EXTENDED LEARNING MODULE E

NETWORK BASICS

Student Learning Outcomes

1. IDENTIFY AND DESCRIBE THE FOUR BASIC CONCEPTS ON WHICH NETWORKS ARE BUILT AND DESCRIBE WHAT IS NEEDED TO SET UP A SMALL PEER-TO-PEER NETWORK AT HOME.
2. DESCRIBE THE COMPONENTS USED TO BUILD LARGE BUSINESS NETWORKS AND DEFINE AND COMPARE LOCAL AREA NETWORKS (LANS), WIDE AREA NETWORKS (WANS), AND METROPOLITAN AREA NETWORKS (MANS).
3. COMPARE AND CONTRAST THE VARIOUS INTERNET CONNECTION POSSIBILITIES.
4. COMPARE AND CONTRAST THE TYPES OF COMMUNICATIONS MEDIA.
5. STATE THE FOUR PRINCIPLES OF COMPUTER SECURITY AND DESCRIBE HOW DIFFERENT NETWORK SECURITY DEVICES REFLECT THOSE PRINCIPLES.
6. DESCRIBE CLIENT/SERVER BUSINESS NETWORKS FROM A BUSINESS AND PHYSICAL POINT OF VIEW.

Introduction

When you're surfing the Web, accessing software on your school's server, sending e-mail, or letting your roommate use his or her computer to access the files on your computer, your computer is part of a network. A ***computer network*** (which we simply refer to as a network) is two or more computers connected so that they can communicate with each other and share information, software, peripheral devices, and/or processing power. Many networks have dozens, hundreds, or even thousands of computers.

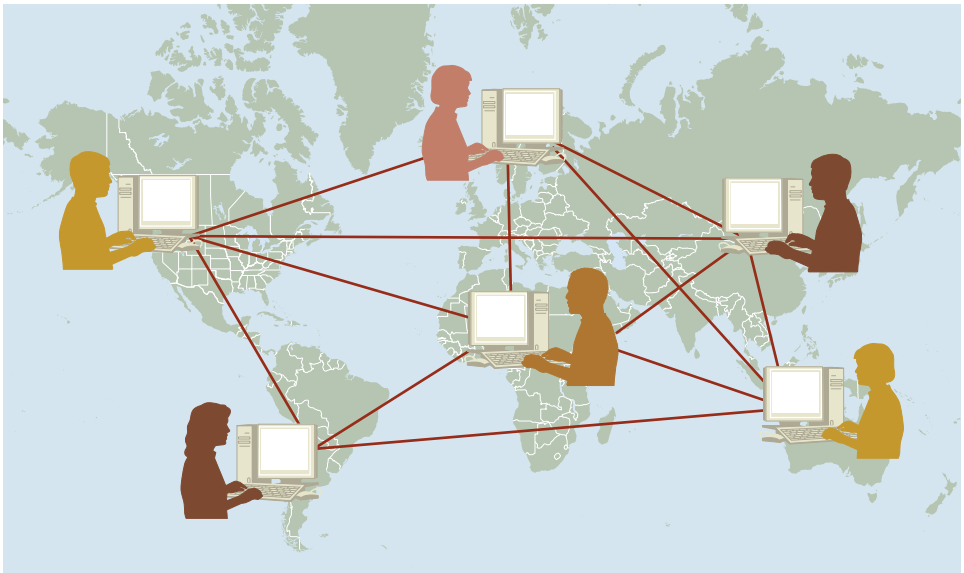
BASIC PRINCIPLES OF NETWORKS

Networks come in all sizes, from two computers connected to share a printer, to the Internet, which is the largest network on the planet, joining millions of computers of all kinds all over the world. In between are business networks, which vary in size from a dozen or fewer computers to many thousands.

Some basic principles apply to all networks, large or small.

1. Each computer on a network must have a network interface (either as an expansion card or integrated into the motherboard, or even through software for a modem) that provides the entrance or doorway in that computer for information traffic to and from other computers.
2. A network usually has at least one connecting device (like a hub, switch, or home/broadband router) that ties the computers on the network together and acts as a switchboard for passing information.
3. There must be communications media like cables or radio waves connecting network hardware devices. The communications media transport information around the network between computers and the connecting device(s).
4. Each computer must have software that supports the movement of information in and out of the computer. This could be modem software and/or a network operating system.

First, we'll examine the smallest networks—a few computers connected in a home or dorm room—and then move on to larger business networks. We'll discuss network devices, LANs, WANs, and MANs, and communications media. Finally, we'll describe network security and illustrate the client/server software model.

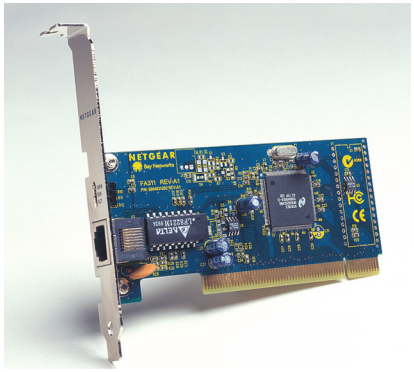


Home Networks

If you have a computer at home with cable or DSL Internet access, you may already be familiar with several network components. A typical home setup has

- An Ethernet network card in each computer, and/or a wireless Ethernet card in each laptop computer.
- Network cables to transmit signals, or no cables if you're using wireless.
- A DSL or cable line from your ISP, and a broadband or home router to pass messages and files back and forth.

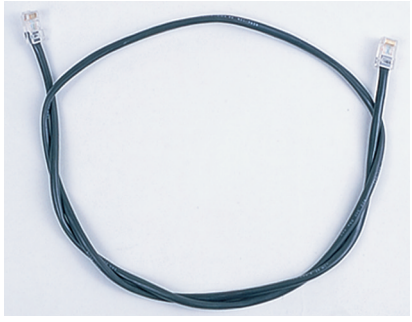
NETWORK CARDS IN EACH COMPUTER



First, each computer needs a network interface. A ***network interface card (NIC)*** is an expansion card for a desktop computer or a PC card for a notebook computer that connects your computer to a network and provides the doorway for information to flow in and out. The network interface card has a jack (or port) for a network cable that connects your computer to a network. Some computers have network interfaces built into their motherboards, referred to as integrated network interfaces.

An ***Ethernet card*** is the most common type of network interface card. It has a jack, usually an RJ-45 that looks like a telephone jack, only a little larger. You run a network cable from your Ethernet card to a hub or switch, or you can use a cable with different wiring called a *crossover cable* to plug straight into another computer or printer if you have only two devices to connect.

WIRED AND WIRELESS TRANSMISSION MEDIA

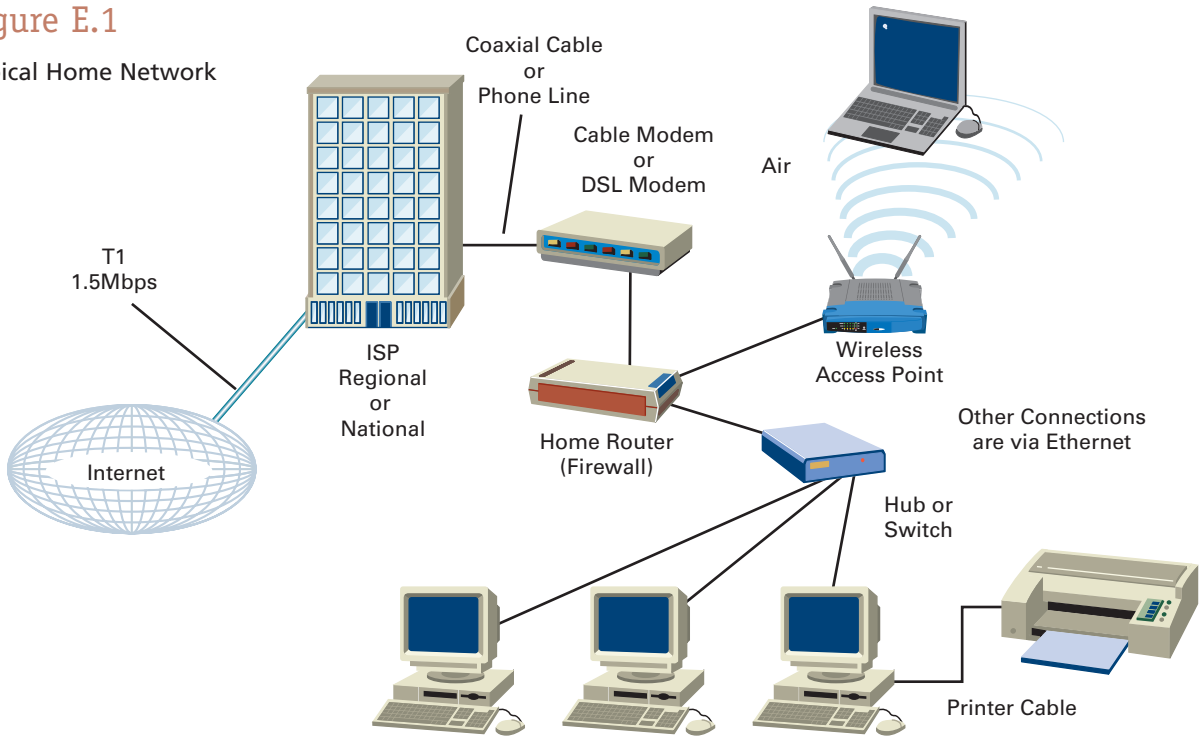


The most common transmission medium for a home network is Cat 5 cable, which is similar to phone cable (ordinary twisted-pair cable). ***Cat 5,*** or ***Category 5,*** cable is a better-constructed version of the phone twisted-pair cable. Each end of the Cat 5 cable has an RJ-45 connector. One end plugs into the Ethernet card in your computer and the other end into a network switch or broadband router (which we'll discuss in a moment).

If you'd like to access your home network wirelessly with your computer, you'll need another device on the network. A ***wireless access point (WAP)*** is a device that allows a computer to use radio waves to access a network. A wireless access point has a transmitter and a receiver for the bidirectional flow of information. It also has an antenna to capture the radio waves out of the air.

Figure E.1

Typical Home Network



If your wireless access point is a separate device, it connects to a wired network with a cable to the hub or switch the same way wired computers do (see Figure E.1). Many new broadband routers (described in the next section) come with a wireless access point built in, so you may not need any extra cables.

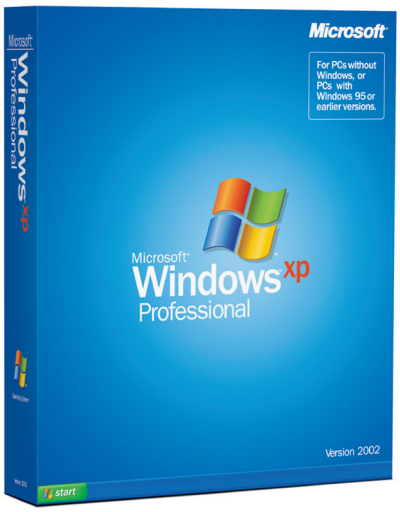
Your notebook and any other device that accesses the network wirelessly must have a wireless adapter. Wireless adapters are available as PC Cards for notebook computers, or sometimes come built into notebooks. The wireless adapter incorporates a transmitter, receiver, and antenna, just like the wireless access point. If all your devices have wireless adapters, you can create a completely wireless network, in which the only cable used is the one connecting to the cable or DSL service.

HOME INTERNET SERVICE AND BROADBAND ROUTERS

A home network with no outside connections can still be used to share files and printers. But in order to access any services or sites outside your home, you need Internet service and equipment to connect it to your home network. Two common types of home Internet service are DSL, available through your telephone company, and cable Internet connection, available from your cable company.

A DSL or cable modem connection is designed to support only one computer, so if you want to connect more computers, you need another device, commonly called a broadband router or home router. A ***broadband router*** or ***home router*** is a device to connect several computers together to share a DSL or cable Internet connection in a home or small office. It has one port to plug in your Internet connection, and usually has several ports to plug in home computers or printers.

Broadband routers are a rapidly changing part of the home network marketplace. Early models required an external DSL or cable modem, but some newer models include that built in. Early models had only one port for a computer and required a separate device to interconnect multiple computers. Many broadband routers today even include a built-in wireless access point.



NETWORK SOFTWARE

As always, when you have hardware you need software to make it work. For a small network, Windows will do fine (use version Windows 98 SE or newer) and must be installed on each network computer. To make the files on your computer available to the other computers on the network, you have to turn on the file-sharing option in Windows and indicate which drives, directories, or files to share. When you do this, the files on one computer will appear as additional folders on the other computer.

