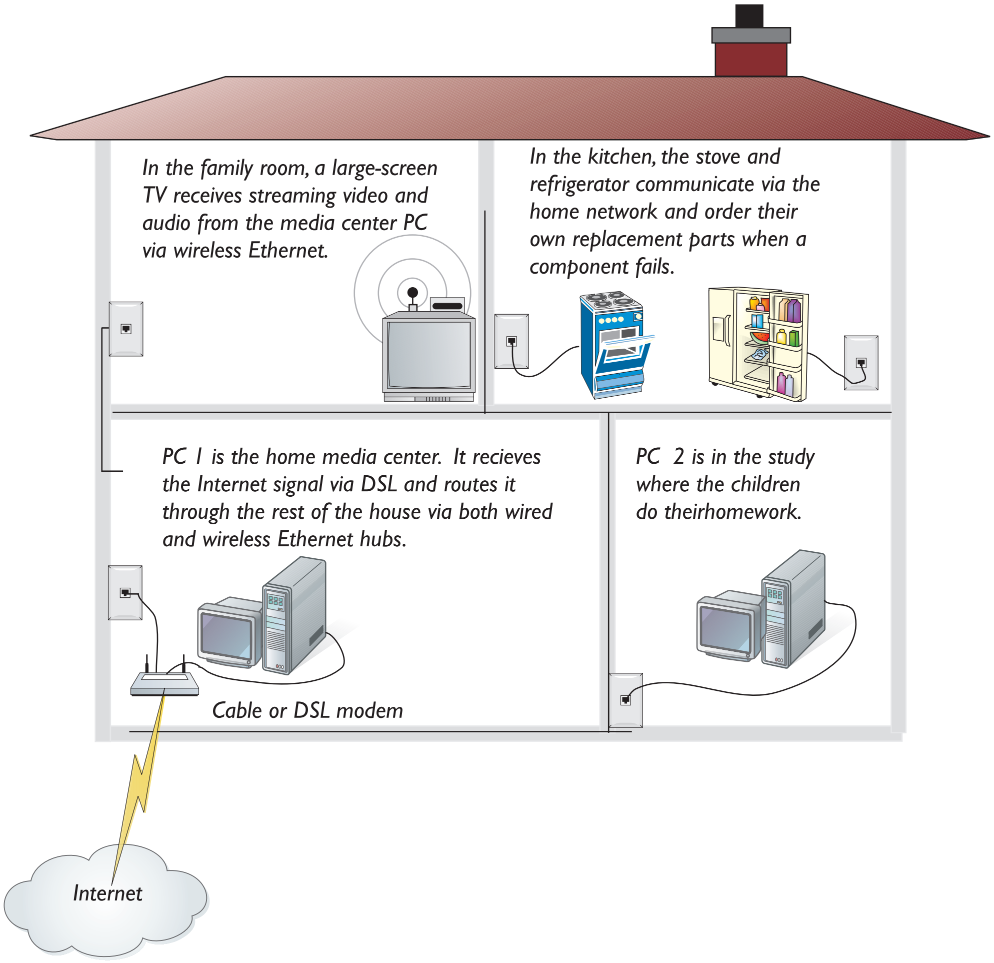

In the family room, a large-screen TV receives streaming video and audio from the media center PC via wireless Ethernet.
In the kitchen, the stove and refrigerator communicate via the home network and order their own replacement parts when a component fails.
PC 1 is the home media center. It recieves the Internet signal via DSL and routes it through the rest of the house via both wired and wireless Ethernet hubs.
PC 2 is in the study where the children do theirhomework.
Cable or DSL modem
Internet

FIGURE 10-1 Any device that contains a Network Interface Card (NIC) and follows the applicable protocol can communicate over the network and provide or receive services, depending on its role. Such devices include common household appliances with built-in NICs.

Mainframe/Terminal Model

When networking started, computers were large and expensive. They cost so much and required so much maintenance that you didn't even think about owning your own. Instead, you connected via the **mainframe/terminal model**, which Figure 10-2 illustrates. A **mainframe** is a centralized computer to which users connect in order to obtain network services. The **terminal** is a device with a keyboard upon which you type commands or enter data to communicate with the mainframe computer. The first terminals were typewriter-style devices that had no built-in intelligence, which is why they are often referred to as *dumb terminals*. Eventually, terminals got display screens and were called *graphics terminals*. The addition of computer chips created so-called *smart terminals*, which had some processing power but could not function on their own as stand-alone computers. Terminals that contain their own central processing unit (CPU) became known as *intelligent terminals*. Today, you can run terminal emu-

note *Since there is only one computer, this mainframe/terminal model can create bottlenecks. The single point of failure adversely affects every user if the mainframe goes down. Due to these vulnerabilities, the mainframe/terminal model is declining in popularity, although many large companies continue to operate legacy mainframe computers.*

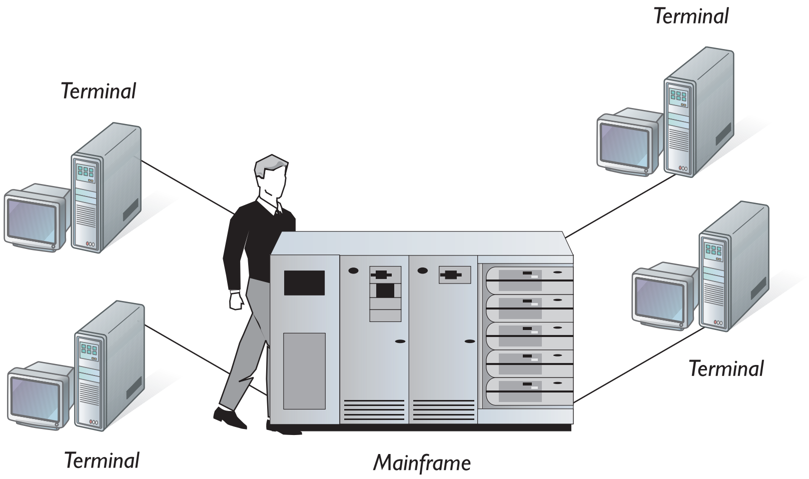


FIGURE 10-2 *In the mainframe/terminal model, users compete for resources on a centralized computer that uses time-sharing to allocate computing cycles to each user.* ■

lation software on personal computers whenever you need to connect to a legacy mainframe computer in terminal mode.

Client-Server Model

A more efficient way of distributing networked resources is the client-server model. As you learned in Chapter 1, the term **client-server** refers to the manner in which computers exchange information by sending it (as servers) and receiving it (as clients). Some computers are dedicated servers. A file server, for example, is dedicated to storing files that authorized users can upload or download via the network. A print server provides network access to one or more printers. A database server processes queries that retrieve or store information in a database. A network server manages network traffic.

Other computers serve multiple purposes. On a small network, for example, one computer can function as a file server, a print server, and a database server. Even workstations that are used primarily as clients can run network services. An end user who wants to permit other users to upload or download local files, for example, can run an FTP server that exposes certain folders to authorized users over the Internet. You will learn how to run an FTP server in Chapter 11, which is devoted to Internetworking.

The most strategic aspect of client-server computing is the manner in which computers can serve dual roles as both servers and clients. Figure 10-3 illustrates how this dual role enables the creation of multi-tier networks in which one server can become a client in order to request something from another server. This enables large organizations to subdivide complex applications into multiple stages called *tiers*. **Multi-tier** computing typically includes three tiers consisting of (1) the user interface tier, (2) the business tier, and (3) the database tier.

Figure 10-3 shows end users connecting to a Web application running on the business tier that serves the end-users. When the Web application requires information from the corporate database, however, the business

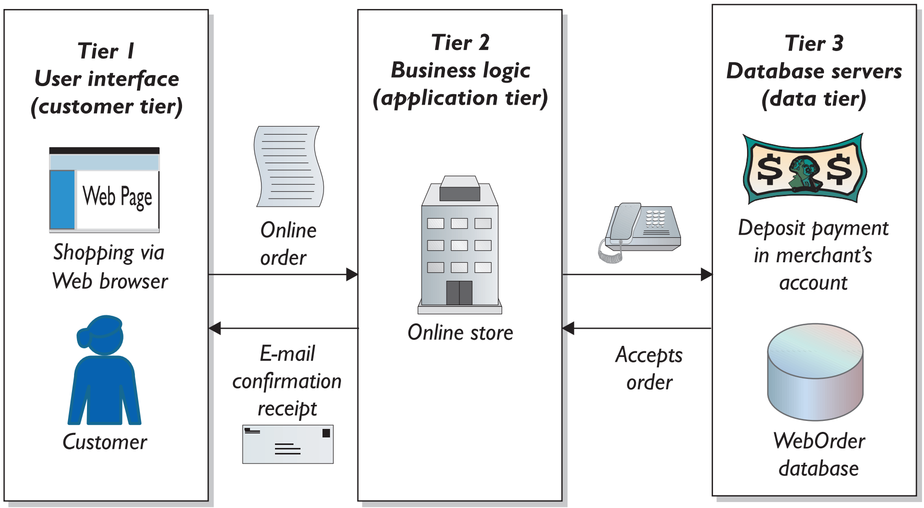


FIGURE 10-3 *In multi-tier computing, mid-level computers perform the dual role of client and server. Pictured here is the classic e-commerce model in which end users connect to a Web application running on the business tier that serves the end users.* ■

tier becomes a client that issues a query against the database service running on the data tier. In large operations, more than one mid-level computer can share the responsibility for serving end users. Similarly, the data tier can distribute a large database over multiple computers known as a *server farm*.

Peer-to-Peer Model

In a LAN, **peer-to-peer (P2P)** is a network architecture in which each workstation has equal responsibilities. No dedicated server is in charge of managing a P2P network. In a home or small office environment, P2P is a simple way to set up a network that can share digital resources throughout the LAN. On larger networks under heavy loads, however, P2P does not perform as well as client-server networks, which do a better job of balancing and managing network traffic.

Out on the Internet, the term *P2P* refers to a form of peer-to-peer file sharing brought to public attention by the controversy over music file sharing. Figure 10-4 illustrates that no dedicated server is in charge of managing a P2P file-sharing environment. Because no one is in charge, the music industry finds it difficult to identify users who violate the law by using P2P file sharing to distribute copyrighted music over the Internet.

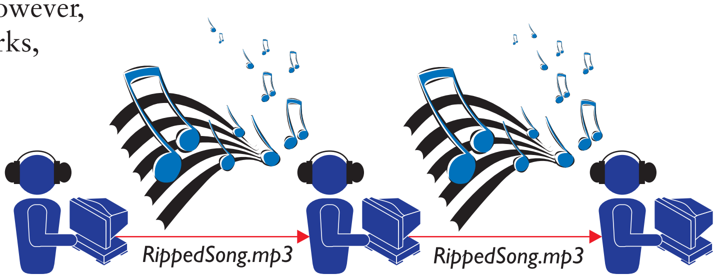


FIGURE 10-4 *In a peer-to-peer (P2P) network, workstations have equal responsibility for sharing files and accessing services on each other's computers. In the music industry, this absence of authority makes it difficult to identify and prosecute copyright infringers who share copyrighted music via P2P file sharing without permission.* ■

Enterprise Model

The term **enterprise model** refers to networking within large organizations that dedicate entire servers to handling important tasks in the most efficient manner. A large organization, for example, may need individual servers dedicated to the tasks of serving mail, hosting databases, managing security, and routing network traffic. Figure 10-5 shows that an enterprise network can include a large mainframe computer, which is front-ended by network servers that provide access to authenticated users. Within a large organization, individual departments may have minicomputers, which are smaller than mainframes but larger than individual workstations. As microelectronic technology continues to progress, the distinctions among mainframes, minicomputers, workstations, and personal computers begin to blur. The least expensive PC you can buy today, for example, dwarfs the early mainframes.

Push vs. Pull Technology

There are basically two ways to receive information from a network. Either you ask for it, and the information appears on demand each time you request it; or you subscribe to an information service, which provides you with the information automatically when the data becomes available. The computer industry uses the **push-pull metaphor** to distinguish between these two ways of receiving information.

When you browse the Web and click hyperlinks that bring requested resources onscreen, for example, you are pulling the information toward you. Thus, hyperlinks are an example of pull technology. If you install onto your computer a stock-monitoring client, on the other hand, financial news and stock prices scroll onscreen as the server pushes information onto your computer. Another application of push technology is automatic software and document updating, as exemplified by BackWeb's Polite Sync Server at www.backweb.com/products/html/psstech.html.

Push technology can also be used to broadcast important messages to network users. In a weather emergency, for example, a Windows network administrator can use the "net send" feature to push a warning message onto each logged-on worker's screen. Users who want to monitor the weather continuously can download the WeatherBug from www.weatherbug.com. The current temperature displays on the Windows status bar, and impending weather emergencies push warnings onto your screen.

Network Operating Systems

A **network operating system** is the software that adds to a computer the functions required for connecting computers together for the purpose of networking. The most popular network operating systems are Microsoft Windows, UNIX, Linux, the Mac OS, and Novel NetWare.

