EXTENDED LEARNING MODULE E

NETWORK BASICS

Student Learning Outcomes

1. IDENTIFY AND DESCRIBE THE FOUR BASIC CONCEPTS ON WHICH NETWORKS ARE BUILT.

2. LIST THE COMPONENTS YOU NEED TO SET UP A SMALL PEER-TO-PEER NETWORK AT HOME.

3. COMPARE AND CONTRAST THE VARIOUS INTERNET CONNECTION POSSIBILITIES.

4. DESCRIBE CLIENT/SERVER BUSINESS NETWORKS FROM A BUSINESS AND PHYSICAL POINT OF VIEW.

5. DEFINE LOCAL AREA NETWORKS (LANs), MUNICIPAL AREA NETWORKS (MANs), AND WIDE AREA NETWORKS (WANs).

6. COMPARE AND CONTRAST THE TYPES OF COMMUNICATIONS MEDIA.
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 card (either as an expansion card or integrated into the motherboard) 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 or a router) that ties the computers on the network together and acts as a switchboard for passing messages.

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 discuss ways to connect a single computer or home network to the largest network of them all—the Internet. Finally, we’ll move on to large business networks, LANs, MANs, WANs, and communications media.
Peer-to-Peer Home Network

The simplest kind of network is a peer-to-peer network. If you have two computers and you’d like both to be able to print to a single printer, you can connect all three devices together to create a peer-to-peer network. A peer-to-peer network is a network in which a small number of computers share hardware (such as a printer), software and/or information. Each computer independently stores its own software and information but can access the information on the other computers.

You can set up a small peer-to-peer network one of two ways: either with Ethernet cards and dedicated network cabling or by using your existing phone wiring.

HOME NETWORK COMPONENTS

You can set up a peer-to-peer network at home with a few computers—say between two and ten—to share a printer or an Internet connection relatively easily. You’ll need

- An Ethernet network card in each computer
- A home router as a connecting device to tie the computers together and pass messages between them
- Cables as the transmission medium
- Software that allows information to flow between computers (Windows will do nicely).

NETWORK CARDS IN EACH COMPUTER

First, the network cards; you’ll need a network interface card in each computer. A network interface card (NIC) is an expansion card 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. Many computers today have an NIC integrated into the motherboard.

An Ethernet card is the most common type of network interface card. You plug the card into an ISA or PCI expansion slot in your desktop computer. An Ethernet card has a connector, usually an RJ-45 type, that looks very like a telephone connector, except that it’s a little larger. Ethernet cards are also sold as PC Cards that plug into the side of notebook computers.

NETWORK CONNECTING DEVICES

Second, the connecting device; you’ll need a way to pass information and messages to the correct destination computers. To do that you use a connecting device that ties the computers together and lets information pass from one to the other. Network connecting devices come in various types. The ones we’ll consider here are basic hubs, switches, and routers (see Figure E.1 on the next page).

A network hub is a device that connects multiple computers into a network. A basic hub allows only one communication link at a time, in the same way that only one car at a time can proceed at an intersection that has four-way stop signs. Now imagine that, instead of a junction of just four roads, the intersection has hundreds of roads coming together. It might take a while for each car to move forward. In cities, where there’s heavy traffic at road junctions, there are cloverleaf intersections so that no car has to stop to let others pass. In networking, a switch does the cloverleaf thing. A switch is a device that connects multiple computers into a network in which multiple communications links can be in operation simultaneously.
Four-way stop and cloverleaf intersections let all vehicles go wherever they want. This is fine for highways, but not so good on networks. Back in the metropolis, let’s say that one road runs between two large intersections, one of which is in Internet City and the other is in Home Network City. If Home Network City were to be quarantined, police would set up a roadblock just outside Home Network City, and every vehicle would be checked to see that it was actually going to a destination in Home Network City. If it was not, the vehicle would be turned back. Also, the police wouldn’t let vehicles through whose origin and destination are both in Home Network City.