Network Components

Large networks are built in much the same way as small networks, using the same types of components. One difference is that home network devices often perform several different functions that are separated onto separate devices in large networks. Let's take a closer look at these different network components, and also look at how they're used in larger networks at corporations and universities.

HUBS

A ***hub*** is a device that connects computers together and passes messages by repeating all network transmissions to all the other computers. Because of this, only one computer on a hub can transmit at a time. A network built on a hub is also called a *shared* network, because all the computers share the entire network and have to take turns using it.

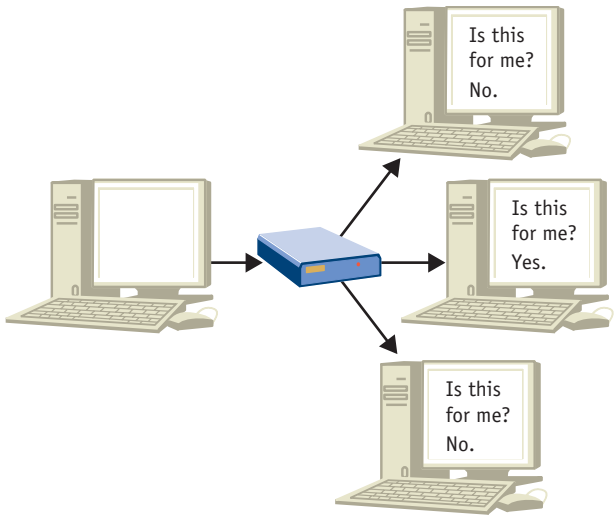
Imagine a building that has several offices, a manufacturing floor, and no telephones—only a public-address system. When the ordering clerk needs to check inventory, he or she pushes the button on the microphone, and the PA system broadcasts his or her voice over all the speakers in the building. Someone on the shop floor counts the supplies, goes to his or her microphone, and his or her voice is transmitted over every speaker in the building.

This is how hubs work, and you can see several problems with this approach. Only one computer can transmit at a time, because every message is sent to every computer, tying up every communications line. For the same reason, information transmitted over hubs isn't private—you wouldn't want your boss discussing your raise request with the Human Resources department over a set of loudspeakers that are heard throughout the entire building.

Hubs are also inefficient for the computers on the network to use, because every time a message comes across, they have to interrupt what they're doing to determine whether the message pertains to them (see Figure E.2). And finally, hubs can have *collisions,* when two computers decide to start sending at the same time. This garbles both of their messages, and they would have to stop sending and

Figure E.2

Hub



try again later. In fact, the more computers connected to a hub, the more frequently collisions happen, sometimes to the point that very little actual data gets transmitted.

Historically, hubs were very inexpensive compared to other types of network devices. They've been largely replaced by switches, but in spite of their shortcomings, they're still used in some home and small offices and in older business networks.

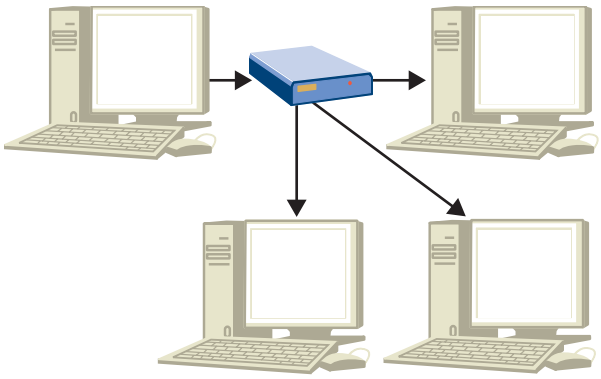
SWITCHES

A ***switch*** is a network device that connects computers and passes messages by repeating each computer's transmissions only to the intended recipient, not to all the computers connected. Several computers can have different conversations at the same time through a switch, and such a network is called a *switched* network.

A switch works like a small business telephone system. When the marketing director needs to check on the status of a brochure, she calls the graphic artist to ask about it. At the same time, the shop supervisor can be giving a delivery date to the shipping manager. And the telephones all have speakers, so the operator can still get everyone's attention all at once if necessary.

Figure E.3

Switch



You can see several advantages over hubs. Many data transmissions can happen at the same time, so a switch gives better support to a busy network (see Figure E.3). Information transmitted over switches is generally private, unless it's specifically meant to be broadcast to all the computers on the network. Likewise, computers on switches are more efficient than computers on hubs, because they only have to process messages actually meant for them, plus occasional broadcasts. And finally, switches don't have collisions, because different transmissions don't interfere with each other.

The advantages of switches are so great that switches have almost completely replaced hubs in new installations. Switches are the most commonly used components in networks today, and range in size from four- and eight-port models (connecting four or eight computers or printers) in home networks, to 24- and 48-port models (connecting 24 or 48 devices) common in business networks, to very large switches with hundreds of ports used to connect large call centers or run entire floors of office buildings.

ROUTERS

Routers connect together separate networks of computers, unlike hubs and switches that connect individual computers. A ***router*** is a device that passes network traffic between smaller *subnetworks* (or *subnets*) of a larger network.

Think of a large business with a warehouse in one building, management offices in another, and manufacturing in yet another. Long ago, each building had its own telephone system with its own extensions—the warehouse has numbers 100–199; management has extensions 200–299; and manufacturing has numbers 400–699.

At first, the telephone systems weren't connected, and the telephones would call only within the same building. But then the business ran telephone cables from each building to a central phone system to tie them all together. Now the warehouse phone system "knows" that if it gets a call for any extension other than 100–199, it routes the call to the central system to direct to the proper building. And the central system knows to route any call starting with 1 to the warehouse phone system, any call starting with 2 to management, and any call starting with 4, 5, or 6 to manufacturing.

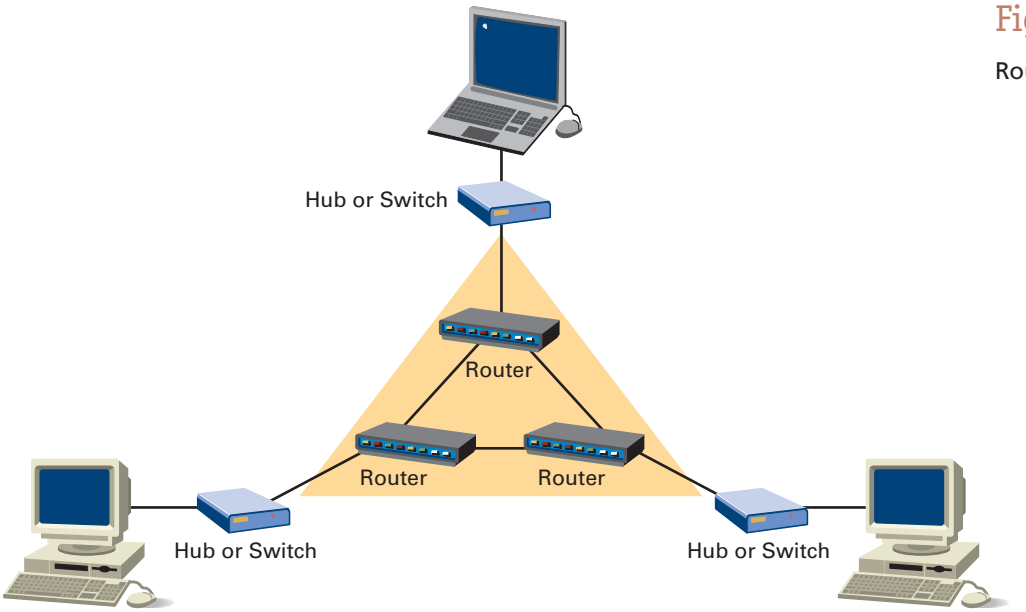


Figure E.4
Routers

Routers work the same way. When a computer wants to send a message to another computer on a different subnet (like in a different building), it actually sends the message to the router on its subnet. The router then looks at the message's destination address—where the message is going—and figures out how to get it there. Medium-sized networks may have only one router at the center, in which case it can always deliver messages directly. Larger networks may have many routers connected together, in which case messages may pass through several routers on their way from one computer to another (see Figure E.4).

It's important to understand that even though you have a router, you still need a hub or a switch to plug the computers into. Because large routers are expensive, it's not practical to build them with enough ports to directly support all the computers on a network. Home routers that run your Internet connection usually have both a router and a hub or switch built into the same box. But even though they may be labeled routers, remember that switching and routing are really two separate functions.

Hubs and switches can often be taken out of the box, hooked up to computers, and used without any configuration. But routers need to be programmed with information about which computer addresses are on which subnets, so installing a router generally requires someone with knowledge of network administration. Adding to or reconfiguring the network generally requires reconfiguring the router.

Classifying Networks by Distance

We've discussed the different devices used to build networks, and next we'll talk about ways networks are connected together. One way of describing large networks is in terms of the geographic area they cover. The size of a network can also impact whether an organization owns the communications lines or leases them from an independent provider.

LANs, WANs, AND MANs

A ***local area network (LAN)*** is a network that covers a building or buildings in close proximity, such as one campus of a university or corporation. The defining characteristic of a LAN isn't the actual size, but rather that the geographic area it serves is

continuous. So the large network on a two-square mile campus of an aircraft manufacturer would be considered all one LAN, but the small networks of a daycare center with two buildings a city block apart would be considered separate LANs.

A ***wide area network (WAN),*** then, is a set of connected networks serving areas or buildings not in immediate proximity to each other. Another way to think of a WAN is as a network of networks. WANs generally use routers to connect LANs together, just as LANs can use routers to connect different subnets together.

Imagine a business that's large enough to have a production plant near a railroad and trucking depot, and separate corporate headquarters in a downtown office park. It has separate telephone systems on each site—in fact, the production plant has separate telephone systems in the warehouse, the manufacturing building, and the packing and shipping plant. But they also have telephone lines connecting the production plant and the headquarters, and the telephone systems know how to send calls from one to the other. In fact, except for using a different type of telephone line, sending calls from one site to the other is set up exactly the same as sending calls from one building to another.

WANs work the same way to connect networks (LANs) on different sites. WANs may connect networks at different locations around a city, or in different cities across a state, a country, or even the entire world.

Because WANs connect areas that are some distance apart, organizations don't usually own the communications lines that WANs run over. Instead, the lines are usually leased, often from a telephone or cable television company, or other commercial communications provider. Some types of WAN circuits are 56 kilobits per second (56 Kbps) leased lines; T1, running at 1.544 megabits per second (1.544 Mbps); and DS3, running at 44.736 Mbps. (T1 and DS3 are described in more detail in this module under Internet Connection Types.)

A metropolitan area network is a relatively recent term for a specific type of WAN. A ***metropolitan area network*** or ***municipal area network (MAN)*** is a set of connected networks all within the same city or metropolitan area, but not in immediate proximity to each other.

Internet

An internet, with a lowercase *i,* comes from the word internetworking, and is a network of networks, connecting networks managed by different organizations. The largest internet of all is the ***Internet*** (with a capital *I*) which is a vast network of computers that connects millions of people all over the world.

To understand how computers send network communications across the Internet, consider the business described earlier that has telephone systems in separate buildings and on separate sites. When employees place calls to other buildings, each building's phone system directs the calls through a central system that knows how to route the calls to their destinations.

Besides the connections to the different buildings, the company also has connections to the public telephone system, so employees can make phone calls to place materials orders, and receive calls to accept orders for products. The company's outside telephone lines don't run directly to each building, but rather to the central system that knows how to route calls among all the buildings.

When employees at this company want to make outside calls, they dial a code starting with 9 (a digit different from the first digit of any of their local extensions), and the central system knows to route their calls over the outside lines to the public telephone system. And when customers call, they dial one of the company's telephone numbers,

and the public telephone system sends the calls over the company's outside phone lines to the central system, which routes the calls to the correct departments. If customers don't know the right phone numbers to call, they can look up the company's name in a telephone directory and find the numbers they need.

This is much the way the Internet works. When a computer needs to send a message to another computer somewhere else on the Internet, it sends the message to its local router. If the router doesn't recognize the recipient as being attached to one of its LAN, MAN, or WAN connections, it sends the message over the connection to its Internet Service Provider (ISP). The ISP has bigger routers that learn paths to get to even more networks. Even if they're not connected directly to the receiving network, the ISP's routers send the message to another router, which may send the message to still *another,* and so forth, until the message finally gets to the receiving network. There, the receiving router will at last deliver the message to the computer at the ultimate destination.

Computers and routers refer to each other using network addresses, commonly Internet Protocol (IP) addresses, like *192.168.1.1.* This is similar to the way telephone systems use telephone numbers, like *+1 (414) 555-1212,* to route calls. You probably remember the phone numbers of some of your friends and family, but no one knows all the different phone numbers in the world.