Microsoft Windows

The most widespread network operating system is Microsoft Windows. No matter what version of Windows you have, certain networking components are built right in. Every Windows user, for example, has the capability to use the NetBEUI, IPX/SPX, and TCP/IP protocols that are discussed later in this chapter. Not all versions of Windows, however, enable you to run certain

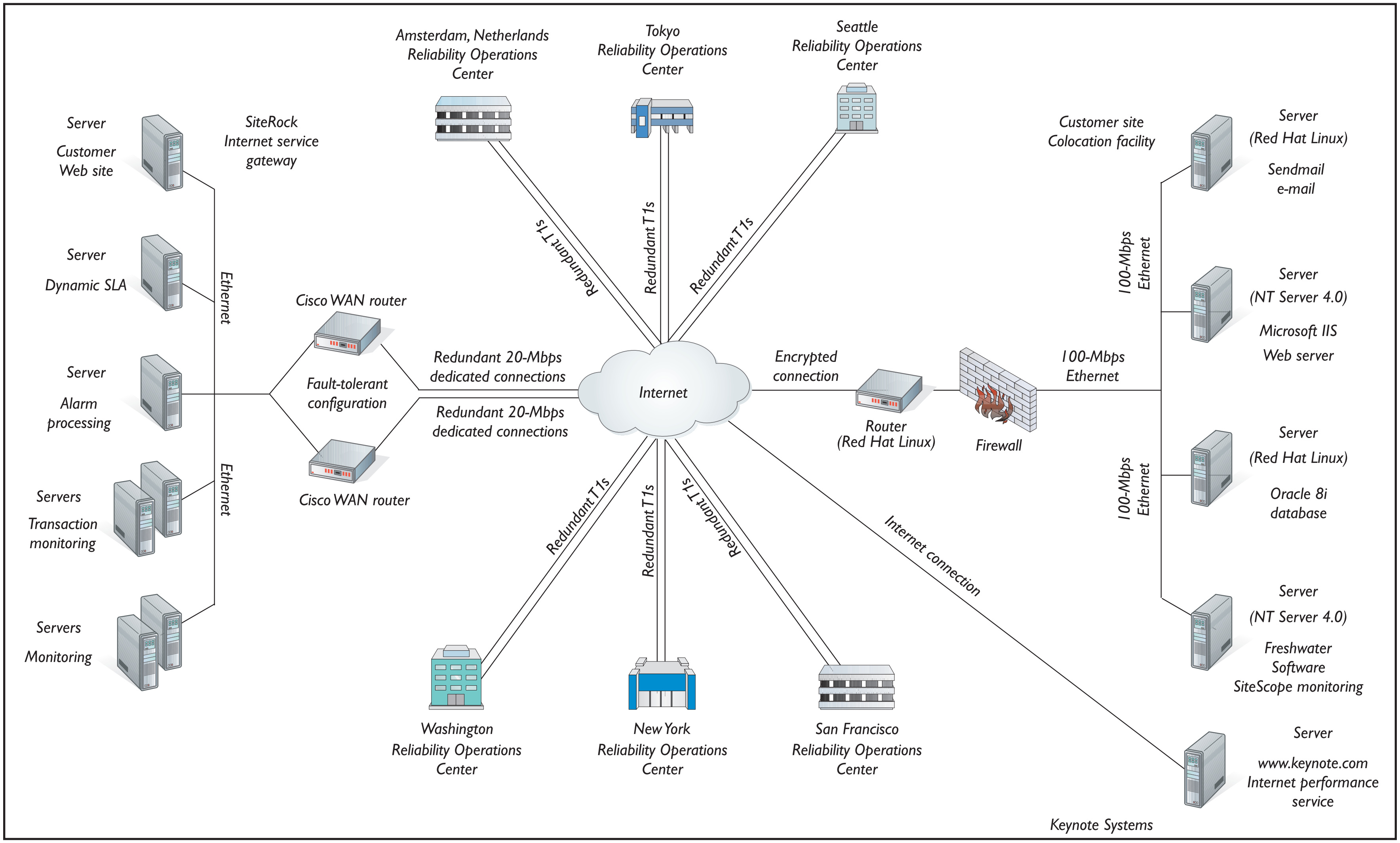


FIGURE 10-5 *The enterprise model pulls out all the stops as large organizations combine different networking strategies to accomplish computing tasks efficiently. The network shown here has a legacy mainframe system front-ended by network servers that communicate with departmental minicomputers and local area networks that are primarily client-server based, although small groups use peer-to-peer networking to share files efficiently among team members.* ■

networking services. Internet Information Services (IIS), which is the Windows Web application server, for example, does not come with every version of Windows. Windows XP Home Edition users, for example, cannot install IIS. Windows XP Pro, on the other hand, comes with IIS, as does the complete line of Windows Server products, including Windows NT, Windows 2000, and Windows 2003, which can host mail, news, directory, catalog, and transaction services. To find out which versions of Windows support which server products, go to the history of Windows Server products at www.microsoft.com/windows/winhistoryserver.mspx.

UNIX and Linux

The **UNIX** and **Linux** operating systems support the full range of networking services, including both client- and server-side components. Bell Labs invented UNIX in the early 1970s. Because UNIX was distributed in C source code, C programmers could modify the operating system, and many different versions of UNIX began circulating. In the 1980s, AT&T worked to create a standardized version of UNIX. Today, The Open Group holds the trademark and defines the official version of UNIX at www.unix-systems.org.

Developed by Linus Torvalds, Linux is an open source operating system that mimics the form and function of UNIX on an independently developed platform. The general public license permits anyone with the necessary technical skills to download and modify the Linux source code. As you have probably noticed in recent television commercials, IBM is touting Linux as an alternative to the Windows operating system for e-commerce solutions. To learn more about Linux, go to www.linux.org.

Mac OS

Another operating system that has networking built in is the **Macintosh OS X** operating system. According to Apple, OS X is the most widely distributed UNIX-based operating system. In other words, behind the Macintosh user interface, OS X is based on a UNIX environment. To learn more about the OS X implementation of UNIX, go to www.apple.com/macosx/features/unix.

Novell NetWare

Developed by Novell Corporation, **NetWare** is a PC-based local area networking product that was one of the most dominant network operating systems during the decade following its invention in 1983. Microsoft's release of Windows NT in 1993, however, created overwhelming competition. Nevertheless, Novell still markets NetWare and has added support for the Apache Web server, the database engine MySQL, the scripting languages Perl and PHP, and the Jakarta Tomcat container for Java servlets and Java Server Pages (JSP). For more information, go to www.novell.com/products/netware.

Classifying Network Topologies

A popular way of classifying networks is to describe the different kinds of geographical configurations that form when computers get connected for the purpose of networking. A network's geographical shape is referred to as the network's **topology**. The five kinds of network topology are (1) bus topology, (2) ring topology, (3) star topology, (4) hybrid topology, and (5) mesh topology.

Bus Topology

The **bus topology** has a single cable, called the **bus** or the **trunk**, to which every device on the network connects. Figure 10-6 shows that you can connect a wide range of devices to the bus or trunk, which is a coaxial cable. The fittings and connectors are similar to those used in cable TV. Like a cable TV signal, information on the bus travels in both directions along the entire length of the cable. To prevent the signal from feeding back when it reaches the end of the line, each end of the bus has a terminator that absorbs the signal.

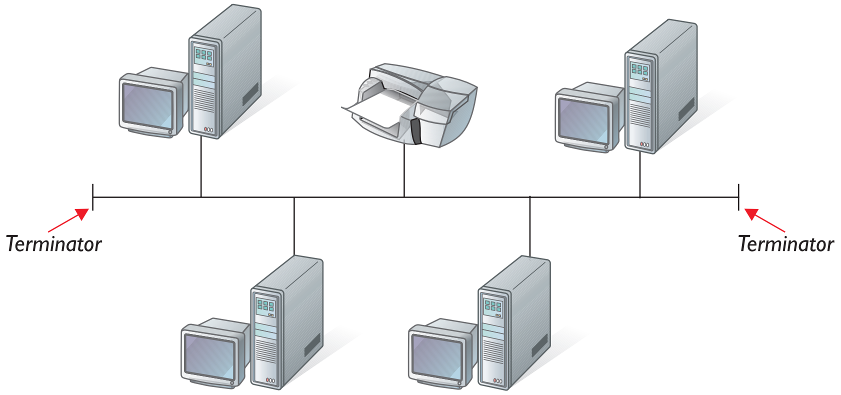


FIGURE 10-6 *The bus topology uses a single cable, called the bus or trunk, to connect every device on the network. The bus uses coaxial cable that is inexpensive and easy to install, although a break anywhere along the cable causes all network traffic to stop.* ■

All of the messages on the bus pass by each device, or node, on the bus. Each device examines all of these messages, acts on the ones intended for that node, and ignores the others. The advantage of this design is its simplicity. The bus is inexpensive and easy to install. If a break occurs anywhere on the cable, however, all network traffic stops. Such a problem can be troublesome to correct because the break may be hard to find, especially if the bus is long and has many devices connected to it. Another disadvantage is that the speed of the bus declines as network traffic increases.

Ring Topology

Figure 10-7 shows how the **ring topology** takes its name from the loop that forms when you connect a network's nodes in a circle. Messages flow in a

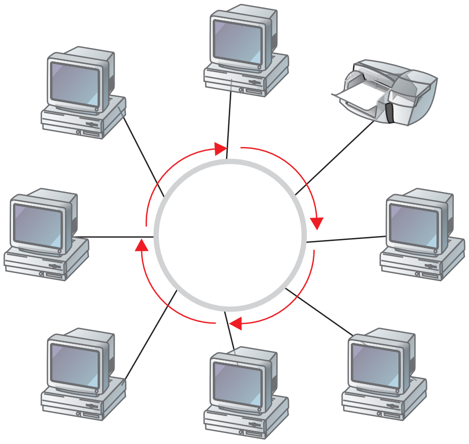


FIGURE 10-7 *The ring topology takes its name from the loop that forms when you connect the network's nodes in a circle. Messages flow in one direction around the ring, as does a token that provides each device its turn to communicate. Because the token enables the network to avoid data collisions, the ring topology is not as prone to slowdowns as networks that must cope with data collisions as traffic increases.* ■

note *Token ring networks can run extremely fast. My workplace at the University of Delaware (UD), for example, has a 10 gigabyte per second ring that runs from UD, to Philadelphia, to Wilmington, and back to UD. This network significantly increased UD's bandwidth at a lower cost than the university was paying previously.*

single direction around the ring. Each device acts on the messages addressed to it and passes the rest of the messages onto its neighbor. If a message comes all the way back around to the sender without being acted upon, the message is discarded.

Most rings use a small piece of data called a *token* to give every node an equal chance at obtaining bandwidth from the network. The token circles the ring continually as it passes from node to node. A device can communicate over the network only when it has the token. The advantage of this token ring design is that each node on the network gets an equal share of the bandwidth, and as traffic increases, the ring does a very good job of continuing to run fast by avoiding the data collisions that can slow down other types of networks. An obvious disadvantage of the ring topology is that the network stops working if one of the nodes fails and stops sending the data to its neighbor.

Star Topology

In a **star topology**, each device in the network connects to a central hub, which distributes messages from one node to another. As illustrated in Figure 10-8, one of the disadvantages of the star is that if the central hub fails, the central point of failure makes the network stop working. Stars also require more cabling than bus or ring topologies.

The advantages of a star topology are (1) centralized control, which makes the network easier to maintain and control; (2) easy expansion, which enables you to add a new device without affecting the rest of the network; and (3) fault tolerance, which enables the network to keep functioning if a node stops working, or if you disconnect a device to reconfigure it.

The central hub has jacks that each workstation's network cable plugs into.

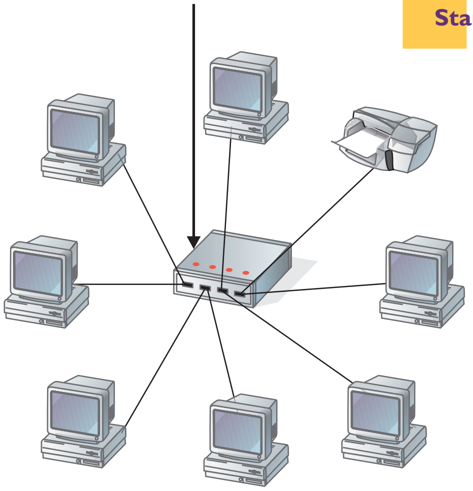


FIGURE 10-8 *The star topology arranges network devices as nodes that are each connected directly to a central hub. Network problems are solved more quickly because the hub makes it easy to trace the cable to the device that is failing.* ■

Hybrid Topology

When you studied the hypermedia design paradigms in Chapter 6, you learned that a design is considered hybrid when it combines different paradigms to create a more complex web. In the field of networking, the term **hybrid topology** is used in a similar fashion to refer to a network that employs more than one topology to connect devices for the purpose of networking. Figure 10-9 shows an example of a star-ring hybrid topology that uses a ring to distribute packets rapidly among three star-shaped subnetworks. Figure 10-10 illustrates a bus-star hybrid that demonstrates a less expensive way of networking the three stars.