The roadblock separates the two cities and their traffic. In networking, the police roadblock is a router, but the router does more: It’s also the cloverleaf. A router is a device that acts as a smart hub connecting computers into a network, and it also separates your network from any other network it’s connected to. In fact, this isolating feature of routers is precisely the reason that network administrators install them on larger networks. The reason it’s necessary is related to how an Ethernet network works.

On an Ethernet network, each message sent out goes to all the computers on the network, and each computer looks at the address on the message to see if it’s meant for that computer or not. This makes the network relatively simple to design and operate, but it means that heavy traffic slows the network down since every computer looks at every message that every other computer sends. A way around this problem is to divide the large network into smaller networks and connect them with a router. A router is a device you can also use to connect two networks (as well as computers), passing information from one to the other. A router makes sure that messages get to the right destination computer without going to everyone else, but also makes sure that the messages go outside the network only when necessary.

In a home network, the isolating feature of a router is a very good reason to use it since the network you’re separating yours from is the Internet (see Figure E.2). You want to be able to send and receive information and messages to and from the Internet, but you don’t want unauthorized access from intruders. A home router protects your home network by making it more or less invisible to the Internet. It therefore acts as a hardware firewall giving you much better security for your home computers. A firewall is software or hardware that protects a computer or network from intruders.

**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 Cat
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 plugs into the Ethernet card in your computer and the other end into the home router.

**WIRELESS ACCESS TO YOUR HOME NETWORK**

If you’d like to wirelessly access your home network with your notebook computer you’ll need another device on the network called a wireless network access point. A **wireless network access point** or **wireless access point** is a device that allows computers to access a network using radio waves. 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.

Your wireless access point connects to a wired network with a cable to the hub or switch in the same way the wired computers do (see Figure E.2). Your notebook and any other device that wirelessly accesses the network must have a wireless adapter, which would be a PC Card in the case of the notebook computer, incorporating a transmitter, a receiver, and an antenna. A wireless access point is usually itself a router, so you could use it to create a completely wireless network where the wireless access point would be the connecting device also.

The type of radio wave transmission often used in wireless networks is WiFi. **WiFi**, which stands for **Wireless Fidelity** (also known as **IEEE 802.11b**), is a way of transmitting information in wave form that is reasonably fast and is often used for notebooks. Currently, 2 million people use it, and that number is expected to double.
within a year. Apart from home networks, WiFi is used by companies to allow their employees to go wireless, and is also available in various public places such as airports, hotels, and even restaurants like Happy Donuts and Starbucks. Pretty soon we’ll have WiFi-capable airplanes.¹

A relatively new and competing wireless technology for short-range wireless connections, also using radio waves, is called Bluetooth. Named for a Viking king, Bluetooth technology provides entirely wireless connections for all kinds of communication devices. For example, Bluetooth could replace the cable connecting a notebook computer to a cellular telephone. Virtually all digital devices, such as keyboards, joysticks, printers, and the like, can be part of a Bluetooth system. Bluetooth is also adaptable to home appliances like refrigerators, microwaves, and so on.

NETWORK SOFTWARE
As always, when you have hardware, you need software to make it work. For a small home 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 you want accessible. When you do this the files on one computer will appear as additional folders on the other computer.

HOME NETWORK WITH EXISTING PHONE WIRING
A relatively new technology called Home PNA, which stands for Home Phoneline Networking Alliance, allows you to network your home computers using telephone wiring. You’ll need

- PNA adapter cards for each computer
- Ordinary phone wire with phone jacks for each computer

First, you must install a PNA adapter card in each computer. A PNA adapter card is an expansion card that you put into your computer to act as a doorway for information flowing in and out. The PNA adapter card has a connector for a telephone jack (RJ-11 connector) into which you plug one end of the phone cable. You plug the other end into an extra phone jack in the wall (see Figure E.3). And that’s pretty much all you have to do, assuming you have a newer version of Windows on all the computers.

Note that in this case you don’t need a router. You also don’t need special cable or connectors. It’s simpler than the previous home network configuration, but it’s also slower.