Similarly, you don't have to remember the low-level network address of every computer you send network messages to. Instead, you can use names for computers, like www.mhhe.com, and your computer looks up the receiving computer's address for you in a directory called the Domain Name System, or DNS. Without DNS, the Internet would be virtually impossible to use.

BANDWIDTH

The most common measurement used when comparing different types of communications media is bandwidth, which refers to capacity. ***Bandwidth,*** or capacity of the communications medium, is the amount of information that a communications medium can transfer in a given amount of time. You can think of bandwidth as the thickness of a drinking straw: the thicker the straw, the more quickly you can move the liquid from the cup into your mouth. In fact, in the communications industry, bandwidth is sometimes referenced informally as what size "pipe" you have between two locations.

Bandwidth is described as a quantity of data transferred in an amount of time, most commonly as a number of bits per second. A *bit* is the smallest possible amount of data, representing a single 1 or 0, and is abbreviated as the letter *b.* A *byte* is eight bits, and is used to store one letter or symbol of text, so the number of bits divided by eight gives you the approximate number of text characters. (See *Extended Learning Module A* for more information about bits, bytes, and characters.)

Bandwidth is sometimes represented in bits per second, abbreviated *bps.* Because a single bit is such a small quantity, and communications media speeds are constantly increasing, the bandwidth of different media is more likely to be represented in thousands of bits per second (kilobits per second—Kbps or kbps), millions of bits per second (megabits per second—Mbps), or billions of bits per second (gigabits per second—Gbps).

For example, if a particular communications medium has a bandwidth of 16 Mbps, then 16 millions bits can be transferred in a single second. This module has about 70,000 characters in it, which is approximately 560,000 bits, so it could be transferred in less than half a second across a 16 Mbps channel.

INTERNET CONNECTION TYPES

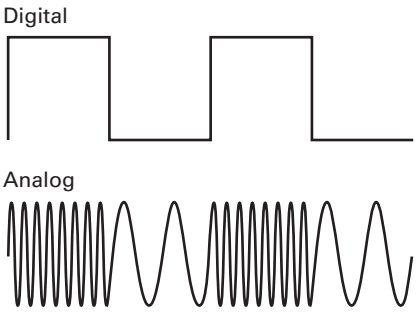
Like the circuits used to make wide-area connections, Internet circuits aren't usually owned by individual companies. Instead, the circuits are supplied by an Internet Service Provider. Types of Internet circuits include:

- Dial-up circuits, using an ordinary telephone line and a modem
- Digital Subscriber Line (DSL), which runs a high-speed connection over a telephone line without interfering with the voice telephone service
- Cable modem, which runs a high-speed connection over a cable television line without interfering with television reception
- Satellite modem, which runs a high-speed connection through your cable TV satellite without interfering with television reception
- Dedicated high-speed lines such as T1 and DS3, which run on separate circuits and are generally used for business connections

DSL, cable modem, and dedicated lines are classified as broadband connections. A ***broadband*** connection is a high-bandwidth (high-capacity) telecommunications line capable of providing high-speed Internet service. The Federal Communications Commission defines broadband as a capacity of 200 kbps (200 kilobits, or thousands of bits, per second) both upstream (to the Internet) and downstream (from the Internet). Other industry experts feel that broadband implies a speed of at least 750 kbps.

Figure E.5

Digital and Analog Signals



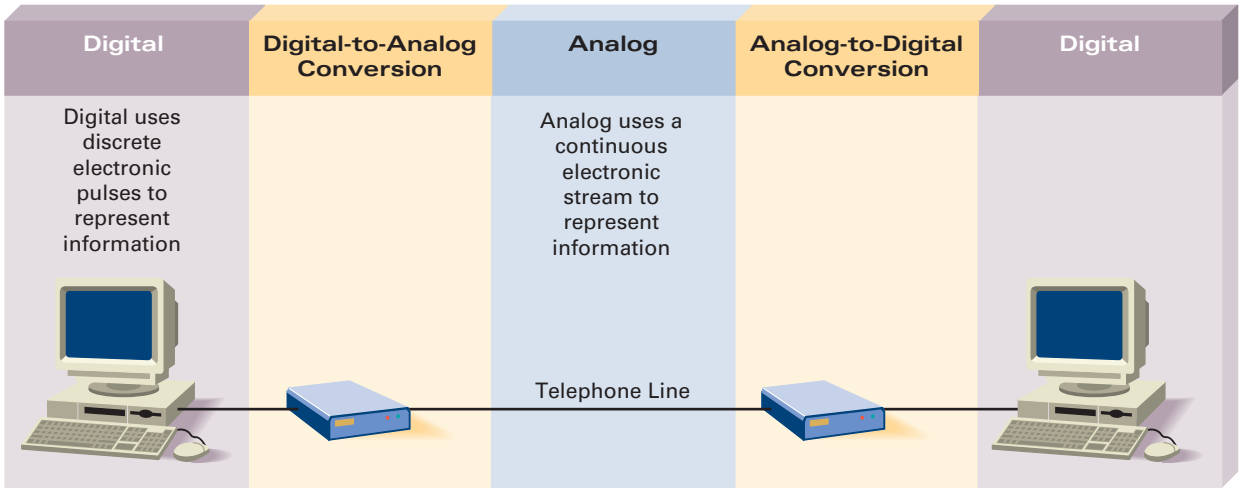
DIAL-UP CONNECTIONS

To make a telephone or dial-up connection, you need a computer, a phone line, a modem, and, of course, an Internet service provider. Just as people use telephones to talk over telephone lines, a ***telephone modem (modem)*** is a device that connects a computer to your phone line so that you can access another computer or network. And as it is with people and telephones, the computer at the other end needs a modem too.

A modem converts the digital signals from your computer into an analog form (by modulating the signal) that can be transmitted over a phone line, and then converts the analog signal back to digital signals (by demodulating the signal) for the computer at the receiving end of the transmission (see Figures E.5 and E.6). The word modem is a contraction of the modem's function of **mo**dulating outgoing and **dem**odulating incoming transmissions.

Figure E.6

The Role of a Telephone Modem



Modems are often integrated into the motherboards of new computers. If your computer doesn't have a built-in modem, you can buy a card to plug into an expansion slot of your desktop, or a PC card for your notebook. A modem is the slowest type of Internet connection you can get. The fastest possible transmission speed using a modem over a normal telephone line is 56 kbps, or about 56,000 bits per second.

DIGITAL SUBSCRIBER LINE

A ***Digital Subscriber Line (DSL)*** is a high-speed Internet connection using phone lines, which allows you to use your telephone for voice communication at the same time. There are different kinds of DSL systems, including ADSL or asymmetric DSL, SDSL or symmetric DSL, and HDSL or high-bit-rate DSL, that offer different combinations of speeds from the Internet provider to the customer and from the customer to the provider.

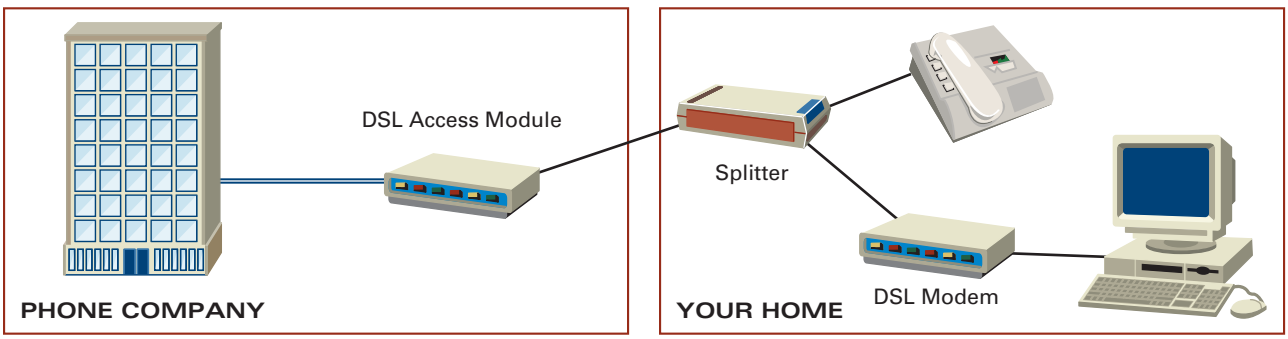
DSL works similarly to a traditional modem, modulating and demodulating the computer's digital signal into an analog form for transmission over the telephone line. However, unlike traditional modems which modulate into audible sounds (the screech you hear if you pick up a telephone while your computer is connected to the Internet through its modem), DSL modems use frequencies too high for you to hear; this is how they can allow telephone conversations to happen at the same time. Even so, DSL modems sometimes cause clicks, pops, or buzzing on telephone lines, so most DSL connections use a splitter or filter to make sure that only voice calls go to the telephone and only DSL signals go to the DSL modem (see Figure E.7).

Because the high frequencies used by DSL are outside the range that telephone lines were originally designed to carry, only telephone lines that meet certain criteria can deliver DSL service. You need to live within about three miles of the phone company. (In larger cities, phone companies have branch offices that can connect you throughout the metropolitan area.) The phone company may have restrictions about the type of equipment it uses to provide your phone line—a relatively recent central system, and a direct line to your house without any signal processing devices along the way. And the speed of your connection may depend on the distance to the phone company and the quality of your line. Speeds may vary from 144 kbps to 1.5 Mbps, or even up to 6 Mbps for a business-class DSL connection.

DSL circuits—the physical cabling to your house—are always provided by the phone company. The phone company usually provides the Internet service that you use over the DSL connection, too. However, in some areas, you may be able to buy your Internet service from an independent service provider instead. To connect to a DSL circuit, you need the filter or splitter provided by the phone company (to keep noise out of your telephone conversations) and the DSL modem. The cable from the DSL modem connects to your computer in one of two ways: either to an Ethernet card, or to a USB port.

Figure E.7

DSL Internet Access



DSL service has three big advantages over dialup connections:

1. DSL is much faster—up to 30 times faster than a traditional modem.
2. You can use the line for voice calls at the same time.
3. DSL can be an always-on connection—because it doesn't interfere with voice calls, you can leave it connected all the time, instead of having to wait for your modem to connect each time you want to use the Internet.

CABLE MODEM

If you have wired cable television, you know it comes into your home on a coaxial cable that connects to your television set. This same cable can connect you to the Internet, too. Both cable TV signals and your Internet connection travel from the cable company on one wire.

A splitter at your home splits the signals on the incoming cable, sending one part to the TV and the other to your cable modem. A ***cable modem*** is a device that uses your TV cable to deliver an Internet connection (see Figure E.8). The cable from the cable modem attaches to either an Ethernet card (an expansion card that connects your computer to a network) or to a USB port in your computer. Like DSL, cable modems provide an always-on connection. However, unlike DSL, cable modems don't use a phone line at all.

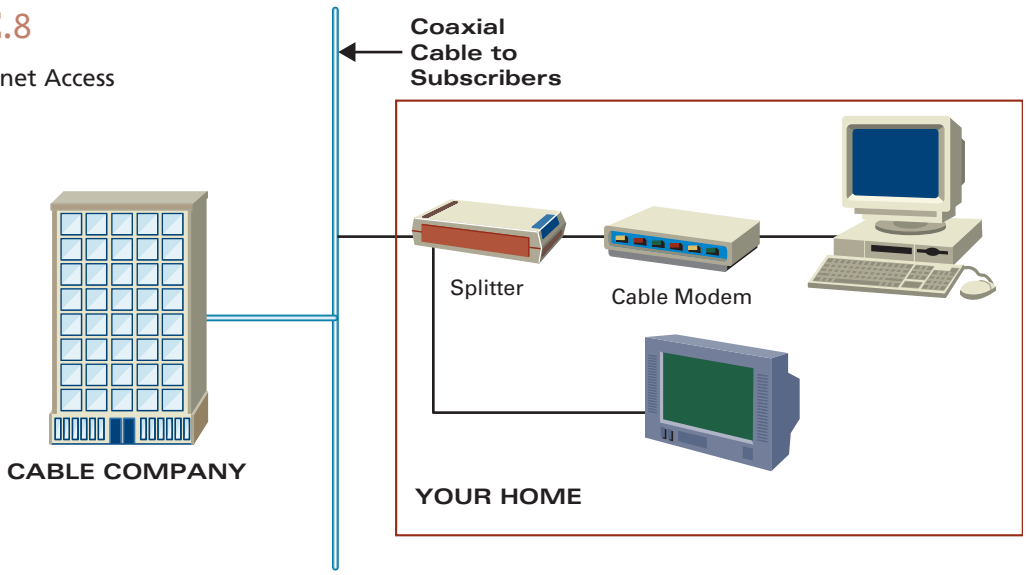
The speed of transmission with a cable modem is much faster than a phone modem, running at about 10 Mbps (10 million bits per second). While the speed of a DSL connection is guaranteed, though, the speed of a cable Internet connection depends on how many users are online, because the connection to the cable company is shared throughout a neighborhood. If all your neighbors are surfing the Web with a cable connection at the same time you are, you may notice a reduction in your access speed.