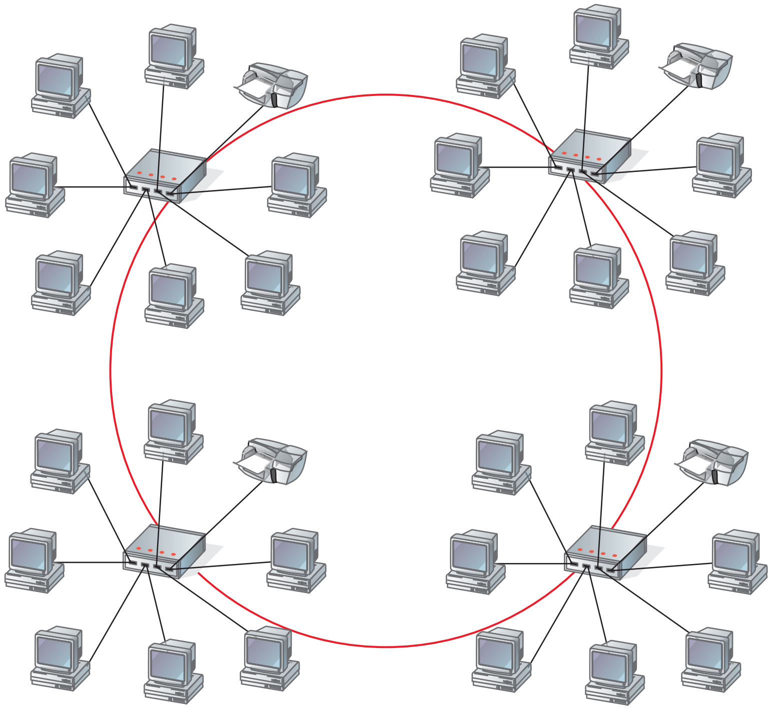


FIGURE 10-9

This hybrid topology uses a star-ring design to create a very fast and efficient network. Because the ring uses a token to synchronize the passing of messages from star to star, the network is not as prone to slowdowns as the star-bus design depicted in Figure 10-10.

The advantage of a hybrid topology is that you can easily add network nodes. Since there is no single point of failure, the network continues to function when one of the nodes stops working. The disadvantage is that if your part of the network is being served by the part of the trunk that has failed, your packets will not get through until that part of the trunk has been repaired. In the meantime, you can continue to communicate with local devices with which you still have connectivity.

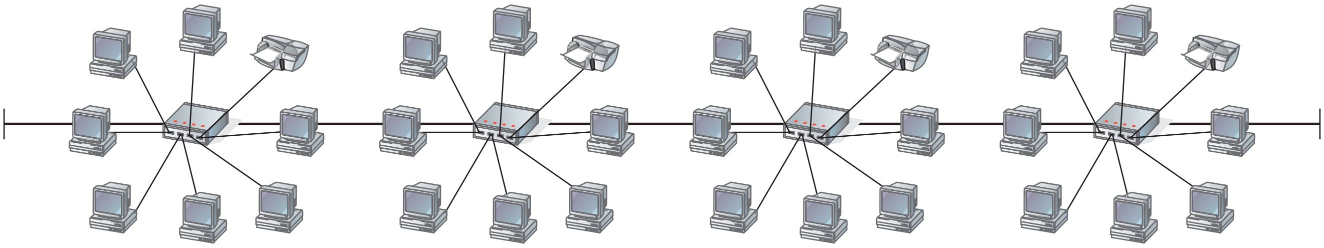


FIGURE 10-10 *A less expensive hybrid topology is the star-bus network pictured here. As traffic increases among the stars, however, this network is more prone to slowdowns than the star-ring network shown in Figure 10-9.*

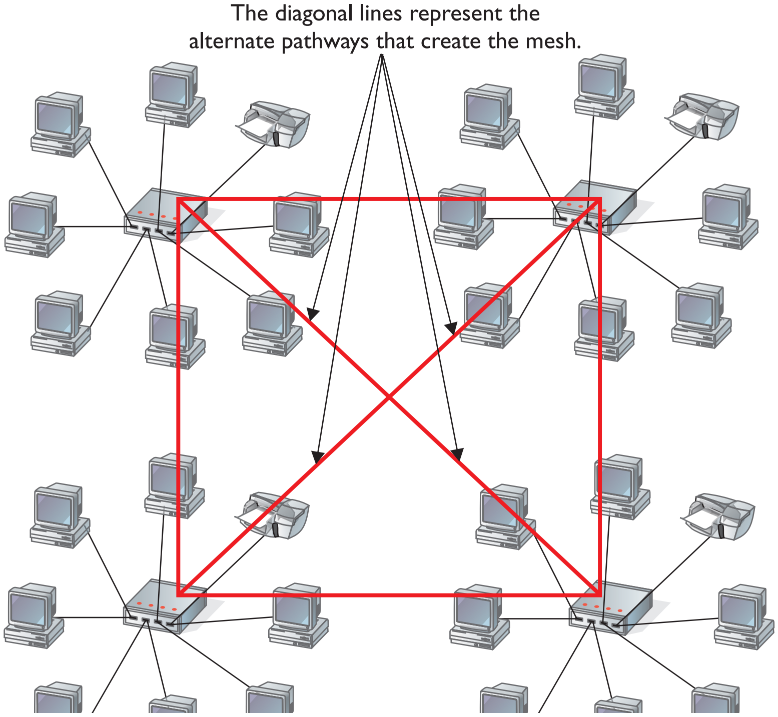
Mesh Topology

In mission-critical operations, you want as much redundancy as possible so that if one part of the network goes down, the packets can find an alternate path to their destination. You achieve this kind of redundancy with the **mesh topology**, which has multiple paths between network hubs. As you will learn in the next chapter, the Internet uses mesh topology to help ensure that if one part of the network fails, packets find alternate routes to reach their destinations. Intelligent hubs called *routers* contain microprocessors that detect network outages, determine the most efficient alternate pathway, and reroute packets accordingly.

Figure 10-11 illustrates that a mesh provides alternate pathways between networks. The advantage of the mesh is that if one of the hubs fails, the packets will find an alternate path to their destination. The only disadvantage is that if you happen to be connected to the hub that has failed, your packets will not be able to get past your local network until the hub returns to service.

FIGURE 10-11

The mesh topology adds alternate pathways to the network to enable packets to find the most efficient routing to their destinations. The public Internet can be thought of as the ultimate in mesh technology, due to the multiple pathways that the telecomm carriers have provided to help prevent network failures.


The diagonal lines represent the alternate pathways that create the mesh.

Adopting Network Protocols

In the field of computer networking, a protocol is a set of rules that define how computers communicate with each other. Without protocols, computers would not know how to exchange messages with each other, and the network would be a chaotic Tower of Babel.

Thanks to the work of the International Standards Organization (ISO), the world has agreed upon a networking specification called the Open System

Interconnection (OSI) Reference Model (OSI/RM). This model defines seven layers of communication that are involved in the networking process. At each layer, the OSI/RM defines the protocols that computers must follow to participate in these communications. The key to understanding the OSI/RM is to define what happens at each layer.

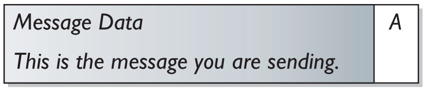
Defining the Seven Layers of the OSI Reference Model

Remember that the purpose of a network is to enable two computers to exchange messages. The seven OSI/RM layers account for what happens to the messages as they work their way down from the sending computer's Application Layer to the Physical Layer of the wire or transport medium that carries the messages across the network to the receiving computer, in which the messages work their way back up through the Application Layer to be processed. Imagine that you are using a Web browser on one computer, and you just clicked a link to view a Web page residing on a second computer. The following sections describe what happens to your request as it works its way down the seven OSI/RM layers:

Layer 7: The Application Layer

Through an Application Programming Interface (API), the browser informs the **Application Layer** of your request. The Application Layer begins to form the packet that will eventually travel across the network. This packet consists of the data that comprises the message, plus a header containing protocol information that is communicated down to the next layer. So far, the packet has the following structure:

Ill 10-1

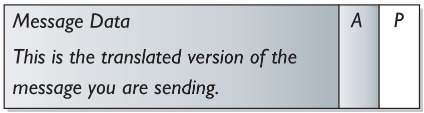


The A header contains protocol information from the Application Layer.

Layer 6: The Presentation Layer

The **Presentation Layer** translates the data into a standard network data format and may use data compression to streamline the packet so it does not consume unnecessary bandwidth on the network. The Presentation Layer may also encrypt the data for sensitive data transmissions, such as banking information. To the front of the packet, the Presentation Layer adds a header containing protocol information describing how it translated, compressed, or encrypted the data. So far, the packet has the following structure:

Ill 10-2

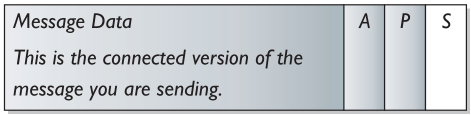

Message Data
This is the translated version of the message you are sending.
A
P

The P header contains protocol information from the Presentation Layer.

Layer 5: The Session Layer

The **Session Layer** negotiates the connection that will be made between the two computers exchanging data. If the amount of data being transmitted is large, the Session Layer inserts a **checkpoint**, which is a marker used to signal that a certain amount of the data has arrived all right. If errors occur in the sending of subsequent packets, the servers know not to resend data prior to the most recently acknowledged checkpoint. To the front of the packet, the Session Layer adds a header containing protocol information describing the connection to be negotiated. So far, the packet has the following structure:

Ill 10-3



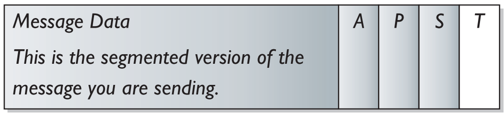
Message Data This is the connected version of the message you are sending.	A	P	S

The S header contains protocol information from the Session Layer.

Layer 4: The Transport Layer

The **Transport Layer** works to ensure that the data arrives reliably at its destination. If the amount of data is large, the Transport Layer splits it into **fragments**, which are smaller data segments that the Transport Layer numbers sequentially. If any of the fragments do not arrive reliably, the sending computer retransmits them. To the front of the packet, the Transport Layer adds a header containing protocol information describing the reliability checks and any fragmentation. So far, the packet has the following structure:

Ill 10-4



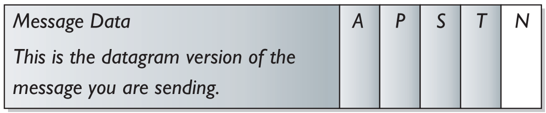
Message Data This is the segmented version of the message you are sending.	A	P	S	T

The T header contains protocol information from the Transport Layer.

Layer 3: The Network Layer

The **Network Layer** organizes the data into **datagrams**, which combine the data from the Transport Layer with routing information that includes the source and destination addresses along with the recommended path depending on network conditions and the nature of the data. To the front of the packet, the Network Layer adds a header containing protocol information describing the addressing and routing. So far, the packet has the following structure:

Ill 10-5



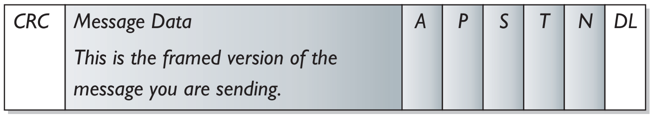
Message Data This is the datagram version of the message you are sending.	A	P	S	T	N

The N header contains protocol information from the Network Layer.

Layer 2: The Data Link Layer

The **Data Link Layer** transforms the data into **data frames**, which use a raw bit format consisting of 0's and 1's to put the data into packets that can be passed down to the Physical Layer for transmission over the network. The Data Link Layer has two sublayers called **Logical Link Control (LLC)**, and **Media Access Control (MAC)**. The LLC performs error checking and regulates the flow of data to and from the Physical Layer. The MAC handles the actual placement of the packets onto the Physical Layer. To the front of the packet, the Data Link Layer adds a header containing framing information. To ensure that the data gets transmitted without error, the LLC performs a mathematical calculation called a **cyclic redundancy check (CRC)**. To the end of the packet, the LLC adds a trailer containing this CRC value. When the packet gets transmitted, the receiving computer performs its own cyclic redundancy check to determine whether the CRC values match. If not, the packet is discarded, and the sending computer resends it. The completed packet has the following structure:

Ill 10-6



CRC	Message Data This is the framed version of the message you are sending.	A	P	S	T	N	DL

The DL header contains protocol information from the Data Link Layer.

The trailer contains CRC information that is used to determine whether the packet arrives at its destination without error.

Layer 1: The Physical Layer

The **Physical Layer** transforms the 0's and 1's from the Data Link Layer into signals that flow over the transmission media. Depending on the type of transmission media, these signals may be electrical voltages, radio signals, air waves, or light pulses. At the receiving end, the Physical Layer converts these signals back into 0's and 1's and passes them up to the Data Link Layer. Figure 10-12 shows the receiving computer working its way back up in reverse order through the same seven layers through which the data passed on its way out from the sending computer. Because the receiving computer must understand the same protocols that the sending computer used to create the packets, both computers must be running the same networking protocols. The next part of this chapter describes the major networking protocol suites that follow the OSI/RM.