Figure E.3
PNA Home Network
Internet Access

Whether or not you have a network at home, if you have a computer, you probably already are, or want to be, connected to the Internet. There are five possible ways of accessing the Internet from home. These include using a

1. Telephone line and a telephone or dial-up modem
2. Telephone line and a Digital Subscriber Line (DSL) modem
3. Cable TV line and a cable modem
4. Satellite dish and a satellite modem
5. Provider that offers wireless connection for your notebook computer or one that offers wireless connection for hand-held devices (some cellular phone companies do this).

DSL, cable, satellite, and metropolitan wireless systems are broadband connections. **Broadband** is a high-capacity telecommunications pipeline capable of providing high-speed Internet service. There is some disagreement in the industry as to what “high-speed” means exactly. The Federal Communications Commission defines it as a capacity of 200 Kbps (or 200 kilobytes per second). At the other end of the spectrum are experts who believe that the high speed must be at least 750 Kbps.

**TELEPHONE OR DIAL-UP CONNECTION**

A telephone or dial-up connection requires that you have a computer, a phone line, a modem, and, of course, an Internet service provider or ISP. Simply put, a telephone modem is a telephone for your computer. People use a phone apparatus to talk to each other using the phone line. Similarly, computers can use telephone or dial-up modems to swap information. A **telephone modem** (usually referred to as simply a **modem**) is a device that connects your computer to your phone line so that you can access another computer or network. If you want to connect to the Internet, you use your modem to first access your ISP. Your ISP then connects you to the Internet. A modem is a device that converts the digital signals from your computer into 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 Figure E.4). In short, a modem **modulates** outgoing and then **demodulates** incoming transmissions.

![Figure E.4](image-url) The Role of a Telephone Modem

<table>
<thead>
<tr>
<th>Digital</th>
<th>Digital-to-Analog Conversion</th>
<th>Analog</th>
<th>Analog-to-Digital Conversion</th>
<th>Digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital uses discrete electronic pulses to represent information.</td>
<td></td>
<td>Analog uses a continuous electronic stream to represent information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Nowadays, telephone modems are often integrated into the motherboard of new computers. If your computer doesn’t have this feature, you can buy a modem board or card to plug into a PCI expansion slot in your desktop or a PC Card for your notebook computer.

A telephone modem is the slowest type of Internet connection that you can get. The fastest transmission possible with a telephone modem is 56 Kbps (or about 56,000 bits per second).

**DIGITAL SUBSCRIBER LINE (DSL)**

A Digital Subscriber Line (DSL) is a high-speed Internet connection using phone lines, which allows you to use your phone for voice communications at the same time. There are many kinds of DSL systems (ADSL or asymmetric DSL, SDSL or symmetric DSL, HDSL or high-bit-rate DSL, to name a few). DSL divides your phone line into channels which separate the information and voice traffic on the line so you can still make and take phone calls while you’re connected to the Web.

In order to get a DSL Internet connection, you need to live within about 3 miles of the phone company, which is called the CO or Central Office. In larger cities, remote COs are located throughout the metropolitan area. The speed of your DSL line depends on the distance between you and the CO. Speeds vary from 144 Kbps (144,000 bits per second) to 1.54 Mbps (1,540,000 bits per second) and can even go as high as 6.0 Mbps.

A phone company provides the DSL connection. However, you can buy the Internet service directly from the phone company, in which case it becomes your ISP too, or from an independent ISP that buys the service from the phone company and sells it to you.

Once you’re within range of a DSL provider, you’ll need a DSL modem that connects on one side to the splitter at your house and on the other to your computer (see Figure E.5). The cable from the DSL modem connects to your computer in one of two ways, either to an Ethernet card in your computer or to a USB port. A DSL Internet connection has three big advantages over a dial-up connection:

1. DSL is much faster—up to 25 times faster than a telephone modem
2. DSL is an always-on connection giving you Web access without having to dial into your ISP first
3. You can use the same phone line for voice communications

**CABLE MODEM**

If you have 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 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 de-
liver an Internet connection (see Figure E.6). 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. The speed of transmission with a cable modem is much faster than a phone modem. It’s also an always-on connection and doesn’t use a phone line at all.

While the speed of a DSL connection is guaranteed, the speed of a cable Internet connection depends on how many users are online. 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.