SATELLITE MODEM

If you have wireless cable television, that is, if you receive your cable programming via a satellite, you can often also obtain your Internet service through the same provider of your satellite cable. A ***satellite modem*** allows you to get Internet access from your satellite dish. In certain instances, you may not be receiving your cable programming via satellite, but you may be able to receive your Internet service via a dedicated satellite dish. It really all depends on where you live and what types of services are offered for cable programming and Internet service.

Figure E.8

Cable Internet Access



The concept and implementation of receiving your Internet service from your satellite cable programming provider are the same as for using a cable modem. You would have a splitter with wiring for your cable programming going to your television and wiring for your Internet service going to your computer or a connecting device such as a hub or router.

T1, DS3, FRAME RELAY, AND ATM

A ***T1*** is a high-speed circuit typically used for business connections, running at speeds up to 1.544 Mbps (1.544 million bits per second), and a ***DS3*** is a high-speed business network circuit running at 44.736 Mbps. T1s were originally designed to carry 24 telephone conversations on phone companies' long-distance lines between cities. Later, equipment was developed to connect computer networks over T1 and DS3 lines. A T1's speed of 1.544 Mbps is about 24 times the speed of an analog telephone modem. A DS3 line is equivalent to 28 T1 lines bundled together, and its total speed of 44.736 Mbps is about 672 times the speed of an analog modem.

With some providers, a portion of the price of T1 and DS3 lines depends on the distance they run. Because of this distance-based pricing and their overall higher cost than some other connection types, T1 and DS3 lines are most commonly used for metropolitan area network connections—between two branches of a business within the same city. One advantage of T1 lines is that, because of their origin in voice telephony, it's possible to split their 24 channels between voice and computer communications, using the same T1 circuit to connect both telephone systems and computer networks at two offices.

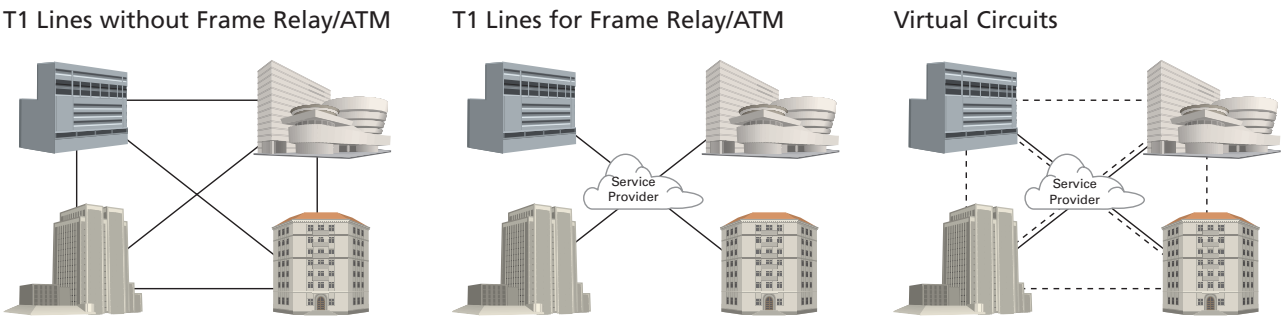
Frame Relay and Asynchronous Transfer Mode (ATM) are services that the phone company or other telecommunications providers can set up over high-speed lines like T1s and DS3s to create "virtual circuits" connecting multiple offices. These virtual circuits can provide network connections from each office to every other one without having to run physical lines directly between each pair.

For example, if a business had four offices that all needed to be connected to each other, it would take six T1 lines to hook them all up (see Figure E.9). With Frame Relay or ATM, each office has a single T1 line going to the communications provider (for a total of four), and the provider makes it work the same as it would if the six direct lines actually existed.

Remember that the price of T1 and DS3 lines can depend on the distance they run. With Frame Relay or ATM, the T1 or DS3 lines actually run from each office to the telecommunications provider, rather than from office to office, so the distance and price can both be lower than when T1 lines are run directly from office to office.

Figure E.9

Frame Relay/ATM Virtual Circuits



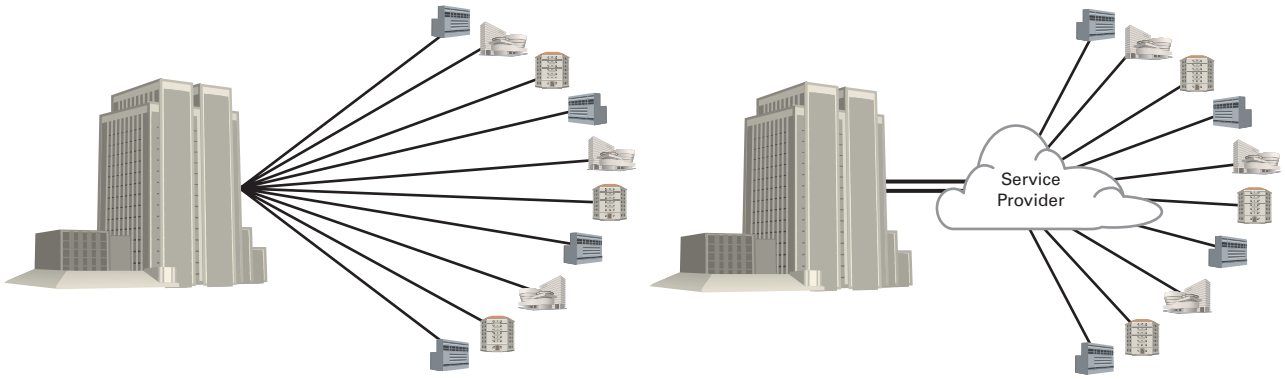


Figure E.10

Frame Relay/ATM Circuit Aggregation

Because of this, Frame Relay and ATM are also used to connect many branch offices to a single main office. If a business had 10 branch offices, it would take 10 T1 lines to connect all the branches back to the headquarters (see Figure E.10)—each potentially running a great distance. With Frame Relay or ATM, the business can instead install a DS3 from its headquarters to the communications provider and a T1 to each branch office. The provider makes it work as it would if the headquarters had a direct connection to each branch office, and the business potentially spends less money than if it ran all of the T1 lines directly between offices. And the company has a single DS3 connection at its headquarters instead of 10 separate T1 connections, simplifying circuit management and potentially increasing reliability.

VOICE OVER IP

We've just talked about different types of communications lines that can carry network information, but now it's time to turn that inside out. Several types of communications lines—telephone lines, T1s, and DS3s—were originally developed to transmit voice telephone calls, and later adapted to carry computer data. Voice over IP (VoIP) does the opposite—it's a means of transmitting a voice telephone call over a computer data network. ***Voice over IP (VoIP)*** allows you to send voice communications over the Internet and avoid the toll charges that you would normally receive from your long-distance carrier.

Why go to the trouble of sending voice calls over a computer network when they can already be sent directly through existing telephone systems and services? The answer has everything to do with overhead and with metered billing, meaning you pay an additional amount for each call and/or for each minute of the call.

Offices in most businesses and universities today have at least two different cables run to them—one that goes back to a telephone system, and one that goes back to a network hub or switch. On many telephone systems, the telephone extension number is assigned to a particular port on the central equipment. So when an employee moves from one office to another, making his or her telephone extension work in the new office involves either changing wiring or reprogramming the phone system.

In contrast, network addresses are assigned directly to the computer or other device, regardless of which switch or hub port it's connected to. So moving a VoIP extension from one office to another is as easy as unplugging the network phone from one location, carrying it to another, and plugging it back in. This reduction of maintenance effort can dramatically reduce the overhead of telephone system operation during office expansions and moves. Additionally, office technicians no longer have to maintain two sets of wiring to two different systems, which can also reduce overhead.

Both network companies like Cisco Systems and telephone companies like Nortel are producing VoIP telephones that look like any other business phone, except they plug into a network jack instead of a telephone jack. Many even have an extra network jack on them for your PC, so your phone and computer can share a single connection back to the building's hub or switch.

Voice over IP is also starting to gain popularity with home users across the Internet. In most parts of the world, traditional telephone calls made from one local dialing area to another have metered billing, and some large U.S. cities even have metered billing for local calls.

Network access is often unmetered, though, particularly for broadband home access (cable modem and DSL). If you already have an Internet connection, you can use a network telephone or network phone software for your PC to make calls to other VoIP users anywhere in the world at no additional cost per call or per minute—for the moment, anyway. Most telephone billing rates in the United States are set by federal and state governments by regulations called tariffs, and it remains to be seen how long it will be before Voice over IP becomes tariffed as well.

Network Communications Media

The objective of networks and telecommunications is to move information from one place to another. This may be as simple as sending information to the office next door, or as far-reaching as sending a message to the other side of the world. Whatever the case, information must travel over some path from its source to its destination. ***Communications media*** are the paths, or physical channels, in a network over which information travels.

All communications are either wired or wireless. ***Wired communications media*** transmit information over a closed, connected path. ***Wireless communications media*** transmit information through the air. Forms of wired and wireless communications media include:

Wired

- Twisted-Pair Cable
- Coaxial Cable
- Optical Fiber

Wireless

- Infrared
- Microwave
- Satellite

WIRED COMMUNICATIONS MEDIA

Wired communications media are those which tie devices together using cables of some kind. Twisted-pair, coaxial cable, and optical fiber are the types of cabling you'd find in computer networks.

TWISTED-PAIR

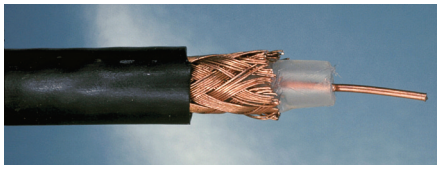
Twisted-pair cable is a bundle of copper wires used for transmitting voice or data communications and comes in several varieties. The Cat 5 that you already read about in connection with home networks earlier in this module is one type. Most of the world's phone system is twisted-pair and since it's already in place, it's an obvious choice for networks.

The simplest type of twisted-pair phone cabling (Cat 1) provides a slow, fairly reliable path for information at up to 64 kilobits per second (Kbps), while a better type (Cat 3) provides up to 10 megabits per second (Mbps). However, distance, noise on the line, and interference tend to limit reliability

for most types of twisted-pair cabling. For example, a crackle that changes a credit card number from 5244 0811 2643 741 to 5244 081**0** 2643 741 is more than a nuisance; in business it means retransmitting the information or applying a charge to the wrong person's credit card.

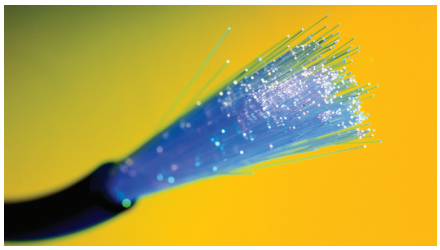
Cat 5 or Category 5 provides a much higher bandwidth than ordinary phone cable, meaning it carries more information in a given time period, at least for distances up to 100 meters. It's commonly used for connections at 100 megabits per second (Mbps), and an enhanced version called Category 5e is capable of carrying 1 gigabit per second (Gbps). Cat 5 is relatively inexpensive and is fairly easy to install and maintain. Because of these advantages, it's the most widely used cabling for data transfer in today's LANs. Note, however, that twisted-pair of any kind is relatively easy to tap into and so it's not very secure. It's even possible to access the information by simply detecting the signals that "leak" out.

COAXIAL CABLE



An alternative to twisted-pair cable is ***coaxial cable (coax),*** which is one central wire surrounded by insulation, a metallic shield, and a final case of insulating material. (Coax is the kind of cable that delivers cable television transmissions and also carries satellite TV from the dish to your house.) While coaxial cable was once the cable of choice for internal LAN wiring, it has been almost completely replaced by twisted-pair cable. Coaxial cable is capable of carrying at least 500 Mbps, or the equivalent of 15,000 voice calls, simultaneously. Because of its shielded construction, coaxial cable is much less susceptible to outside interference and information damage than twisted-pair cable. However, coaxial cable is generally more expensive than twisted-pair and is more difficult to install and maintain. Security is about the same with coaxial cable as with twisted-pair, except that the radiation, or leaking, of information is much less. Coax is commonly used for leased line private networks.

OPTICAL FIBER



The fastest and most efficient medium for wired communication is ***optical fiber,*** which uses a very thin and flexible glass or plastic fiber through which pulses of light travel. Information transmission through optical fiber works rather like flashing code with a light through a hollow tube.