Remembering the Seven OSI/RM Layers

If you are studying for the CIW Foundations exam, you need to memorize the names and the order of the seven OSI/RM layers. Networking professionals use a seven-word slogan to help people remember the order of these layers. The slogan is "All people seem to need data processing."

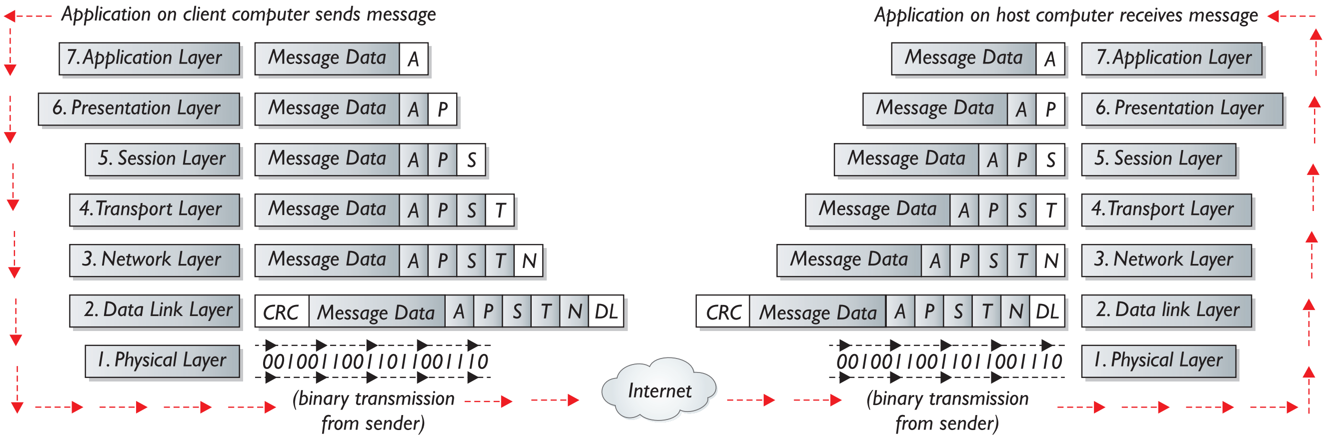
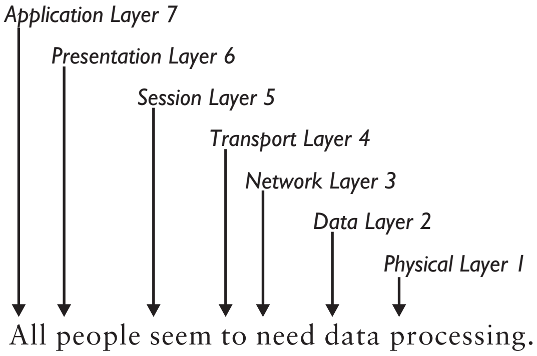


FIGURE 10-12 *When one computer communicates with another via the OSI/RM layers, the messages proceed down from the Application Layer on the sending computer to the Physical Layer, which transmits the message over the network's transmission medium. On the destination computer, the data travels back up the protocol stack. At each of the seven layers, both computers must be running the same protocols in order for this communication to be understood.* ■

Study the callouts below to see how this slogan can help you memorize the order of the seven OSI/RM layers:



OSI/RM Protocol Suite Examples

The term **protocol suite** refers to a collection of protocols that work together in order to conform to a multilayered protocol standard, such as the OSI/RM. Six major protocol suites follow the OSI/RM. These protocol suites include (1) TCP/IP, (2) NetBEUI, (3) IPX/SPX, (4) AppleTalk, (5) DLC, and (6) SNA.

TCP/IP

TCP/IP is the Internet's protocol suite. It has become so important in Internetworking that TCP/IP is built in to virtually every computer's operating system, including Microsoft Windows, the Mac OS, UNIX, and Linux. The TCP/IP protocol suite takes its name from the Transport Control Protocol (TCP) that manages the Transport Layer, and the Internet Protocol (IP) that handles the routing on the Network Layer.

note *In the next chapter, you will learn how to configure the TCP/IP settings that enable a computer to communicate over the Internet and access the wide range of services that use the TCP/IP protocol suite.*

NetBEUI

NetBEUI stands for NetBIOS Extended User Interface, and NetBIOS stands for Network Basic Input/Output System. On versions of the Windows operating system produced before 2001, NetBEUI was the native protocol suite for peer-to-peer networking on local networks. The advantage of NetBEUI is that it is very fast and efficient. Unlike TCP/IP, however, NetBEUI is not routable, which means you can use NetBEUI only to communicate with computers on the local network. To get beyond the local network, you need to use a routable protocol, such as TCP/IP.

IPX/SPX

Another routable protocol is **IPX/SPX**, which stands for Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX). Developed by Novell for use with the NetWare network operating system, the proprietary IPX/SPX protocol suite has been declining in importance due to the popularity of TCP/IP, which is based on an open standard. The latest version of Novell NetWare, for example, defaults to TCP/IP instead of IPX/SPX.

AppleTalk

AppleTalk is to the Macintosh what NetBEUI is to Windows. In other words, AppleTalk is the legacy protocol suite for peer-to-peer networking on local networks of Macintosh computers, and TCP/IP has become the preferred protocol.

Data Link Control (DLC)

IBM invented **Data Link Control (DLC)** to enable microcomputers to connect as clients to legacy mainframes. Today, DLC lives on as the primary protocol used by Hewlett-Packard printers that have **Network Interface Cards (NICs)**.

Systems Network Architecture (SNA)

Invented by IBM in 1974, the **Systems Network Architecture (SNA)** is a protocol suite for connecting different kinds of networks. Still popular in the mainframe world, the SNA framework was an early model of the kind of layered network architecture that evolved into the OSI/RM.

Combining Protocols

Most computers run more than one networking protocol. In the next chapter, you will learn how to configure a computer's Network Interface Card (NIC) to use multiple protocols. The process of assigning a protocol to a NIC is called **protocol binding**.

When combining protocols, however, you should not overdo it. Each protocol adds overhead to your computer by creating processes that monitor the network for packets to handle. You can reduce this overhead

Try This!

Discover Your NIC's MAC Address

Every NIC has a unique Media Access Control (MAC) address. The Physical Layer of the OSI/RM uses MAC addresses to identify the nodes at the ends of each segment of a network. To find out your NIC's MAC address, follow these steps:

1. Click the Windows Start button, choose Control Panel, and double-click Network Connections. The Network Connections window appears onscreen.
2. Double-click the connection you are using to get on the network. If you are using a local area network connection, for example, double-click the Local Area Connection. The connection's Status window appears.
3. Click the Support tab, and then click the Details button. The Network Connection Details window appears.
4. Read the line that says Physical Address. It includes a value consisting of six hexadecimal numbers separated by hyphens. The first three hexadecimal numbers are your NIC vendor's unique manufacturer code, and the other three numbers are the serial number of your NIC. This NIC is the only one in the world containing that number.

by specifying the optimal binding order, which determines the order in which your computer tries protocols when attempting to communicate over the network.

Creating LANs, MANs, and WANs

A **local area network (LAN)** is the connection of two or more computer devices for the purpose of networking within a relatively small area, such as a home, school, or departmental office building. A **metropolitan area network (MAN)** connects local networks across a larger geographical region typically ranging in size up to 50 kilometers in diameter. The term *metropolitan* implies that MANs cover an area the size of a city, although they can also cover small groups of buildings within a corporation. Figure 10-13 shows that a MAN can provide access to other networks by connecting to a wide area network (WAN), which uses high-speed transmission lines to connect MANs and LANs over large geographical areas. The Internet is a network of WANs that use the Internet Protocol to route packets to their destinations through the MANs and LANs that the network comprises.

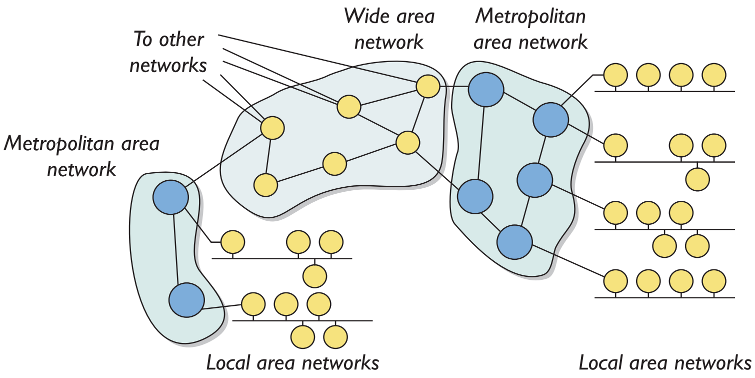


FIGURE 10-13 *Metropolitan area networks (MANs) enable local area networks (LANs) to share the cost of connecting to wide area networks (WANs). The interconnection of LANs, MANs, and WANs that follow the TCP/IP protocol forms the Internet.* ■

IEEE Project 802 Networking Standards

The Institute of Electrical and Electronic Engineers (IEEE, pronounced "I triple-E") is in charge of defining the networking standards that connect devices to form different kinds of local and metropolitan area networks. The IEEE's LAN/MAN Standards Committee (LMSC) performs this work under IEEE Project 802. Table 10-1 shows that this committee is organized according to working groups in charge of defining the networking standards. These groups are numbered from 802.0 through 802.20, as are their corresponding standards.

When a new standard gets created, it is available only to IEEE members for a period of six months. After this waiting period, the LMSC publishes the standards at www.ieee802.org, where anyone can download and study them.

Number	Purpose	Status
802.0	Sponsor Executive Committee	Coordinating, Active
802.1	High Level Interface (HILI) related to network management and Internetworking	Published, Active
802.2	Logical Link Control (LLC) sublayer of the OSI/RM Data Link Layer	Published, Hibernating
802.3	CSMA/CD (Ethernet)	Published, Active
802.4	Token Bus	Published, Hibernating
802.5	Token Ring	Published, Hibernating
802.6	Metropolitan area network (MAN)	Published, Hibernating
802.7	Broadband	Published, Hibernating
802.8	Fiber optics	Unpublished, Disbanded
802.9	Integrated Services LAN (ISLAN) for voice and data integration	Published, Hibernating
802.10	Standard for Interoperable LAN Security (SILS)	Published, Hibernating
802.11	Wireless LAN (WLAN)	Published, Active
802.12	Demand Priority Access LAN	Published, Hibernating
802.13	Not used for superstitious reasons	Avoided
802.14	Cable TV LAN	Unpublished, Disbanded
802.15	Wireless personal area network (WPAN)	Published, Active
802.16	Broadband Wireless Access (BBWA)	Published, Active
802.17	Resilient Packet Ring (RPR)	Published, Active
802.18	Radio Regulatory Technical Advisory Group	Published, Active
802.19	Coexistence Advisory Group	Published, Active
802.20	Mobile Wireless Access	Published, Active

TABLE 10-1 *Working Groups of the IEEE Project 802 LAN/MAN Standards Committee* ■

note *IEEE Project 802 defines the LAN standards commonly used today, except for AppleTalk, which is Apple Computer's proprietary protocol suite for creating local networks of Macintosh computers.*

IEEE 802.2 Standard: Logical Link Control (LLC)

If you are studying for the CIW exam, you need to be able to identify IEEE standards 802.2, 802.3, 802.5, and 802.12. The **IEEE 802.2** standard is the Logical Link Control (LLC) sublayer of the OSI/RM Data Link Layer. The other 802 standards build upon the LLC, which performs error checking and regulates the flow of data to and from the Physical Layer.

The Data Link Layer's other sublayer is the Media Access Control (MAC), which handles the actual placement of the packets onto the Physical Layer. Most of the other 802 standards, including 802.3, 802.5, and 802.12, mainly define the MAC sublayer for different kinds of networks.

IEEE 802.3 CSMA/CD (Ethernet)

The **IEEE 802.3** standard defines Ethernet, which is the most popular method of local area networking. Bob Metcalfe invented Ethernet in his doctoral dissertation project at Harvard in 1973. To save you from having to read his dissertation, you can get a basic understanding of how Ethernet works by learning what **CSMA/CD** stands for, because the words in this acronym describe the essence of Metcalfe's invention. CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. In other words, Ethernet works by detecting the data collisions that can occur when two or more devices use a data channel simultaneously. According to the rules in Metcalfe's thesis, a device waits a random amount of time after detecting a collision and attempts to resend the message. If the data collides again, the device waits twice as long before resending the message.

Metcalfe's rules worked so well that the IEEE codified them as standard IEEE 802.3, which is the standard for ordinary Ethernet networks. The maximum speed of an ordinary 802.3 Ethernet is 10 Mbps. To run Ethernet networks at higher speeds, the IEEE CSMA/CD working group created standards for a so-called **Fast Ethernet** running at 100 Mbps, and an even faster **Gigabit Ethernet** running at 1000 Mpbs.

Table 10-2 defines and compares the ordinary, Fast, and Gigabit Ethernet standards. Notice that the Topology row of this table specifies that Fast and Gigabit Ethernet must have a star topology. In an Ethernet star topology, each device is connected to a central connecting point that is called an **Ethernet hub**. This hub functions as an Ethernet multiport repeater, which is also known as a *concentrator*.

	Ethernet	Fast Ethernet	Gigabit Ethernet
IEEE standard	802.3	802.3u (u stands for updated)	802.3z (specialty copper & fiber optic) 802.3ab (unshielded twisted pair)
Speed	10 Mbps	100 Mbps	1000 Mbps
Media Access Control (MAC) method	CSMA/CD	CSMA/CD	CSMA/CD
Topology	Bus or star	Star	Star
Wiring standards	10base2, 10base5, 10baseT, 10baseFL	100baseTX, 100baseT4, 100baseFX	1000baseT, 1000baseCX, 1000baseSX, 1000baseLX

TABLE 10-2 *Ordinary, Fast, and Gigabit Ethernet standards* ■

IEEE 802.5 Token Ring

The **IEEE 802.5** standard defines token ring, which derives from IBM's local area network design in which a token travels continually around the cable ring to which the network devices are attached. A device can send data only when it has the token. Thus, data collisions never occur on a token-ring network. Under heavy load, token-ring networks are not as likely to degrade as Ethernet networks, which can slow down when multiple data collisions are occurring.

Although IEEE 802.5 does not specify a wiring standard, token-ring networks run typically over twisted-pair wiring at either 4 Mbps or 16 Mbps. Each device attaches to a central connecting point called a **Multi-Station Access Unit (MAU)**. Although the MAU is analogous from a physical standpoint to the hub in an Ethernet network, the MAU contains the ring that passes the token, which prevents data collisions from slowing down the network.

IEEE 802.12 Demand Priority Access LAN (100VG-AnyLAN)

The **IEEE 802.12** standard defines a **Demand Priority Access LAN** that is known in the marketplace as **100VG-AnyLAN**. 100VG means that the network is designed to transmit at a speed of 100 Mbps over voice grade (VG) telephone wiring. AnyLAN refers to the fact that this network can handle packets framed for transmission on either Ethernet or token-ring networks.

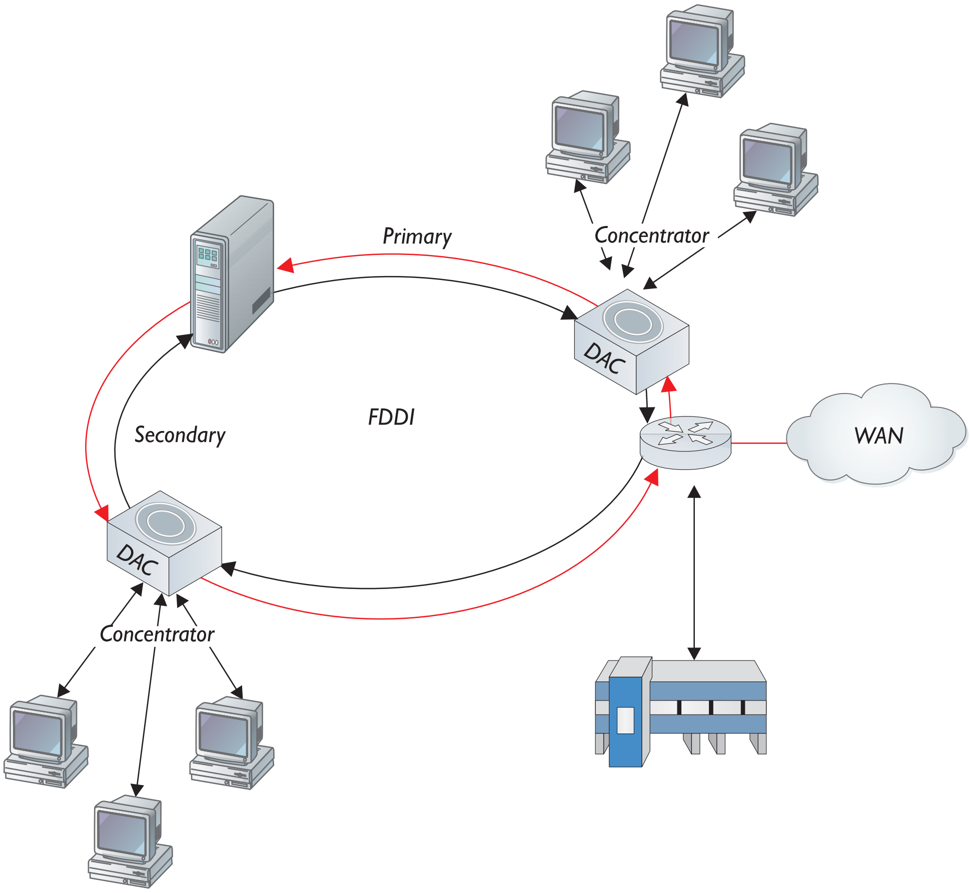
From a physical cabling standpoint, the 100VG-AnyLAN looks like a star-based Ethernet in that all of the devices are connected to hubs. If two nodes try to transmit data simultaneously, however, the 100VG-AnyLAN hub detects this and services first the device that has the higher priority. If the devices have equal priority, the hub randomly selects the node to service first. Moreover, the 100VG-AnyLAN hub sends the message only to its destination. Thus, the 100VG-AnyLAN hub is an intelligent hub with priority servicing and switching that prevents packets from going to every node on the network.

Fiber Distributed Data Interface (FDDI) Networks

As you can tell from its name, a **Fiber Distributed Data Interface (FDDI)** uses fiber optics to create a very fast network. Developed by American Standards Institute (ANSI) committee X3T9.5, FDDI uses two counter-rotating token rings operating at a speed of 100 Mbps. Each fiber optic ring can be up to 100 kilometers long, making FDDI popular for metropolitan area networks (MANs). Each cable can serve up to 500 nodes. Figure 10-14 shows that the two rings can run in parallel to provide redundancy for mission-critical operations in case one of the cables fails. Otherwise, the second ring can extend the network another 100 kilometers and serve up to 500 more nodes, for a total of 1,000 nodes over 200 kilometers. Due to its high reliability, FDDI is often used for **backbones**, which are network cables that act as the primary pathways for traffic that is most often destined for other networks.

FIGURE 10-14

To provide redundancy for mission-critical operations, FDDI can be configured to use counter-rotating primary and secondary rings. The concentrator is the building block of the FDDI network. Known as a dual-attachment concentrator (DAC), it attaches to both rings and enables the network to keep functioning whether or not the PCs connected on the network are powered on or off.



Wide Area Networks (WANs)

A **wide area network (WAN)** is the connection of two or more LANs that can be located in different buildings, cities, countries, or continents. Depending upon the distance and the bandwidth needed for communications among the LANs, you can use different telecommunication strategies for connecting the local networks, such as telephone lines, ISDN connections, broadband, and high-speed fiber optic devices employing frame relay and Asynchronous Transfer Mode (ATM) technologies. The world's largest WAN is the Internet.

X.25

Developed in the early 1970s, **X.25** is a WAN standard that enables data to be transmitted over the packet-switched networks (PSNs) of the telephone companies. In 1976, X.25 became an International Telecommunications Union (ITU) standard. Back then, telecommunication lines did not have the robust error checking of modern communications carriers. Therefore, the telephone companies built a lot of error checking into X.25, which double-checks the accuracy of the data many times along each packet's path. Today, X.25 is not fast enough for high-speed WAN connections, but it still is used by banks for automated tellers and card-swipe machines for credit-card verification.

Frame Relay

Frame Relay is a high-speed WAN standard that was originally developed for the Integrated Services Digital Network (ISDN) but is used today over many kinds of high-performance network interfaces. Sometimes referred to as a streamlined version of X.25, Frame Relay takes advantage of the higher reliability of modern telecommunication lines and does not have the overhead of the windowing and retransmission of last data features that are built into X.25. Frame Relay is an ITU standard, and in the United States, it is also an ANSI standard.

Frame Relay uses variable-length switching to route variable-length packets between various network segments until the final destination is reached. Through a technique called *statistical multiplexing*, packets headed for the same destination can travel different routes that may be available, therefore making more efficient use of available network resources.

Frame Relay connections can be either switched or permanent. A switched virtual circuit (SVC) gets created for each data transfer and is terminated when the data transfer is complete. A permanent virtual circuit (PVC), on the other hand, is a more expensive dedicated network connection that is constantly on. Because SVCs are less expensive, they are used in many of today's networks. Through a feature called **bandwidth on demand**, customers choose the connection speed of their Frame Relay port. The higher the speed, the more the cost.

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is an ITU standard for cell relay that can transmit voice, video, or data in small, fixed-size 53-byte chunks called *cells*. The first 5 bytes contain the cell's header, and the other 48 bytes contain the transmission, which can be voice, video, or data. Because the cells have a fixed size, ATM switches and endpoints do not need to spend valuable processor time dealing with variable-length packets. Instead, the ATM switches can simply route the cells from their sources to their destinations, which are identified in each cell's header. Because the cells are small, clients do not experience the network delay that can occur while waiting for long packets to download. If multiple time slots are available, the addresses in the headers enable the ATM to go ahead and send them; hence the adjective *asynchronous*, which means that the cells do not have to line up and wait to be transmitted sequentially over a single connection.

ATM grew out of the ITU's Broadband Integrated Services Digital Network (B-ISDN) standard, which was originally conceived as a high-speed method for transferring voice, video, and data over public networks. Now available for use over private as well as public networks, ATM combines the flexibility of packet switching with the guaranteed capacity of circuit switching, with bandwidth scalable from a few megabits to many gigabits per second.

Figure 10-15 shows an ATM network comprising ATM switches and ATM endpoints. An ATM switch (1) receives the incoming cell from an ATM endpoint or another ATM switch, (2) reads and updates the cell

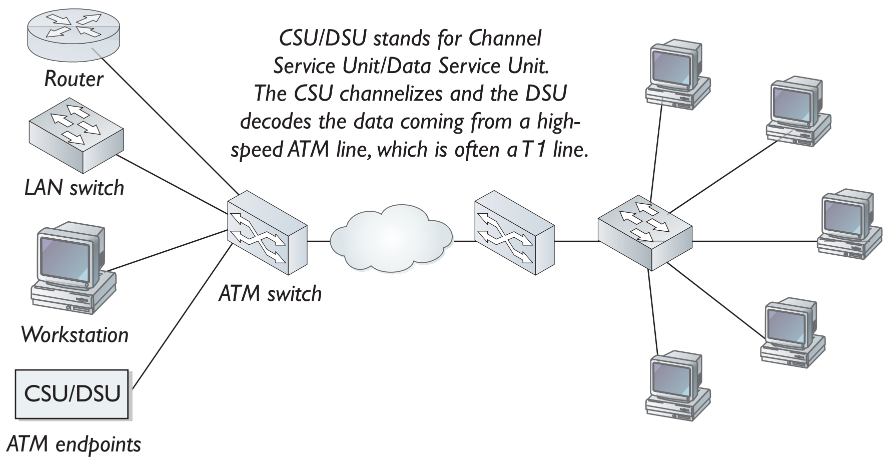

Router
LAN switch
Workstation
CSU/DSU
ATM endpoints
ATM switch
CSU/DSU stands for Channel Service Unit/Data Service Unit. The CSU channelizes and the DSU decodes the data coming from a high-speed ATM line, which is often a T1 line.

FIGURE 10-15 *An asynchronous transfer mode (ATM) network consists of an ATM switch that routes the traffic and ATM endpoints that send or receive the traffic. ATM sends the data in fixed-size units called cells. Because the switches do not deal with variable-length packets, they can process and route the data much faster than more traditional packet-switched technologies.* ■

header information, and (3) switches the cell toward its destination. An ATM endpoint is an end system that contains an ATM network interface adapter, which can reside in a workstation, router, digital service unit (DSU), LAN switch, or video coder-decoder (CODEC).

Network Access Points (NAPs)

A **network access point (NAP)** is a junction that provides direct access to the traffic on a network. To connect two or more LANs to form a WAN, for example, a network administrator connects them through a NAP. Internet service providers use NAPs to exchange traffic on the Internet's backbone. The three major NAPs used by the ISPs are located in New York City, Chicago, and San Francisco.

T-Carrier System

In North America, NAPs often use the T-carrier system to connect a LAN to a WAN. Table 10-3 shows the data rates of the different levels of T-carrier services. The telephone companies offer the public the T1 and T3 service levels, which you can lease for a monthly fee.

The **T1 service** consists of 24 channels running at 64 bps for a total bandwidth of 1.544 Mbps. Organizations that cannot afford the cost of a full T1 can lease a **fractional T1**, which is a subset of the T1's 24 channels.

The **T3 service** consists of 672 channels running at 64 bps for a total bandwidth of 44.736 Mpbs, which is equivalent to 28 T1 lines. As they can with T1, organizations can lease a fractional T3, which is a subset of the T3's 672 channels.

Service Level	Number of 64 Kbps Channels	Total Bandwidth
T1	24	1.544 Mbps
T2	96	6.312 Mbps
T3	672	44.736 Mbps
T4	4032	274.176 Mbps
T5	5760	400.352 Mbps

TABLE 10-3 *T-Carrier Service Levels Used in North America* ■

The T-carrier system uses the Time Division Multiplexing (TDM) transmission method, according to which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit. The advantage of TDM is that customers have guaranteed bandwidth available to them at all times. The disadvantage is that unused time slots do not carry any data. Therefore, the T-carrier is not as good as an ATM for time-sensitive information such as video transmissions.