Optical fiber's advantages are size (one fiber has the diameter of a human hair); capacity (easily hundreds of gigabits per second, and getting faster every year); much greater security; no leakage of information. It's very hard to "tap" into optical fiber. Attempts are pretty easy to detect since installing a tap disrupts service on the line—and that's noticeable. Optical fiber is also used for nearly all connections between different buildings, as it doesn't conduct electricity and so is immune to damage from lightning strikes. Optical fiber is more expensive than twisted-pair cable, however, and requires highly skilled technicians to install and maintain.

WIRELESS COMMUNICATIONS MEDIA

For many networks, wired communications media are simply not feasible, especially for telecommunication across rugged terrain, great distances, or when one or more parties may be in motion. For whatever reason, if wired communications media don't fit your needs, wireless may be the answer. Wireless communications radiate information into the air, either very narrowly beamed or in many directions like ripples from a pebble tossed into a pond. Since they radiate through the air, they don't require direct cable

TEAM WORK

WHAT'S THE BIG DEAL WITH FREQUENCIES?

A radio wave is an electromagnetic wave sent out by an antenna. Radio waves have different frequencies, and by tuning a radio receiver, a cell phone (which has a receiver), or a baby monitor (which also has a receiver) to a certain frequency you can pick up a specific signal. Frequencies are measured in KHz (kilohertz—thousands of cycles per second), MHz (megahertz—millions of cycles per second), and GHz (gigahertz—billions of cycles per second).

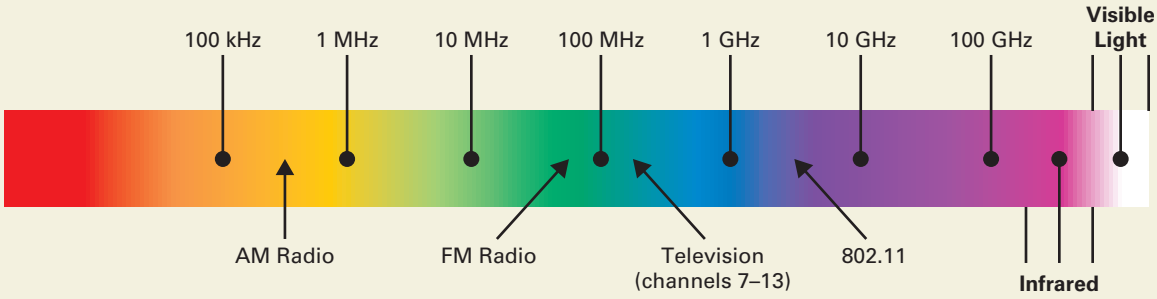
You may have heard that there is a fixed number of frequencies and competition for control of those available is fierce. All wireless devices require a radio frequency to transmit and receive, so communications companies spend billions of dollars for the rights to part of the spectrum that's for sale. Other parts are designated for public use (like the WiFi part), and still others are set aside for government agencies like the Department of Defense.

The figure below shows the part of the spectrum in common use for wireless information delivery. Here are some common frequency bands:

- FM radio: 88 megahertz to 108 megahertz
- AM radio: 535 kilohertz to 1.7 megahertz
- Television stations: 174 to 220 megahertz for channels 7 through 13.

Place on the spectrum the following wireless services:

A. WiFi
B. GPS devices
C. Microwave ovens
D. Police radar guns
E. TV channels 2–6
F. Wildlife tracking collars
G. CB radio
H. Aviation navigation
I. Cordless phones



connections of any kind. Obviously, security is a big problem since the information is available to anyone in the radiation's path. However, wireless encryption methods are good, and getting better.

INFRARED AND BLUETOOTH FOR VERY SHORT DISTANCES

Infrared is the oldest type of wireless communication. ***Infrared*** uses red light to send and receive information. The light is invisible to humans, but snakes and some other animals can see it. Your TV remote control uses infrared. You can use infrared to connect handheld devices, such as pocket PCs, to peripheral devices such as printers. Wireless keyboards and mice usually connect to your PC with an infrared link. Infrared communication is totally line-of-sight, meaning that you can't have anything blocking the path of the signal, or it won't work. Infrared transmission has very limited bandwidth (typically 1 Mbps).

A relatively new and competing wireless technology is called Bluetooth. Named for a Viking king, ***Bluetooth*** is a standard for transmitting information in the form of short-range radio waves over distances of up to 30 feet and is used for purposes such as wirelessly connecting a cell phone or PDA to a computer. Virtually all digital devices, like

keyboards, joysticks, printers, and so on, can be part of a Bluetooth system. Bluetooth is also adaptable for home appliances like refrigerators and microwave ovens.

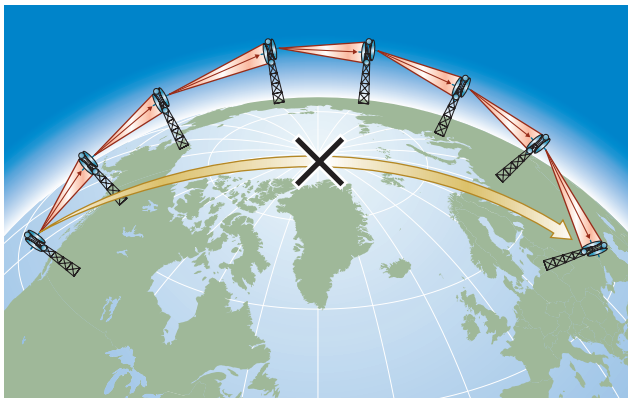
OMNIDIRECTIONAL MICROWAVE (WIFI) FOR SHORT DISTANCES

Another method of short-distance wireless communications is omnidirectional (all directions) microwave transmission. ***Microwave transmission*** is a type of radio transmission. Microwaves occupy a portion of the electromagnetic spectrum between television signals and visible light. (See the Team Work exercise on page E.17.) Microwave ovens use high-powered microwaves to heat food, and can interfere with some types of microwave wireless transmissions.

The most common types of wireless networking used today—802.11b and 802.11g (known to most people as WiFi)—use microwave transmissions. ***WiFi (wireless fidelity)*** is a standard for transmitting information in the form of radio waves over distances up to about several miles. WiFi is actually a wireless industry alliance that provides testing and certification that 802.11 devices communicate with each other properly. *IEEE 802.11b* and *802.11g* are two versions that run at 11 Mbps and 54 Mbps, respectively.

Figure E.11

Microwave

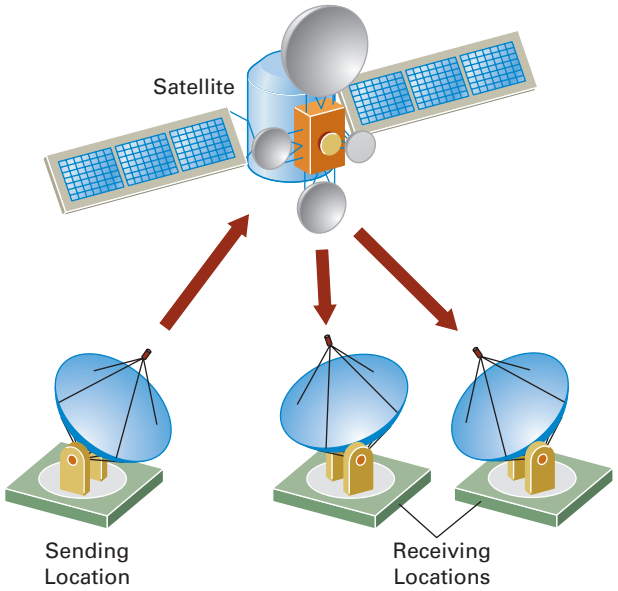


DIRECTIONAL MICROWAVE FOR MEDIUM DISTANCES

Microwaves may be transmitted very directionally with a parabolic dish antenna or can be radiated in a wide curved path for broader use. Microwave transmission is a line-of-sight medium. That is, the microwave signal cannot follow the curved surface of the earth. So to send the information over a distance of more than about 20 miles you'd have to use repeaters (see Figure E.11). A ***repeater*** is a device that receives a radio signal, strengthens it, and sends it on. (You've probably seen microwave towers—they're the tall towers with lots of little dishes on them that stand near an industrial complex.) Microwave signals have difficulty getting through walls or trees or other solid objects, so there must be a clear path from sender to receiver.

Figure E.12

Satellite



SATELLITES FOR LONG DISTANCES

Communications satellites are microwave repeaters in space. They solve the problem of line-of-sight since the transmission shoots up into the sky in a straight line, bounces off, and shoots back down to earth again (see Figure E.12). Since satellites are so high, an array of them can cover essentially the whole earth (as the two dozen or so GPS satellites do). As with land-based repeaters, satellites receive information from one location and relay it to another. You'd usually use satellite communications to connect land-based networks in far-flung locations or to connect moving vehicles to each other or to the organizational network.

Satellite communications are cost effective for moving large amounts of information, especially given a large number of receiving sites. For example, K-Mart and other retailers place very small aperture terminal (VSAT) satellite dishes on the roofs of their stores. The VSATs allow individual stores to transmit information to the home of-

fice, and the home office, in turn, can transmit information to all the stores simultaneously. Satellite radio is another example of far-flung satellite transmission. If you have satellite radio in your car, you'll never be completely out of range of your favorite satellite radio station.

Network Security

Thinking about network security may call to mind images from movies of computer rooms criss-crossed by laser beams, voice and handprint recognition, security cameras, and CDs or DVDs full of top-secret blueprints. Or it may make you think of jumpsuit-wearing technicians clipping wires onto someone else's connection, greasy-haired teenagers illuminated only by the green glow of their computer monitors, or an investigator frantically trying to guess the criminal's password as the footsteps in the hallway get ever closer.

These images, although dramatic, don't give you much of an idea of the real threats to computer and network security and how to guard against them. In reality, connecting computers together can make it easier to take advantage of existing security weaknesses—attacks can be performed from any distance away instead of only from within the same room—and introduces some new weaknesses.

PRINCIPLES OF COMPUTER SECURITY

The best way to understand network security is to look at the components of computer security, evaluate different threats in terms of these components, and then figure out how to reduce the effectiveness or damage of those threats. The basic principles of computer and network security are confidentiality, authenticity, integrity, and availability.

CONFIDENTIALITY

Confidentiality means that information can be obtained only by those authorized to access it. In even simpler terms, it means keeping secrets secret. Confidential information includes things like bank statements, business plans, credit card reports, and employee evaluations. Threats to confidentiality include network transmissions that can be captured or monitored by unauthorized individuals, passwords that are easily guessed, and even printouts left lying out in plain sight. In the world outside of computers, confidentiality is protected by sealing envelopes and locking doors and file cabinets.

AUTHENTICITY

Authenticity means that information really comes from the source it claims to come from. It's important to be sure of the authenticity of things like military orders, medical diagnoses, and buy/sell directions to your stockbroker. Threats to authenticity include fraudulent e-mail messages claiming to be from your bank (probably spoofing), Web sites registered at names that are common misspellings of popular sites, and Web browsers that can be manipulated into making it look as though you're at a different site than you really are. Nonelectronic authenticity is provided by signatures (although they can be forged), or by trusting only people you know personally.

INTEGRITY

Closely related to authenticity, ***integrity*** means that information has not been altered. You would be concerned about the integrity of your bank balance, contents of your corporate Web site, medical prescriptions, and credit card charges. Threats to integrity include network transmissions that can be forged or taken over by unauthorized individuals and Web servers with flaws that allow their content to be replaced. Integrity is hard

to guarantee in the physical world—how can you *really* be sure that no one has changed even a single word of your mortgage contract?—and is generally dependent on a certain degree of trust that's much harder to apply to electronic communications.

AVAILABILITY

Finally, availability means simply that a service or resource is available when it's supposed to be. If a mail-order Web site is unavailable during the Christmas season, a retailer could lose millions of dollars in sales. If a corporate e-mail server is frequently unavailable, the company may lose some of the trust of its business partners. Threats to availability include unintentional network failures, poorly written server software that stops working when presented with unusual inputs, and deliberate attempts to send so much traffic to a company's network that legitimate communications are unable to get through. Noncomputer-related availability is provided by designing buildings with multiple exits in case one is blocked by fire, making photocopies of important documents, and installing electrical generators in hospitals to keep life-critical equipment operating if the city power fails.

FIREWALLS AND INTRUSION DETECTION SYSTEMS

Networks are designed to connect computers together and move information between them. But what if attackers are trying to break into your computers through your network connection? Just as a company may install card readers or hire a guard to admit only staff wearing employee badges, a ***firewall*** is software and/or hardware that protects a computer or network from intruders. As hardware, a firewall is a device that permits or denies network traffic based on security policy. Firewalls provide protection against threats to *confidentiality, authenticity,* and *integrity* by blocking traffic that doesn't look like legitimate access to networked computers.