E-Carrier System

In Europe, E-carrier services provide bandwidth equivalent to the T-carrier system, although the service levels are slightly different. Table 10-4 shows how each E-carrier service level increases bandwidth by a factor of four times higher than its predecessor.

Service Level	Number of 64 Kbps Channels	Total Bandwidth
E1	30	2.048 Mbps
E2	120	8.448 Mbps
E3	480	34.368 Mbps
E4	1920	139.268 Mbps
E5	7680	565.148 Mbps

TABLE 10-4 *E-Carrier Service Levels Used in Europe*

Wireless Access Points (WAPs)

The term **wireless access point (WAP)** refers to wireless network junctions that enable workstations to communicate without cables. Just as NAPs provide junctions for exchanging Internet traffic, so do WAPs provide access points for wireless devices to get on a network.

Network Address Translation (NAT)

NAPs and WAPs may use a technique called **network address translation (NAT)** to transform the IP addresses used for internal traffic into a second set of addresses for external traffic. There are three reasons why you may wish to consider using such a NAT. First, by hiding internal IP addresses, a NAT serves as a kind of firewall that helps protect the internal addresses from being attacked by worms and crackers. Second, a NAT enables a company to combine multiple ISDN connections into a single higher-speed Internet connection. Third, a NAT can translate multiple internal IP addresses into a smaller number of external IP addresses, or just one external IP address. Network administrators who use this third method, however, need to be aware that some NATs do not handle cookies properly.

tip *If you are planning to use a NAT for sharing one external IP address with multiple internal addresses, make sure you choose a NAT that brokers cookies properly so the users of this network can use applications that require cookies.*

Physical Network Components

Physical network components are the actual devices that you connect to create a network. In order to function as a node on the network, each workstation must have a Network Interface Card (NIC). Figure 10-16 shows the NIC containing the jack into which you plug the connector on the network cable. On FDDI equipment, the network interface is called a MIC, which stands for Media Interface Card. On wide area networking equipment, the network interface is called a WIC, for WAN interface card.

Seven kinds of physical devices are commonly found in computer networks: (1) client computers, (2) concentrators, (3) hubs, (4) repeaters,

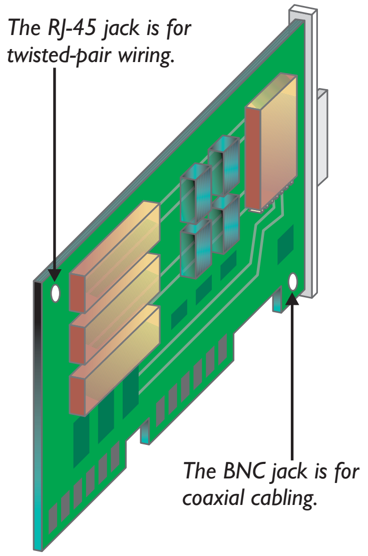

The RJ-45 jack is for twisted-pair wiring.
The BNC jack is for coaxial cabling.

FIGURE 10-16 The Network Interface Card (NIC) contains the female network jack into which you plug the corresponding male connector that is at the end of the network cable. This particular NIC has both RJ-45 and BNC type connectors. Today, however, most NICs come with RJ-45 only. ■

(5) switches, (6) bridges, (7) routers, (8) brouters, and (9) gateways. The following sections describe the functions that these devices serve.

Workstations

Also known as a client computer, the **workstation** is the node upon which end-users perform their work. Most workstations that are sold today come with Ethernet jacks that are connected to the NIC that enables the workstation to function as a node on the network when you plug the network's Ethernet cable into that jack. In the next chapter, you learn how to configure a NIC for local as well as wide area networking.

Concentrators

In an IEEE 802.3 Ethernet network, a **concentrator** is an Ethernet multiport repeater. You use a concentrator when you want to connect multiple Ethernet devices to a single Ethernet cable. The term *concentrator* is synonymous with the term Ethernet hub.

Hubs

In general, the term **hub** refers to the device that serves as the center of a star network topology. In IEEE 802.3 Ethernet networks, a hub is an Ethernet multiport repeater, which is also known as a *concentrator*.

Repeaters

Operating at the Physical Layer of the OSI/RM, a **repeater** interconnects two network cables so they can be treated as a single cable. You use a repeater when you need to run a cable that is longer than the signal can travel without degrading. The number of repeaters you can use is limited by timing and other network issues, depending upon the protocol you are using.

Switches

Operating at the Data Link Layer of the OSI/RM, a **switch** is a network device that filters, forwards, and floods frames based on the destination MAC address of each frame. To **flood** is to pass traffic out all of the switch's connections except for the incoming interface through which the traffic was received.

Bridges

A **bridge** is a relay that operates at the Data Link Layer of the OSI/RM, connecting two network segments and passing packets between them based on the destination MAC address of each frame. The bridged segments must use the same communications protocol.

Routers

A **router** is a relay that operates at the Network Layer of the OSI/RM, forwarding network traffic along the optimal path based on information in the packet's Network Layer header.

Brouters

A bridge router (**brouter**) is a relay that functions as both a router and a bridge.

Gateways

A **gateway** is a computer that routes traffic from a workstation on an internal network to an external network such as the Internet. Thus, a gateway serves as both router and switch.

Physical Connection Media

Physical connection media are the cables, wires, radio signals, or air waves over which network signals travel. There are many categories of coaxial cable, twisted-pair wiring, fiber optic cables, and wireless transmission standards, depending on the distance the data needs to travel and the protocol that is being used to get it there. The following sections define the most commonly used categories.

Coaxial Cable

Coaxial cable, also known as **coax** (pronounced co-axe), consists of a cylindrically braided outer conductor that surrounds and shields a single solid inner copper wire conductor. Figure 10-17 shows these conductors separated by insulating layers. Two categories of coaxial cable are commonly used in LANs, namely, Thinnet and Thicknet.

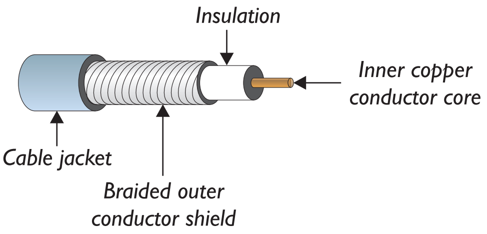


FIGURE 10-17 *From the inside out, coaxial cable consists of (1) a single solid inner copper wire, (2) a layer of nonconducting insulating material normally made of PVC or Teflon, (3) a cylindrically braided conductor that provides electromagnetic shielding, and (4) an outer layer of nonconducting material normally made of plastic or rubber.* ■

Thinnet Thin coaxial cable is called **Thinnet**, which is a very flexible cable about a quarter of an inch in diameter that is used in 10base2 Ethernet networks, in which the cable segments can run up to 185 meters long. Because the cables are so flexible, Thinnet has been a popular choice for connecting devices in small offices and computer labs with many twists and turns. In recent years, however, the use of coax has been declining in favor of the more popular 10baseT Ethernet wiring standard, which uses twisted-pair cabling.

Thicknet Thick coaxial cable is called **Thicknet**, which is a less flexible cable about half an inch thick that is used in 10base5 Ethernet networks, in which the cable segments can be up to 500 meters long. The thicker shielding and cable core enables Thicknet to transmit signals over more than twice the distance of Thinnet. Because of the thicker core, however, Thicknet is much less flexible and therefore considerably harder to work with.

BNC Connector In computer networking, coaxial cables use the **British Naval Connector (BNC)** to plug the cables into workstations, hubs, and other kinds of network devices. Figure 10-18 shows the male style of a BNC connector that is connected to the ends of the coaxial cables. The center pin of the male BNC connects to the copper core of the coax, and the metal tube connects to the braided shield. Outside the tube is a rotating ring that locks the cable to the female BNC connectors found on NICs, hubs, repeaters, and concentrators. You can see a female BNC connector on the NIC pictured previously in Figure 10-16.

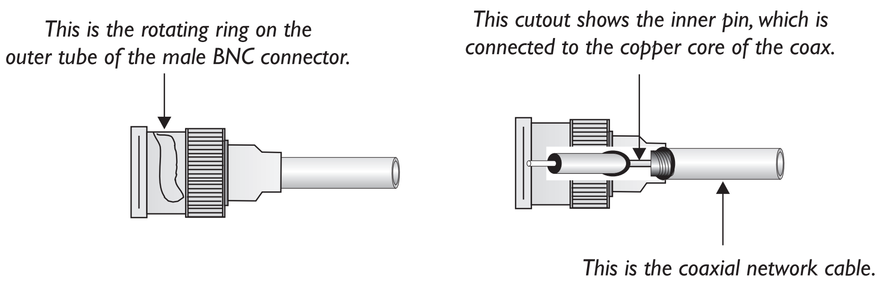
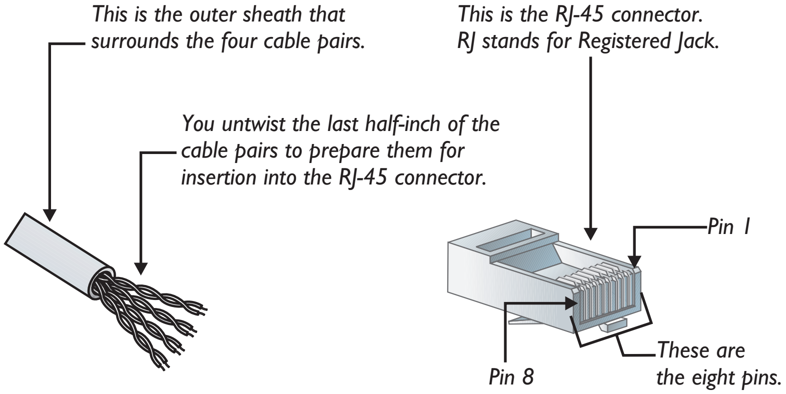

This is the rotating ring on the outer tube of the male BNC connector.
This cutout shows the inner pin, which is connected to the copper core of the coax.
This is the coaxial network cable.

FIGURE 10-18 *The British Naval Connector (BNC) is also known as the Bayonet Nut Connector or the Bayonet Neill-Concelman connector, which is named for the bayonet mounting method and the BNC connector's coinventors, Paul Neill and Carl Concelman.* ■

Twisted Pair

Twisted pair is a transmission medium consisting of two insulated wires that are twisted together to create a double helix that reduces noise levels and eliminates crosstalk between the wires. There are two families of twisted-pair wiring: **unshielded twisted pair (UTP)** and **shielded twisted pair (STP)**, which has an extra layer of insulation that reduces electromagnetic interference. STP is used in gigabyte bandwidth applications. Figure 10-19 shows twisted-pair cabling containing four twisted pairs, and Table 10-5 defines the seven categories that are numbered 1 through 7. The higher the number, the faster the certified data rate.

Twisted-pair cabling is often referred to simply by its category. **CAT 5**, for example, means category five UTP wiring, which is commonly used for Ethernet LANs. In CAT 5, the wires in each pair are twisted four times per inch. The four twisted pairs terminate in an **RJ-45** connector, which has eight pin positions that hold the eight wires from the four twisted pairs.



This is the outer sheath that surrounds the four cable pairs.

This is the RJ-45 connector. RJ stands for Registered Jack.

You untwist the last half-inch of the cable pairs to prepare them for insertion into the RJ-45 connector.

These are the eight pins.

FIGURE 10-19 *Twisted-pair cabling consists of four twisted pairs wrapped inside an outer sheath. The cabling is twisted to create a double helix that reduces noise levels and eliminates crosstalk between the wires. The four twisted pairs terminate in an RJ-45 connector, which has eight pin positions that hold the eight wires from the four twisted pairs. The Try This! exercise at the end of this section teaches you the order in which the wires of a 10/100baseT Ethernet cable must be connected to the pins in the RJ-45 connector.*

Fiber Optics

Fiber optics is a transmission method that transmits light-modulated video, voice, or data signals through hair-thin strands of glass called *fibers*. Because fiber-optic cables are not prone to the problems of electromagnetic interference that copper networks must cope with, fiber has much higher bandwidth potential than conventional copper wire. Fiber costs much more than copper, however, so fiber is normally reserved for applications that require very high bandwidth.

The light pulses that transmit signals through a fiber-optic cable move at the speed of light and can travel for miles without any degradation. At least two fiber strands are normally in each cable. These strands are encased by a layer of Kevlar-reinforced reflective material called *cladding*, which keeps the light inside the fiber.

Category	Type	Certified Speed	Commonly Used For
1	UTP	Not certified	Plain old telephone service (POTS)
2	UTP	4 Mbps	Token-ring networks
3	UTP	10 Mbps	Ethernet
4	UTP	16 Mbps	Token-ring networks
5	UTP	100 Mbps	Ethernet and Fast Ethernet
6	UTP	155 Mbps	Fast Ethernet
7	STP	1000 Mbps	Gigabit Ethernet

Legend: UTP = Unshielded twisted pair
STP = Shielded twisted pair

TABLE 10-5 *Categories of Twisted-Pair Wiring (all categories contain four twisted pairs)*

Due to the high cost and technical expertise required to make fiber-optic connections, the fiber normally terminates in a junction box from which coaxial or twisted-pair cables that are easier to work with carry the packets to their destination.

Wireless Media

Wireless transmission media include cellular, radio, microwave, satellite, and infrared signals. Network nodes that use wireless connections must have a wireless NIC, which connects to a transceiver known as a wireless access point (WAP). The convenience of being untethered by cables has made wireless devices a popular mass-market consumer item. Consumer electronic outlets such as Circuit City, CompUSA, and Best Buy sell many devices that follow the 802.11 wireless networking protocols. Wireless NICs are built in to many laptops, and home media centers use wireless LAN protocols to route digital video, audio, and computer signals to wireless devices throughout the home.

By the time you read this, for example, you will be able to buy a wireless Ethernet extender for the Media Center edition of Windows XP Pro. This extender can attach to any TV or monitor in your home, enabling you to view, control, record, or play up to five simultaneous media streams from the PC on five different display devices throughout your home. When you turn on one of these wireless Ethernet devices, it uses the Dynamic Host Configuration Protocol (DHCP) to establish an IP connection on your home network. You will learn about DHCP in the next chapter, which is devoted to TCP/IP. For the latest on the Windows Media Center Extender and related wireless Ethernet media devices, go to www.microsoft.com/windowsxp/mediacenter.

Try This!

Make a 10/100baseT Ethernet Cable

The two basic kinds of 10/100baseT Ethernet cables are straight through and crossover. You use straight through cables to connect PCs and workstations to an Ethernet hub. You use a crossover cable when you need to connect two hubs, or to connect one computer directly to a second computer, without going through a hub. If you have two computers that have Ethernet jacks, for example, a crossover cable can come in handy whenever you want to connect those computers directly to each other.

There is only one difference between straight-through and crossover cables. In a straight-through cable, the four pairs of wires go to the exact same pins in the RJ-45 connector that is on each end of the cable. In a crossover cable, on the other hand, the cable pairs that do the transmitting and receiving reverse their pin positions on each end of the cable.

This exercise enables you to create either a straight-through or a crossover 10/100baseT Ethernet cable. Follow these steps:

1. Go to your local electronic supply store, such as Radio Shack, and buy some category 5 wiring, a bag of RJ-45 connectors rated for use with 10/100baseT Ethernet, and an RJ-45 crimping tool. If you plan to do a lot of your own Ethernet wiring around the home or office, you can buy CAT 5 wiring in bulk. The author, for example, bought from Home Depot a thousand feet of CAT 5 wiring for about $35.

Try This! *continued*

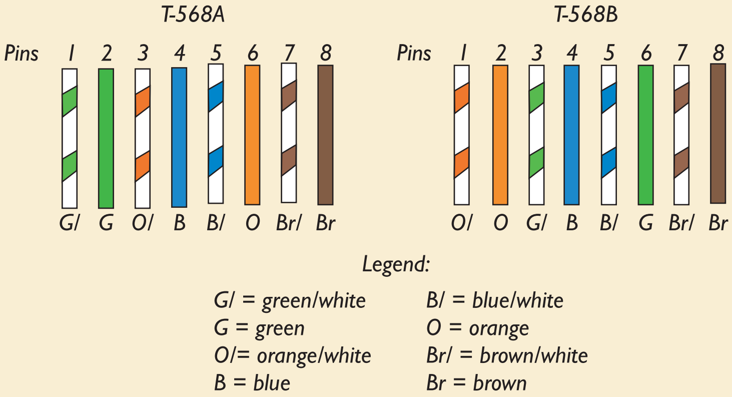
2. Cut a length of CAT 5 cable that is a few feet longer than you need. You want to leave some slack so you can easily maneuver and reposition equipment if you need to reconfigure it. Ethernet does not work well with a lot of extra cable coiled up, however, so you should not make the cable excessively longer than you need. The maximum length you can make a 10/100baseT cable is 100 meters (328 feet).

3. Remove about an inch from each end of the CAT 5 cable's outer sheath or jacket. As you do this, be careful not to harm or nick any of the insulation on the twisted pairs inside the jacket.

4. Inspect the twisted pairs carefully. If you see any nicks, cut off the end of the CAT 5 cable and return to step 3.

5. Untwist the protruding inch of the four twisted pairs. To avoid crosstalk, do not untwist more of the wiring than necessary. You will notice that the wires are color coded.

6. Arrange the wires in the proper order according to their color. The two wiring standards are called T-568A and T-568B. If you are making a straight-through cable, you must use either T-568A or T-568B on both ends of the cable. If you are making a crossover cable, you make one end follow T-568A and the other T-568B. Arrange the wires in the order needed for the kind of cable you are creating:

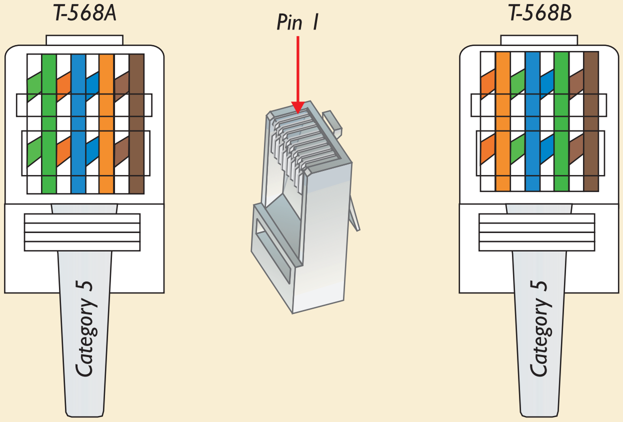


7. Use the cable-cutting part of the crimping tool to trim the eight wires to make them even with each other. When you do this trim, you must let only slightly less than half of an inch of the wires protrude from end of the CAT 5 cable's jacket. If you let more than half an inch protrude, the cable is prone to crosstalk.

8. Hold the RJ-45 connector in one hand with the clip facing down or away from you, and insert the cable slowly yet firmly. Make sure it goes all the way in.

9. Double-check to make sure each pin has the proper color wire. As you look down through the connector from the top, it must appear as follows, depending on whether you followed T-568A or T-568B:

10. After you are sure the pins have the proper color wires, insert the cable into the RJ-45 socket of your crimping tool. Hold the wires in place, and squeeze the crimper handles quite firmly. After you do this to both ends of the cable, you can test it by plugging it in to your network.



11. Reflection: If you compare the T-568A and T-568B wiring standards presented in step 6, you can see that they reverse the transmit (pins 1 and 2) and receive (pins 3 and 6) wiring pairs.

Chapter 10 Review

Chapter Summary

After reading this chapter and completing the step-by-step tutorials and Try This! exercises, you should understand the following facts about the Internet:

Understanding Networks

- A network is the connection of two or more digital devices for the purpose of communicating, transferring, or obtaining data.
- In order to have a network, you must have three things characteristic of all networks: (1) a physical connection through which the data flows; (2) a set of communication rules called *protocols* that the networked devices use to communicate; and (3) one or more network services that receive these communications and respond appropriately.
- Networking is the act of communicating over a network. In the mainframe/terminal model of networking, users compete for resources on a centralized computer that uses time sharing to allocate computing cycles to each user.
- A more efficient way of distributing networked resources is the client-server model, in which computers exchange information by sending it (as servers) and receiving it (as clients). The most strategic aspect of client-server computing is the manner in which computers can serve dual roles as both servers and clients.
- In a peer-to-peer (P2P) network, workstations have equal responsibility for sharing files and accessing services on each other's computers. In the music industry, this absence of authority makes it difficult to identify and prosecute copyright infringers who share copyrighted music over P2P networks without permission.
- The term *enterprise model* refers to networking within large organizations that dedicate entire servers to handling important tasks in the most efficient manner. A large organization, for example, may need individual servers dedicated to the tasks of serving mail, hosting databases, managing security, and routing network traffic.
- A network operating system is the software that adds to a computer the functions required for connecting computers for the purpose of networking. The most popular network operating systems are Microsoft Windows, UNIX, Linux, the Mac OS, and Novel NetWare.

Classifying Network Topologies

- The geographical shape of a network is referred to as the network's *topology*. The five kinds of network topology are (1) bus topology, (2) ring topology, (3) star topology, (4) hybrid topology, and (5) mesh topology.
- The bus topology has a single cable, called the *bus* or the *trunk*, to which every device on the network connects.
- The ring topology takes its name from the loop that forms when you connect the network's nodes in a circle. Messages flow in one direction around the ring, as does a token that provides each device its turn to communicate.
- In a star topology, each device in the network connects to a central hub, which distributes messages from one node to another.
- The term *hybrid topology* refers to a network that employs more than one topology to connect devices for the purpose of networking. An example is a star-ring hybrid that uses a token to synchronize the passing of messages from star to star.
- Mesh topology creates redundancy by creating multiple paths between network hubs. If part of the network goes down, the packets can find another path to their destination. The public Internet can be thought of as the ultimate in mesh technology, due to the multiple pathways that the telecomm carriers have provided to help prevent network failures.

Adaptive Network Protocols

- Layer 7 of the OSI/RM is the Application Layer. Through an API, Layer 7 receives the message from the client computer and begins to form the packet that will eventually travel across the network.

- Layer 6, the Presentation Layer, translates the data into a standard network data format and may use data compression to streamline the packet so it does not consume unnecessary bandwidth on the network. The Presentation Layer may also encrypt the data for sensitive data transmissions, such as banking information.
- Layer 5 is the Session Layer, which negotiates the connection that will be made between the two computers that are exchanging data. If the amount of data being transmitted is large, the Session Layer inserts a checkpoint, which is a marker used to signal that a certain amount of the data has successfully arrived.
- Layer 4 is the Transport Layer, which works to ensure that the data arrives reliably at its destination. If the amount of data is large, the Transport Layer splits it into fragments, which are smaller data segments that the Transport Layer numbers sequentially.
- Layer 3, the Network Layer, organizes the data into datagrams, which combine the data from the Transport Layer with routing information that includes the source and destination addresses along with the recommended path depending on network conditions and the nature of the data.
- Layer 2, the Data Link Layer, transforms the data into data frames, which use a raw bit format consisting of 0's and 1's to put the data into packets that can be passed down to the Physical Layer for transmission over the network.
- Layer 1 is the Physical Layer, which transforms the 0's and 1's from the Data Link Layer into signals that flow over the transmission media. Depending on the type of transmission media, these signals may be electrical voltages, radio signals, air waves, or light pulses.
- The six major protocol suites that follow the OSI/RM networking standard are (1) TCP/IP, which powers the Internet; (2) NetBEUI, which was Microsoft's native protocol suite for peer-to-peer networking on local networks of Windows computers prior to 2001; (3) IPX/SPX, which was developed by Novell for use with the NetWare network operating system; (4) AppleTalk, which is the legacy protocol suite for peer-to-peer networking on local networks of Macintosh computers; (5) DLC, which IBM invented to connect microcomputers as clients to legacy mainframe computers, and HP still uses in printers that have NICs; and (6) SNA, which IBM invented for connecting different kinds of networks.

Creating LAN's, MAN's, and WAN's

- A local area network (LAN) is the connection of two or more computer devices for the purpose of networking within a relatively small area, such as a home, school, or departmental office building. A metropolitan area network (MAN) connects local networks across a larger geographical region typically ranging in size up to 50 kilometers in diameter.
- A wide area network (WAN) uses high-speed transmission lines to connect MANs and LANs over large geographical areas. The Internet is a network of WANs that use the Internet Protocol to route packets to their destinations through the MANs and LANs that the network comprises.
- The Institute of Electrical and Electronic Engineers (IEEE, pronounced I triple-E) is in charge of defining the networking standards that connect devices to form different kinds of local and metropolitan area networks. The IEEE's LAN/MAN Standards Committee (LMSC) performs this work under IEEE Project 802, which has issued a series of 802 networking standards numbered from 802.0 to 802.20.
- If you are studying for the CIW exam, you must be able to identify IEEE standards 802.2, 802.3, 802.5, and 802.12. The 802.2 standard is the Logical Link Control (LLC) sublayer of the OSI/RM Data Link Layer. The other sublayer is the Media Access Control (MAC). Most of the other 802 standards, including 802.3, 802.5, and 802.12, mainly define the MAC sublayer for different kinds of networks. IEEE standard 802.3 defines CSMA/CD (Ethernet), 802.5 defines token ring, and 802.12 defines Demand Priority Access LAN (100VG-AnyLAN).