Some firewalls make their policy decisions based entirely on network addresses. For example, if you have caller ID on your telephone, you may choose to answer calls only if they come from your friends or family. Likewise, a simple firewall can examine network traffic and permit only the traffic coming from a known source.

Other firewalls may permit traffic from an unknown source if it appears to be a response to a request that was made by a computer on the protected network. For example, if you call a friend at the office but she's in a meeting, you might leave a message for her to call you back. When she does, you may recognize the phone number of her office as a number you just called and answer the call, even though the office number isn't on the list of phone numbers you'd normally answer.

Even more advanced firewalls make decisions based on the content of the network traffic. Thinking back to the company with a security guard in the lobby, the guard may allow a delivery person to enter the building if he's carrying envelopes or pizza, but not if he's carrying dynamite or bottles of acid. Of course, acid may be a regular delivery item in a chemical plant; not every company will want the same firewall policies.

While a firewall typically has a predefined policy about the network traffic it will allow and deny, an ***intrusion detection system (IDS)*** is a device that watches network traffic for intrusion attempts, reports them, and optionally takes action against them. Intrusion detection systems work by having information about many different types of network attacks and matching the current network traffic against their lists of attack characteristics. When they sense an attack in progress, they can e-mail or page network administrators about the attack, so they can take appropriate action. Some intrusion detection systems can even add policies on the firewall to block the source of the attack.

Denial-of-service attacks simply interfere with network *availability.* A ***denial-of-service (DoS)*** attack floods a server or network with so many requests for service that it

slows down or crashes. (See *Extended Learning Module H, Computer Crime and Forensics,* for more details about denial-of-service attacks.) Imagine if someone called every pizza delivery service in town and ordered 20 pizzas delivered to your office. Eventually you'd manage to sort out the confusion and you wouldn't have to pay for the pizzas, but meanwhile you'd be too busy dealing with the situation to get any work done.

Firewalls and intrusion detection systems can protect *availability* by preventing or reducing the effect of denial-of-service attacks. Some denial-of-service attacks use network capabilities that are technically permissible, but are almost never seen in legitimate network traffic; these attacks are easy to foil by denying those types of traffic. Other denial-of-service attacks send completely legitimate but useless traffic. Blocking those attacks involves recognizing an increase in network traffic beyond normal levels, determining the source or sources, and then blocking even legitimate-appearing traffic from those locations.

Most home broadband devices—for DSL and cable modem Internet connections—include a simple firewall. Home networking manufacturers have been packing more and more capabilities into their products, and even though the devices may be marketed as routers or firewalls, they generally contain a router, a firewall, and a switch or hub to connect multiple home computers. Some even include the DSL or cable modem, and some have a wireless access point, all in a device not much larger than a paperback book.

ENCRYPTED COMMUNICATIONS: SSL AND VIRTUAL PRIVATE NETWORKS

Earlier, we talked about types of network devices on which communications can be overheard—hubs and wireless access points. This is a threat to *confidentiality*—unauthorized individuals could be watching your communications. So if you're using wireless access, or are in a location where you don't know whether you're connected to a hub or

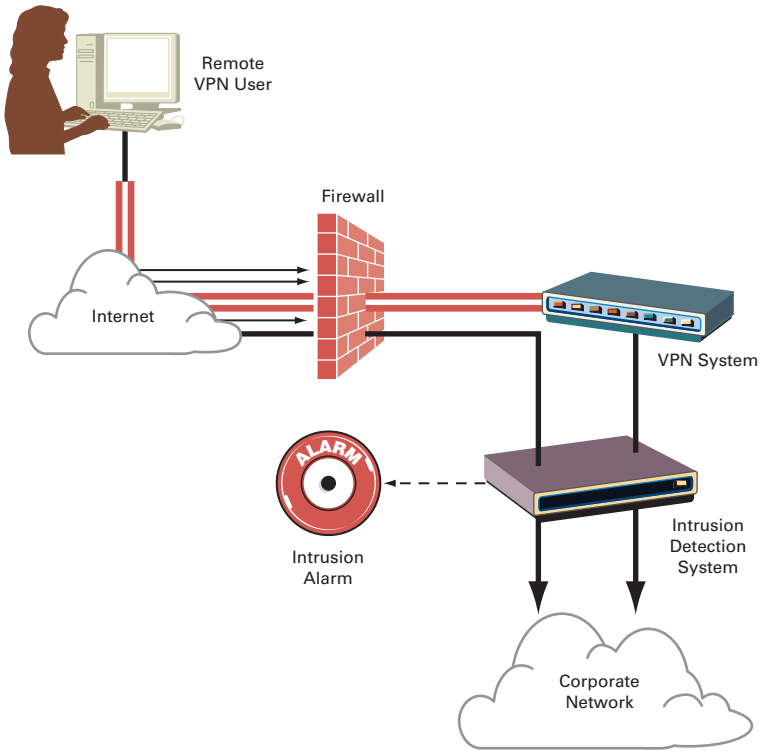


Figure E.13

Firewall, Intrusion Detection System, and Virtual Private Network

a switch—or simply somewhere that you don't know who has access to the communications lines and equipment between you and your network destination—what can you do to protect the privacy of your communications?

The solution is encrypted communication. ***Encryption*** scrambles the contents of a file so that you can't read it without having the right decryption key. It means scrambling your communication in such a way that only the intended recipient can unscramble it. If you wanted to send the message, "Reschedule the grand opening for April 10," the encrypted version might look like

V`9:P)9@A1,||>[D:J_sepnvIf.Xj2FAs_[Dhud+'.

One way of using encryption to protect network transmissions is called Secure Sockets Layer (SSL), or somewhat less commonly, by the name of its successor, *Transfer Layer Security (TLS)*. SSL is a security technology that encrypts each network conversation—between one network client and one server—individually. Web traffic using SSL is called https, instead of just http. When you browse to a secure Web site and see the padlock icon, it's telling you that your browser is using SSL/TLS to encrypt your communications with the Web server. We cover more on SSL and other types of security technologies with respect to electronic commerce in Chapter 5.

In contrast, a ***virtual private network (VPN)*** uses encryption to protect the confidentiality of *all* network transmissions between two endpoints. Typically, one endpoint is a large office or headquarters, and the other endpoint may be a single computer, or it may be another office. All network communications between the two locations are routed through the VPN to be encrypted. This makes it look as though they have a dedicated network connection between them, even though they may really be communicating over public network links, hence the name, *virtual private network* (see Figure E.13).

OTHER SECURITY THREATS: MALWARE

You've probably heard of computer worms, viruses, and spyware, collectively known as malware. ***Malware*** is a contraction of **mal**icious soft**ware,** and refers to software designed to harm your computer or computer security. Malware existed even before most computers were connected to networks, but increased connectivity between computers has made it dramatically easier for malware to transfer to new victims.

A ***virus*** is software that is written with malicious intent to cause annoyance or damage. The virus software is activated unintentionally by the computer user. A ***worm*** is a type of virus that replicates and spreads itself, not just from file to file, but from computer to computer via e-mail and other Internet traffic. Viruses spread by tricking users into running them, for instance, by pretending to be an interesting program or e-mail message; worms spread by taking advantage of errors or weaknesses in computer programs. Viruses and worms most commonly threaten *availability,* by damaging or removing files, or by tying up a computer doing so much unauthorized work that it can't get its real job done.

Viruses and worms can be countered by running anti-virus software. Anti-virus software works very similarly to the intrusion detection systems described earlier. It has a long list of characteristics of known worms and viruses, and when it sees files being transferred or software running on the computer that has those characteristics, it alerts the user and often "quarantines" the file to part of the hard drive where it can't do any harm. Some anti-virus software can even remove the malicious instructions from computer files so that they are still useful once they're disinfected.

Anti-virus software can be run at different places in the network. Some viruses are transferred from computer to computer in e-mail messages, and anti-virus software on the e-mail server will help protect against them. It's very important to run anti-virus software on every PC, to protect against worms and viruses trying to attack the computer directly. And some companies have servers where customers can upload purchase orders or problem reports; they may run anti-virus software on those servers to screen all incoming files.

Spyware is a more recent type of malware than viruses and worms. ***Spyware*** (also called ***sneakware*** or ***stealthware***) is malicious software that collects information about you and your computer and reports it to someone else without your permission. Therefore, spyware is a threat to *confidentiality*. Spyware most often gets installed on your computer secretly along with a piece of software you knew you were getting; for example, some peer-to-peer file sharing programs are notorious for including spyware.

The best defense against spyware is to install software only from trustworthy sources, but that can be hard to determine. Anti-spyware software is available that works just like antivirus software, recognizing patterns of known spyware and removing them from your computer. Two popular anti-spyware programs are Ad-Aware (www.lavasoftusa.com) and Spybot Search & Destroy (www.safer-networking.org).

Another category of malware is servers and bots. Sometimes after breaking into a computer, attackers will set up *unauthorized* servers. These servers are often used to distribute illegal copies of movies, music, and software, or may even be used to distribute kits for breaking into other computers.

In the context of malware, *bots* are programs designed to be controlled by an attacker to perform unauthorized work over a period of time. Some bots are used to send spam, making it look like it's coming from the victim's computer instead of from the attacker's. Other bots try to break into computers or perform denial-of-service (DoS) attacks against other networks or systems.

Bots and unauthorized servers can sometimes be detected by anti-virus or anti-spyware software—but they may be indistinguishable from legitimate servers. They can also sometimes be discovered by network intrusion detection systems. Sometimes they're even discovered by network administrators, noticing an unusual amount of network traffic coming from a single computer.

The Client/Server Software Model

So far, we've talked about how computers are connected together on networks without discussing the roles of the computers themselves. In the peer-to-peer home networks described at the beginning of the chapter, the computers were all equal. Each one had its own files and devices, which it could share with the other computers. But, unless you're a business with very few computers, you'd probably use a client/server network instead of a peer-to-peer network.

A ***client/server network*** is a network in which one or more computers are servers and provide services to the other computers, which are called clients. The server or servers have hardware, software, and/or information that the client computers can access. Servers are usually powerful computers with large storage systems. Depending on the network, the server could be a high-end PC or a minicomputer and large companies often have several servers, each of which may provide services to different parts of the company. It's usually cheaper and more efficient to have software on a server where everyone can access it:

- A network license allowing a fixed number of people or everyone on the network to use a software package is usually cheaper than buying separate copies of software for each computer.
- It's easier to update one server copy of software than to update hundreds or even thousands of separate copies.
- Control and security of software and information are easier if they're on the server.

The parts of the network that connect the servers are usually built with stricter specifications than the parts that connect the clients. The servers' network equipment may have

- Higher-bandwidth connections, to carry the traffic from many clients across the company accessing the servers simultaneously.
- Higher-powered network processors, to route the greater traffic loads.
- Duplicate connections to the rest of the network, to provide continued service if one connection is accidentally or maliciously cut.
- Uninterruptible power supplies, which use batteries to keep the network running even when the power fails.

CLIENT/SERVER—A BUSINESS VIEW

The term client/server network can mean a network structure, that is, one or more computers providing services to other computers. However, client/server is a term that also describes a business model. As a business model, client/server describes distributed processing. That is, it describes where processing takes place. Different companies have different processing needs. For example, if your school has an online system on which you can check your grades, you'll probably find that you can't change grades at your end—access to that kind of processing is severely restricted. On the other hand, a bank employee would need to be able to process a loan at his or her computer.

You can use one of five basic client/server implementation models. Which one you use depends on your business environment and where you want processing implemented. Client/server networks differ according to three factors:

1. Where the processing for the presentation of information occurs, that is, where the information that you see on the screen or printout is formatted, and the editing of information as you enter it.
2. Where the processing of logic or business rules occurs. *Logic* deals with the processing that the software implements. For example, in a payroll application, the logic would dictate how to handle overtime, sick leave, and vacation time.
3. Where the data management component (DBMS) and information (database) are located. Or, put another way, how the information in the database is stored and retrieved.

Here's an example of the concept. Say you have a data warehouse with information on sales over the past five years. Your client workstation gets its information from your company's OLTP (online transaction processing) server or servers. Software on the servers extracts the information you need and transfers it to your client workstation. Your client workstation then builds the data warehouse according to your requirements and you can use your data warehouse for the OLAP (online analytical processing) you need.

TEAM WORK

WHAT SORT OF COMPUTER NETWORK DOES YOUR SCHOOL HAVE?

Find out what kind of network your school has. Ask the technical people the following questions:

- How many computers are on the network?
- How many people use the computers?
- What is the computer to student ratio?

How many servers, the computers that provide services to other computers, are there? (For example, there's probably an e-mail server.)