- Fiber Distributed Data Interface (FDDI) is a fiber-optics networking standard developed by the American Standards Institute (ANSI). FDDI uses two counter-rotating token rings operating at a speed of 100 Mbps. Due to its high reliability, FDDI is often used for backbones, which are network cables that act as the primary pathways for traffic most often destined for other networks.
- X.25 is a WAN standard that enables data to be transmitted over the packet-switched networks (PSNs) of the telephone companies. By modern standards, however, X.25 is relatively slow.
- Frame Relay is a high-speed WAN standard originally developed for the Integrated Services Digital Network (ISDN) but is used today over many kinds of high-performance network interfaces. Sometimes referred to as a streamlined version of X.25, Frame Relay takes advantage of the higher reliability of modern telecommunication lines and does not have the overhead of the windowing and retransmission of last data features that are built into X.25.
- Asynchronous Transfer Mode (ATM) is another high-speed WAN standard that sends the data in fixed-size units called *cells*. Because the switches do not have to deal with variable-length packets, they can process and route the data much faster than more traditional packet-switched technologies.
- A network access point (NAP) is a junction that provides direct access to the traffic on a network. To connect two or more LANs to a WAN, for example, a network administrator connects them through a NAP. Internet service providers use NAPs to exchange each other's traffic on the Internet's backbone. The three major NAPs used by the ISPs are located in New York City, Chicago, and San Francisco.
- Physical network components are the actual devices that you connect together to create a network. In order to function as a node on the network, each workstation must have a Network Interface Card (NIC), which contains the jack into which you plug the connector on the network cable. On FDDI equipment, the network interface is called a MIC, which stands for media interface card. On wide area networking equipment, the network interface is called a WIC, for WAN interface card.
- Other physical components commonly found in computer networks include concentrators, hubs, repeaters, switches, bridges, and routers. A concentrator is an Ethernet multiport repeater, which connects multiple Ethernet devices to a single Ethernet cable. A hub is the device that serves as the center of a star network topology.
- A repeater interconnects two network cables so they can be treated as a single cable. A switch is a network device that filters, forwards, and floods frames based on their destination MAC address.
- A bridge is a relay that operates at the Data Link Layer of the OSI/RM, connecting two network segments and passing packets between them based on the destination MAC address of each frame.
- A router is a relay that operates at the Network Layer of the OSI/RM, forwarding network traffic along the optimal path based on information in the packet's Network Layer header.
- A bridge router (brouter) is a relay that functions as both a router and a bridge.
- A gateway is a computer that routes traffic from a workstation on an internal network to an external network such as the Internet. Thus, a gateway serves as both router and switch.
- To connect PCs and workstations to an Ethernet hub, you use a straight-through 10/100baseT Ethernet cable, which can be up to 100 meters (328 feet) long. To connect a PC directly to a PC, or to connect a hub to a hub, you use a crossover cable, which reverses the location of transmit and receive wires in the RJ-45 connector at one end of the cable.

Key Terms

- **AppleTalk** *(19)*
- **Application Layer** *(15)*
- **Asynchronous Transfer Mode (ATM)** *(25)*
- **backbone** *(23)*
- **bandwidth on demand** *(25)*
- **British Naval Connector (BNC)** *(30)*
- **bridge** *(28)*
- **brouter** *(29)*
- **bus** *(11)*
- **bus topology** *(11)*
- **CAT 5** *(30)*
- **checkpoint** *(16)*
- **client-server** *(6)*
- **coaxial cable** *(29)*
- **coax** *(29)*
- **concentrator** *(28)*
- **CSMA/CD** *(22)*
- **cyclic redundancy check (CRC)** *(17)*
- **data frames** *(17)*
- **datagrams** *(16)*
- **Data Link Control (DLC)** *(19)*
- **Data Link Layer** *(17)*
- **Demand Priority Access LAN (100VG-AnyLAN)** *(23)*
- **enterprise model** *(7)*
- **Ethernet hub** *(22)*
- **Fast Ethernet** *(22)*
- **Fiber Distributed Data Interface (FDDI)** *(23)*
- **fiber optics** *(31)*
- **flood** *(28)*
- **fragments** *(16)*
- **Frame Relay** *(25)*
- **fractional T1** *(26)*
- **gateway** *(29)*
- **Gigabit Ethernet** *(22)*
- **hub** *(28)*
- **hybrid topology** *(13)*
- **IEEE 802.2** *(22)*
- **IEEE 802.3** *(22)*
- **IEEE 802.5** *(23)*
- **IEEE 802.12** *(23)*
- **IPX/SPX** *(19)*
- **Linux** *(10)*
- **local area network (LAN)** *(20)*
- **Logical Link Control (LLC)** *(17)*
- **Macintosh OS X** *(10)*
- **mainframe** *(5)*
- **mainframe/terminal model** *(5)*
- **Media Access Control (MAC)** *(17)*
- **mesh topology** *(14)*
- **metropolitan area network (MAN)** *(20)*
- **Multi-Station Access Unit (MAU)** *(23)*
- **multi-tier** *(6)*
- **NetBEUI** *(19)*
- **NetWare** *(10)*
- **network** *(4)*
- **network access point (NAP)** *(26)*
- **network address translation (NAT)** *(27)*
- **Network Interface Card (NIC)** *(19)*
- **Network Layer** *(16)*
- **network operating system** *(8)*
- **networking** *(4)*
- **OSI Reference Model (OSI/RM)** *(4)*
- **peer-to-peer (P2P)** *(7)*
- **Physical Layer** *(17)*
- **Presentation Layer** *(15)*
- **protocol binding** *(19)*
- **protocol suite** *(18)*
- **push-pull metaphor** *(8)*
- **repeater** *(28)*
- **ring topology** *(11)*
- **RJ-45** *(30)*
- **router** *(29)*
- **Session Layer** *(16)*
- **shielded twisted pair (STP)** *(30)*
- **star topology** *(12)*
- **switch** *(28)*
- **Systems Network Architecture (SNA)** *(19)*
- **T1 service** *(26)*
- **T3 service** *(26)*
- **TCP/IP** *(18)*
- **terminal** *(5)*
- **Thicknet** *(30)*
- **Thinnet** *(30)*
- **topology** *(11)*
- **Transport Layer** *(16)*
- **trunk** *(11)*
- **twisted pair** *(30)*
- **UNIX** *(10)*
- **unshielded twisted pair (UTP)** *(30)*
- **wide area network (WAN)** *(24)*
- **wireless access point (WAP)** *(27)*
- **workstation** *(28)*
- **X.25** *(24)*

Key Terms Quiz

1. In a(n) __________________ network, workstations have equal responsibility for sharing files and accessing services on each other's computers.
2. The __________________ topology has a single cable to which every device on the network connects.
3. In the __________________ topology, each device in the network connects to a central hub, which distributes messages from one node to another.
4. __________________ topology creates redundancy by creating multiple paths between network hubs.
5. In the OSI/RM, the __________________ layer negotiates the connection made between the two computers that are exchanging data.
6. In the OSI/RM, the __________________ layer transforms the data into data frames, which use a raw bit format consisting of 0's and 1's to put the data into packets that can be passed down to the Physical Layer for transmission over the network.
7. The IEEE 802.2 standard is the Logical Link Control (LLC) sublayer of the OSI/RM __________________ layer.
8. CSMA/CD (Ethernet) is defined by the __________________ standard.
9. __________________ is a high-speed WAN standard that sends the data in fixed-size units called cells. Because the switches do not need to deal with variable-length packets, they can process and route the data much faster than more traditional packet-switched technologies.
10. In order to function as a node on the network, each workstation must have a(n) __________________, which contains the jack into which you plug the connector on the network cable.

Multiple-Choice Quiz

1. Which of the following networking models is historically the oldest?
   a. Client-server
   b. Enterprise
   c. Mainframe/terminal
   d. Peer-to-peer
2. What kind of topology is formed when a network uses a token ring to distribute data to the Ethernet hubs of each of four star networks?
   a. Bus
   b. Hybrid
   c. Mesh
   d. Superstar
3. Which of the following OSI/RM layers is responsible for performing the data encryption that is used by banks, for example, to keep financial information secret as it winds its way across the Internet?
   a. Application Layer
   b. Presentation Layer
   c. Session Layer
   d. Transport Layer
4. Of the following protocol suites that follow the OSI reference model, which one powers the Internet?
   a. AppleTalk
   b. IPX/SPX
   c. NetBEUI
   d. TCP/IP
5. Which one of the following IEEE 802 standards defines token-ring networking?
   a. 802.2
   b. 802.3
   c. 802.5
   d. 802.12
6. Which one of the following IEEE 802 standards defines Ethernet networking?
   a. 802.2
   b. 802.3
   c. 802.5
   d. 802.12
7. Sometimes referred to as a streamlined version of X.25, which high-speed WAN standard originally developed for the Integrated Services Digital Network (ISDN) is used today over

many kinds of high-performance network interfaces?

a. 100VG-AnyLAN
b. ATM
c. FDDI
d. Frame Relay

8. Which junction provides direct access to the traffic on a network?

a. LAP
b. NAP
c. SAP
d. TAP

9. On wide area networking equipment, the network interface is called a

a. LIC
b. MIC
c. NIC
d. WIC

10. Which device operates at the Network Layer of the OSI/RM, forwarding network traffic along the optimal path based on information in the packet's Network Layer header?

a. Bridge
b. Hub
c. Router
d. Switch

Essay Quiz

1. The legacy mainframe/terminal networking model that arose in the mid-twentieth century has been superseded by the more efficient client-server model. Many large corporations, however, still have mainframe computers. Describe the kind of software that can enable a client computer to obtain access to the corporate mainframe.
2. Discuss the fundamental design differences between the collision detection of the IEEE 802.3 Ethernet standard as compared to the token passing method of the 802.5 token ring. Under what kind of situation would token ring be better than Ethernet?
3. Why do fiber-optic cables work better than copper as the physical transmission media for network backbones?
4. During the early 1970s, the X.25 standard played an important role in the creation of the Internet. What did the X.25 standard enable that was so critically important in the creation of a public Internet?
5. In creating a network cable that can be used either on a regular10 Mbps Ethernet or on a 100 Mbps Fast Ethernet, what category of UTP wiring should you use?

Lab Projects

• Lab Project 10-1: Network Needs Analysis

Imagine that you work for a mid-sized company or school district that is looking to revamp its networking strategy. Several buildings must be interconnected, each of which contains a couple dozen workstations that have to function as nodes on the network. Your employer has assigned you the task of analyzing their needs and recommending alternative networking strategies. As part of this analysis, your employer wants to know the relative advantages and disadvantages of each alternative in order to make an informed decision regarding the networking strategy your organization should adopt. Use your word processor to write an essay in which you assess the needs and discuss the relative pluses and minuses of possible networking alternatives. In developing this needs assessment, consider the following issues:

- **Bandwidth requirements** What are the bandwidth requirements of the workers who use the network? Do some of the buildings have higher bandwidth requirements than others?

- **Comparative analysis** Compare alternative methods for providing this bandwidth. Search Google or Yahoo for networking companies, and peruse the LAN and MAN solutions provided by the major manufacturers, such as Cisco, 3Com, and Nortel. Which appear to be the best alternatives for providing the required bandwidth?
- **Architecture and topology** Discuss the relative advantages and disadvantages of the different networking topologies that appear to be relevant in the context of this analysis.
- **Network operating system** What network operating system(s) do the workstations need to run in order to access the network? Are the recommended operating systems already running on these workstations, or will new software have to be obtained?
- **Scope of work** Consider the amount of work that will be required to implement the various alternatives you are putting forward, and include an estimate of the amount of time it will take to accomplish them.

If your instructor asked you to hand in the needs analysis, make sure you put your name at the top of the essay, then copy it onto a disk or follow the other instructions you may have been given for submitting this assignment.

• Lab Project 10-2: Network Design

Your mid-sized company or school district has asked you to design a hybrid network in which you will use an appropriate mix of networking topologies to provide efficient and reliable connections among the local area networks operating in five different buildings that are within a ten-mile radius. At the moment, these LANs are using a bus topology that is prone to slow down under heavy traffic and is time consuming to repair when a node goes down and renders the LAN unusable. Connections between the LANs are slow due to the use of legacy X.25 lines leased from the local telephone company. Use your word processor to write an essay in which you present an improved network design for solving these problems. In developing this design, consider the following issues:

- **LAN topology** You clearly need to replace the bus networks with a better LAN topology. Which topology do you recommend for the LANs within each building?
- **MAN topology** The physical distance between buildings is within the geographical radius of metropolitan area network technology. Which MAN topology is most appropriate for your network design?
- **WAN connection** Which WAN protocol or method will you use to connect the MAN to the Internet?
- **Integration** How can your design better integrate the organization's programs and services? If there are databases that serve information through different business processes that interact with end users, for example, could a multi-tier approach make the development, production, and maintenance of these processes more efficient?
- **Wiring plan** What kind of wiring does your plan require? Specify the wiring categories, and state whether any of the existing wiring can continue to be used.
- **Wireless facilities** If users will be accessing the network via wireless devices, specify the WAPs needed to connect them.
- **Draw the network diagram** Depending on your artistic ability, you may find it helpful to use a networking clip art library or design tool. To find these tools, search Google or Yahoo for network design, network symbols, or network clip art. See also the public domain Cisco icon library at www.cisco.com/warp/public/503/2.html, where you will find full color and black-and-white icons as well as stencils for drawing network diagrams with Microsoft Visio.

If your instructor asked you to hand in the network design, make sure you put your name at the top of the essay, then copy it onto a disk or follow the other instructions you may have been given for submitting this assignment.