In this example, you see a separation of duties to suit particular business needs. The servers process companywide OLTP software on transaction information, and copy to your workstation the information you want to have. Your client computer has, and processes, only the information that you need. This is called a distributed data management model where the server's only duty is to help with data management; the client does everything else (see Figure E.14). This is one way of assigning the processing, logic, and data management. In the set of models that you'll see next, this is Model 5.

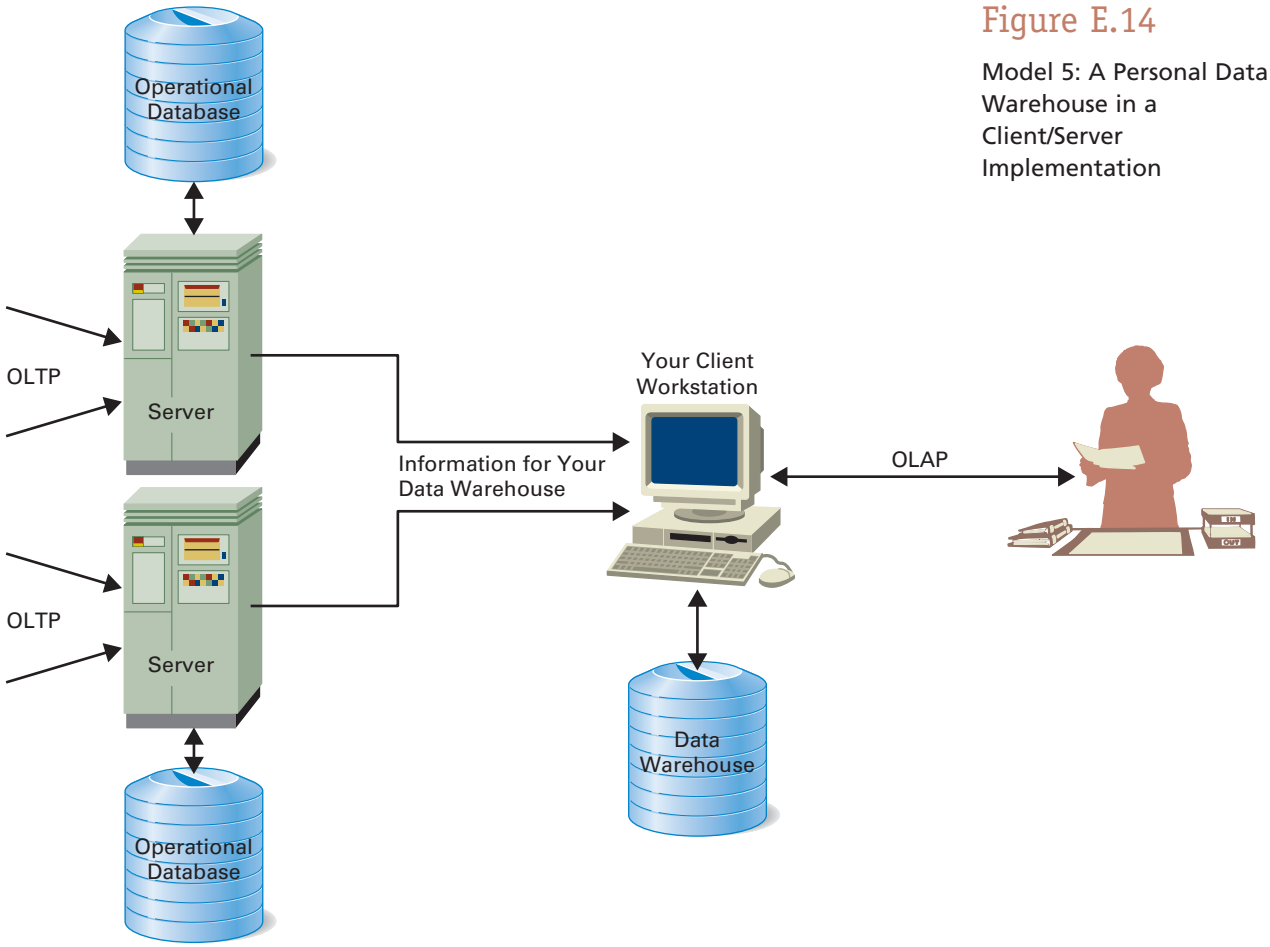


Figure E.14

Model 5: A Personal Data Warehouse in a Client/Server Implementation

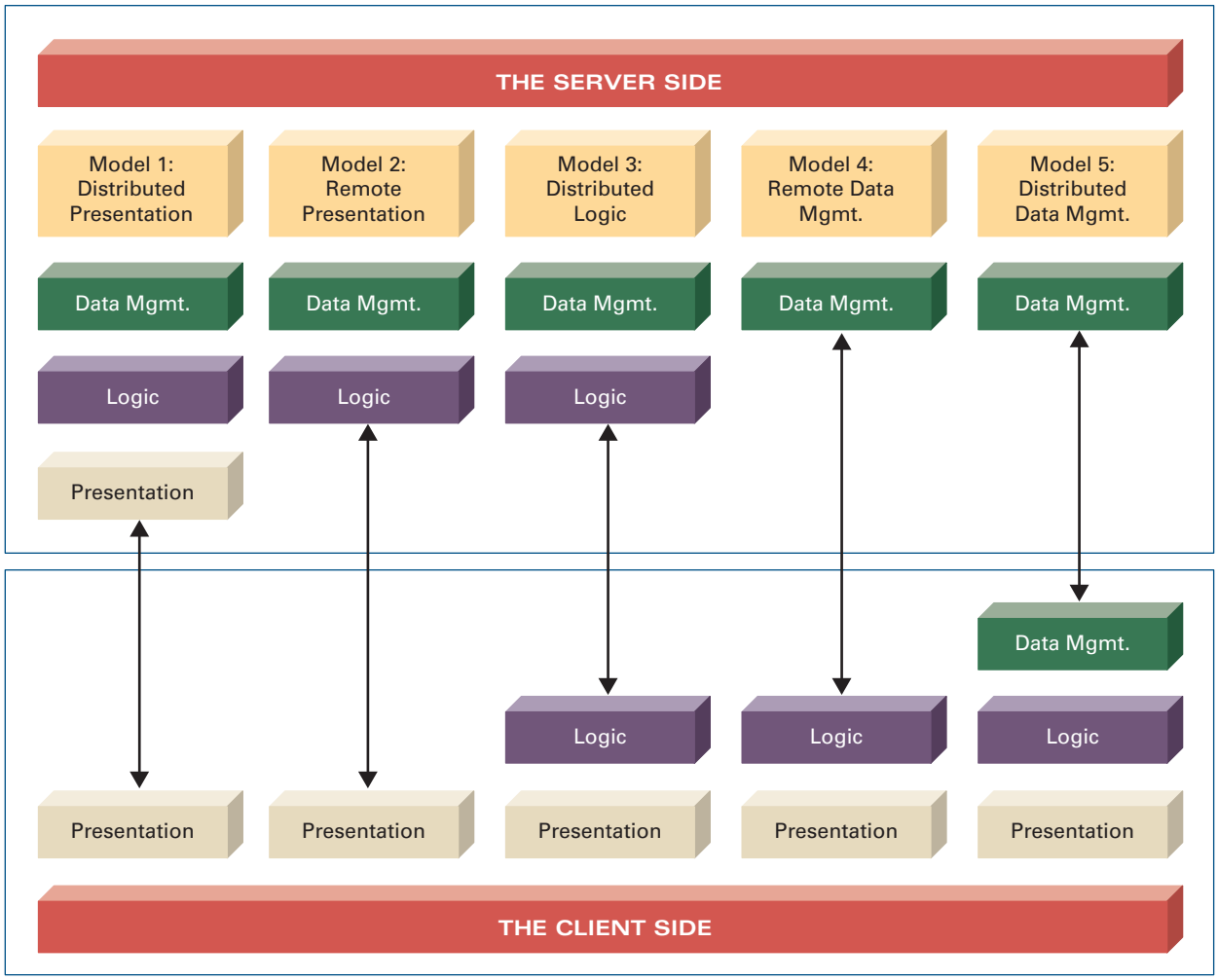


Figure E.15

Five Implementation Models for Client/Server[1]

Each of the five business client/server models that follow has a different way of parceling out the three tasks of presentation processing, logic processing, and data management. See Figure E.15 for a graphic representation of the five models.

CLIENT/SERVER MODEL 1: DISTRIBUTED PRESENTATION

In this first model, the server handles almost all functions, including a major portion of the presentation. The only processing that the client does is to help with formatting the information you see on the screen or printout.

CLIENT/SERVER MODEL 2: REMOTE PRESENTATION

In the second model, the client handles all presentation functions. The processing of business rules happens on the server as does data management.

CLIENT/SERVER MODEL 3: DISTRIBUTED LOGIC

In this model, the server handles all data management and the client handles all presentation formatting, but the logic processing is shared between the server and the client.

CLIENT/SERVER MODEL 4: REMOTE DATA MANAGEMENT

In the fourth model, duties are fully separated again. The server handles data management only, and the client processes business rules and formats the presentation of results.

CLIENT/SERVER MODEL 5: DISTRIBUTED DATA MANAGEMENT

In this final model, the client handles all presentation formatting and business rule processing, and both the server and client share data management duties.

Which model you choose depends on the organization of your business and where you want processing to occur. We have already looked at Model 5, so now let's examine a more complicated case—Model 3, distributed logic.

CLIENT/SERVER IMPLEMENTATION: MODEL 3

In model 3 (distributed logic) the server handles the entire data management function, the client handles the entire presentation function, and server and client share in the processing or application of business rules (see Figure E.16 on the next page).

Suppose you're the manager of the manufacturing division of an organization and need to give pay raises to each of your employees. You use the following divisional and organizational rules for determining pay raises.

Divisional Rules

1. Each manufacturing employee begins with a base raise of $2,500.
2. No manufacturing employee can receive less than a $2,000 raise.
3. If loss of time because of injury is longer than three days, then deduct $500 from the pay raise.
4. If the employee worked less than five days of overtime, then deduct $500 from the pay raise.

Organizational Rules

1. No employee with less than five years of experience can receive a pay raise that exceeds $2,500.
2. Each employee's pay raise must be within 20 percent of last year's raise.
3. Each employee who has taken three or more business-related trips in the last year gets an extra $500 raise.

The following process would then determine the exact pay raise for each employee.

1. You would request information for the employee.
2. Your client workstation would send that request to the server.
3. The server would retrieve the employee information from the employee database.
4. The server would return the employee information to your client workstation.
5. Your client workstation would execute the divisional manufacturing business rules (or logic) that apply to pay raises for manufacturing employees.
6. Your client workstation would format and present the information pertaining to the employee and the appropriate pay raise.
7. You would submit the proposed pay raise for processing.
8. Your client workstation would send that information to the server.
9. The server would execute the organizational business rules or logic relating to pay raises for all employees.
10. The server would return the employee's pay raise (modified according to the organizational business rules) to your work station.
11. Your client workstation would format and present the modified pay raise.
12. You would submit the finalized pay raise for final processing.
13. Your client workstation would send that information to the server.
14. The server would update the employee database to reflect the employee's pay raise.

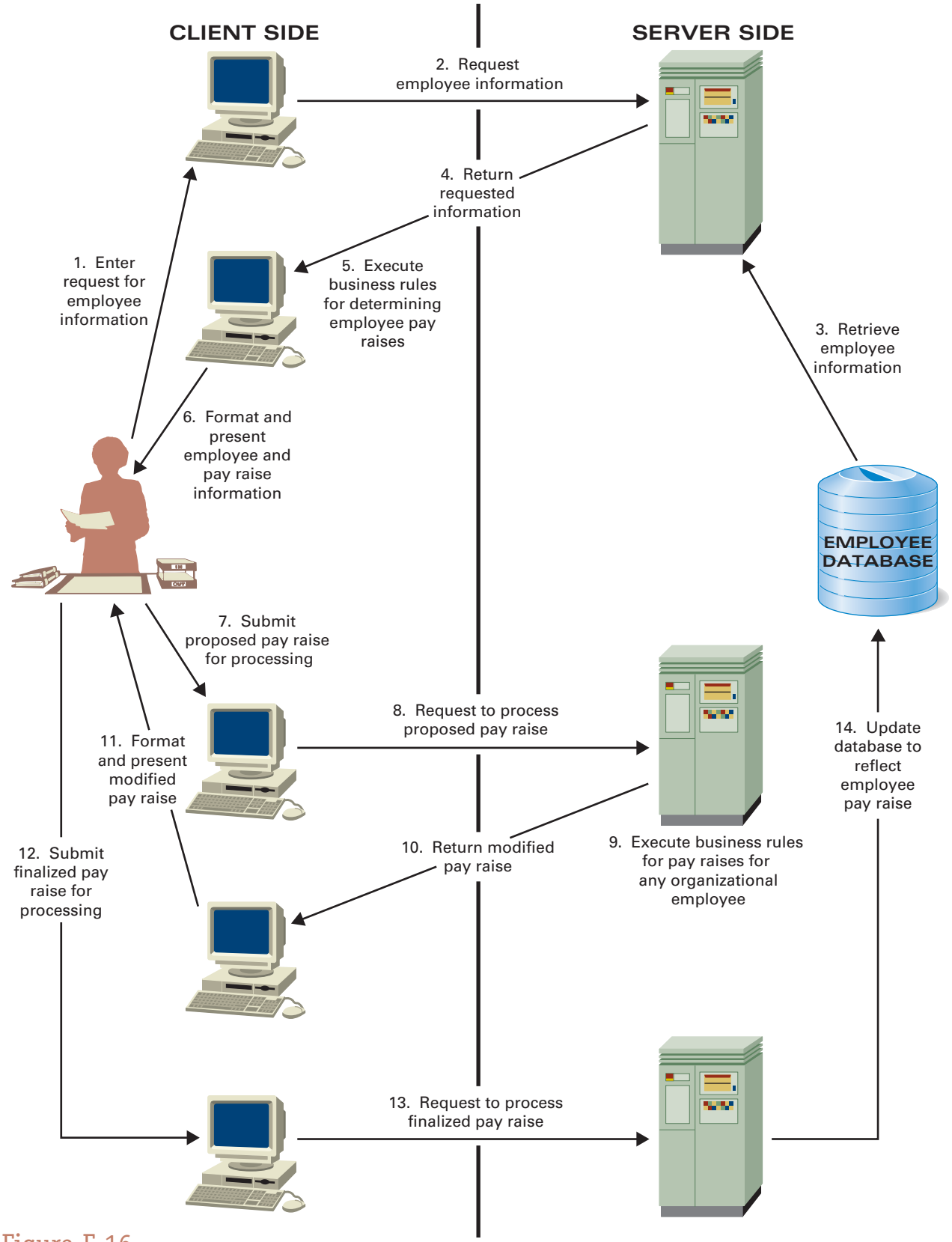


Figure E.16

Model 3: Client/Server Implementation for Employee Pay Raises

ON YOUR OWN

HOW IS A SERVER DIFFERENT FROM A CLIENT COMPUTER?

Compare a high-end rackmount PC designed to be a network server and a typical PC designed for a single individual. What's the difference in the CPU chips? What's the difference in price? How many CPUs are there in the server? Is there a difference in the memory (the amount and type) in the two machines? How about the hard disk drives? Is there any sort of automatic back up on the server? Would you like such an automatic backup system on your computer? Why or why not? www.dell.com and www.gateway.com are places you could start, although they're only two of the many, many sites selling servers.

In this example the server was responsible for data management (retrieving and updating employee information) and executing the business rules or logic that apply to all employees for pay raises. Your client workstation is responsible for editing your entry of information, formatting the presentation of information to you, and executing the business rules or logic that apply to pay raises for manufacturing employees.

When you take the process of distributed logic apart as we did in this example, it seems very complex and tedious. And if you're writing the software to do it, it is. However, as a knowledge worker, the process is completely transparent, meaning that you don't know (or care) how data management, logic, and presentation are handled.

From a management point of view, client/server is a very tidy, organized, and flexible way to make information that all managers need available to them, while keeping information and processing that individual departments need local to the appropriate office.

Summary: Student Learning Outcomes Revisited

1. **Identify and describe the four basic concepts on which networks are built and describe what is needed to set up a small peer-to-peer network at home.** There are four basic concepts on which almost all networks are built. They are
   - ***Network interface cards (NICs)*** in each computer
   - A connecting device like a ***hub, switch,*** or ***home/broadband router***
   - At least one communications medium
   - Network operating system software

   To set up a peer-to-peer network at home, you'd need
   - ***Ethernet cards*** (as the NICs) in each computer
   - A home/broadband router
   - ***Cat 5*** cables
   - A network operating system, like Windows

2. **Describe the components used to build large business networks and define and compare local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs).** Large business networks are built using
   - Network interfaces in each computer
   - ***Hubs*** or ***switches,*** to connect the computers together into subnetworks
   - ***Routers,*** to connect the subnetworks together

   A ***local area network (LAN)*** covers a geographically contiguous area. A ***wide area network (WAN)*** is a set of connected networks serving areas not in immediate proximity. A ***metropolitan area network (MAN)*** is a set of connected networks all within the same city or metropolitan area, but not geographically continuous.

3. **Compare and contrast the various Internet connection possibilities.** There are five ways described in this book to connect a computer or network to the Internet. They are
   - Phone line and ***modem,*** which uses a phone line and prevents your using the same line for voice communication at the same time. It's the slowest type of connection.
   - Phone line and ***Digital Subscriber Line (DSL),*** which, although it uses the phone line, does not prevent simultaneous voice communication. A DSL connection is a ***broadband*** connection.
   - Cable TV line and ***cable modem,*** which brings Internet access in with your cable modem and doesn't use the phone line at all. It's also broadband.
   - Cable programming via a satellite and ***satellite modem,*** which supports both cable television programming and Internet access.
   - ***T1,*** a high-speed business circuit running at 1.544Mbps, or ***DS3,*** a very-high-speed business circuit running at 44.736Mbps.
4. **Compare and contrast the types of communications media.** ***Communications media*** are the paths, or physical channels, over which information travels in a network. There are two options: wired and wireless. Wired communications media include ***twisted-pair cable, coaxial cable,*** and ***optical fiber.*** Of these, optical fiber is the fastest and the most secure. Wireless communications media include ***infrared, Bluetooth, WiFi, microwave,*** and satellite. Infrared and Bluetooth are for very short distances only, Wi-Fi is for short distances, microwave has short and medium distance versions, and satellite is for long distance.
5. **State the four principles of computer security and describe how different network security devices reflect those principles.** The four principles of computer security are
   - ***Confidentiality,*** meaning that information can only be obtained by those authorized to access it
   - ***Authenticity,*** meaning that information really comes from the source it claims to come from
   - ***Integrity,*** meaning that information hasn't been altered
   - Availability, meaning that a service or resource is available when it's supposed to be

   Firewalls protect confidentiality, authenticity, and integrity by blocking traffic that doesn't look like legitimate access to networked computers. ***Intrusion detection systems (IDSs)*** protect all types of computer security by watching for network intrusion attempts and reporting them or taking actions to block them. ***Encryption methods,*** including ***SSL*** and ***virtual private networks (VPNs),*** protect confidentiality by scrambling your communication in such a way that only the intended recipient can unscramble it.
6. **Describe client/server business networks from a business and physical point of view.** A ***client/server network*** is a network in which one or more computers are servers and provide services to the other computers, which are called clients.

   Business View: There are five different configurations based on three factors:
   - Where the processing for the presentation of information occurs
   - Where the processing of logic or business rules occurs
   - Where the data management component (DBMS) and information (database) are located.

   Physical View: The concepts on which larger networks are based are the same as those on which small networks are built. However, the network equipment for the servers may have higher-bandwidth connections and more powerful processors, duplicate connections to the rest of the network, and uninterruptible power supplies to keep the servers available during power failures.

Key Terms and Concepts

Authenticity, 19
Bandwidth, 9
Bluetooth, 17
Broadband, 10
Broadband router (home router), 4
Cable modem, 12
Cat 5 (Category 5), 3
Client/server network, 23
Coaxial cable (coax), 16
Communications media, 15
Communications satellite, 18
Computer network, 2
Confidentiality, 19
Denial-of-service (DoS) attack, 20
Digital Subscriber Line (DSL), 11
DS3, 13
Encryption, 22
Ethernet card, 3
Firewall, 20
Hub, 5
Infrared, 17
Integrity, 19
Internet, 8
Intrusion detection system (IDS), 20
Local area network (LAN), 7
Malware, 22
Metropolitan area network (municipal area network, MAN), 8
Microwave transmission, 18
Network interface card (NIC), 3
Optical fiber, 16
Repeater, 18
Router, 6
Satellite modem, 12
Spyware, 23
Switch, 6
T1, 13
Telephone modem, 10
Twisted-pair cable, 15
Virtual private network (VPN), 22
Virus, 22
Voice over IP (VoIP), 14
Wide area network (WAN), 8
WiFi (wireless fidelity), 18
Wired communications media, 15
Wireless access point (WAP), 3
Wireless communications media, 15
Worm, 22

Short-Answer Questions

1. What is a computer network?
2. How is a peer-to-peer network different from a client/server network?
3. What is an Ethernet card?
4. What does a network switch do?
5. What is a local area network?
6. What is bandwidth?
7. What do you need to have a dial-up connection to the Internet?
8. How is a DSL Internet connection different from a telephone modem connection?
9. What impact does Frame Relay have on a metropolitan area network?
10. What is Cat 5 cable used for?
11. What is Bluetooth?
12. What does WiFi do?
13. How does a VPN protect confidentiality?
14. What does spyware do?
15. How is client/server model 1 different from client/server model 2?

Assignments and Exercises

1. **WHAT ARE THE INTERNET ACCESS OPTIONS IN YOUR AREA?** Write a report on what sort of Internet connections are available close to you. How many ISPs offer telephone modem access? Is DSL available to you? Is it available to anyone in your area? Does your cable company offer a cable modem? If your school has residence halls, does it offer network connections? Compare each available service on price, connection

speed, and extras like a help line, list of supported computers and operating systems, and people who will come out to your home and help you if you're having difficulties. What type of Internet connection do you currently use? Do you plan to upgrade in the future? If so, to what type of connection? If not, why not?

2. **INVESTIGATE BUILDING YOUR OWN HOME NETWORK** Build your own home network on paper. Assume you have the computers already and just need to link them together. Find prices for switches and routers on the Web. Also research Ethernet cards and cables. If you were to get a high-speed Internet connection like DSL or cable modem, how much would it cost? Can you buy your own, or would you have to rent the modem from the phone or cable company?
3. **DEMONSTRATE THE IMPACT OF WIRELESS TECHNOLOGY** How many devices do you own or use that transmit signals (not just computer data) wirelessly? Think of as many as you can, and make a list showing the different types of signaling used by each device. Don't forget that some devices use multiple wireless technologies, like cell phones with both cellular signals for voice transmissions and Bluetooth for syncing their address books. Hint: Don't forget cordless phones, TV and stereo remotes, radios, and portable computers and PDAs with infrared capability (look for a small, glossy black window somewhere on the edge of the case). Can any of your devices communicate with each other?
4. **INVESTIGATE SATELLITE RADIO** At the time of writing, there were two satellite radio services: Sirius and XM. Do a little surfing on the Web and find out if there are any others now. Also find out what you have to buy to install each type, how much the antenna costs, how the system would work in your car, and how much the monthly subscription is.
5. **CONSIDER THE IMPORTANCE OF NETWORK SECURITY** Write a report about the importance of computer and network security in your daily life, in terms of the four principles of computer security. If you have a job in addition to being a student, write about computer security in your workplace. If you don't work outside the classroom, write about how computer security affects you at school and in your personal life. You may be surprised at how many things you do depend on some aspect of secure computer records and communications, like banking, grades, e-mail, timesheets, library and movie rental records, and many more.
6. **FIND OUT ABOUT FIREWALLS** Go to the Web and find out about software and hardware that protect your computer and home network, respectively.

   If you have only one computer connected to the Internet, then a software firewall like Zone Alarm will most likely be enough protection from intruders. Find three different firewall software packages on the Web. A good place to start looking would be the sites that sell anti-virus software. Compare the firewall software on price and features. Some sites to try are
   - Symantec at www.symantec.com
   - Trend Micro at www.trendmicro.com
   - McAfee at www.mcafee.com
   - The Virus List (a virus encyclopedia) at www.viruslist.com

   If you have a home network, look into hardware firewall options. How many different hardware firewalls can you find on the Web site of your favorite electronics retailer? (Hint: Look in the feature lists of home routers and broadband routers, even if they don't have the word firewall in their name.)

PHOTO CREDITS

Page 3, top photo, © Nance Trueworthy.

Page 3, second photo, Courtesy of NETGEAR Inc.

Page 3, third photo, Photo by R.D. Cummings, Pittsburg State University

Page 3, bottom, Courtesy of Linksys.

Page 4, top, Proxim Corporation.

Page 4, bottom, Courtesy of Linksys.

Page 5, Microsoft product box shot reprinted with permission from Microsoft Corporation.

Page 15, Spencer Grant / Photo Edit.

Page 16, top, © Mark Antman / The Image Works.

Page 16, bottom, PhotoDisc / Getty Images.