**INTERNET OVER SATELLITE**

You can also get to the Internet using a satellite dish and a satellite modem. This is called *Internet over Satellite (IoS)*. Satellite Internet uses a satellite dish that looks very like your TV satellite dish. A *satellite modem* is a modem that allows you to get Internet access from a satellite dish (see Figure E.7). You will, however, need the right type of satellite dish (i.e., antenna).
The big difference between a TV satellite dish and an Internet satellite disk is that a satellite Internet system is two-way: You can send as well as receive transmissions. You can get a system for Internet access alone or one that gives you both Internet access and satellite TV. Internet over satellite is relatively new and is an ideal way of bringing the power of the Internet to isolated locations.

The speed of information coming to you is called download speed. The download speed of an Internet satellite is about 10 times faster than a phone modem.

For satellite Internet you’ll need

- An appropriate satellite dish
- A satellite modem
- Cable between the satellite modem and the dish
- An unobstructed view in the direction of the equator, above which the telecommunications satellites orbit. So your dish will point south if you’re in the northern hemisphere and north if you’re in the southern hemisphere.

INTERNET ACCESS ON MULTIPLE COMPUTERS

A DSL, cable, or satellite connection will allow you to use a single Internet connection for all the computers on your home network—you simply connect the appropriate modem to the router. Routers have IP addresses of their own, called private IP addresses, which they assign to the computers on the network. These are separate from the IP address that your ISP assigns. That one is called a public IP address. The router has a network address translator (NAT), which swaps messages between the private, internal IP addresses and the public IP address when moving information between the Internet and network computers. In addition to letting multiple computers share an Internet connection, a router protects your network, since the private IP addresses are not easily accessible to hackers (people who invade the computers of others).

A word of caution: Before you hook up a network to a single Internet connection, make sure that it’s not a violation of the contract you signed with your ISP.

WIRELESS INTERNET CONNECTION

If your notebook, or desktop computer for that matter, has a wireless port and the network you’re accessing has a wireless access point within range, you can wirelessly join that network. And if the network has Web access, you can get to it, too. But what if you don’t have access to such a network?

In that case, you’ll need a wireless Internet service provider. A wireless Internet service provider (wireless ISP) does the same job as standard Internet service providers except that you don’t need a wired connection for access. In fact, some ISPs provide both wired and wireless connections. If you travel a lot, you’ll need a wireless ISP with a wide geographic reach, just as you do with a cellular phone.

If you want to reach the Web with something smaller than a notebook computer, you can use hand-held wireless devices like a PDA, Web phone, or pager. A personal digital assistant (PDA) is a small hand-held computer that helps you surf the Web and perform simple tasks such as note taking, calendaring, appointment scheduling, and maintaining an address book.

Probably, PDAs will be the dominant hand-held wireless devices of the future for Internet access. Distinctions between hand-held devices, however, are already blurring. Some manufacturers are already combining cellular phones and PDAs. Some are mostly phones with PDA capabilities, and others are PDAs with phone capabilities.

There are two major types of PDAs: (1) Palms and Handsprings, and (2) PocketPCs. The difference between Palms/Handsprings and PocketPCs is similar to the differ-
ence between PCs and Macs in that they use different operating systems. The Palm/Handspring-type PDAs run on the Palm Operating System (Palm OS), while PocketPCs run on Pocket PC OS (which used to be called Windows CE).

Wireless ISPs support one or the other or both, so if you plan on buying a wireless PDA for Internet access, be sure to check it out. In general, don’t expect to surf the Web with a hand-held wireless device the way you would with a notebook or desktop computer. The various wireless service providers use one of several older standards that were designed for cell phones and, while they’re fine for talking, they’re too slow for good quality Web access. Also, the size of the screen limits the amount of content.

Business Networks

In the peer-to-peer home networks previously described the computers are all equal. Each one has its own files and devices, which it can share with the other computers. But, unless you operate 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. 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, for the following reasons:

- 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 are more manageable if software and information are on the server.

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 allows you to check your grades online, you’ll probably find that you can’t do anything other than view grades on 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 as well as view a loan application 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.

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 in fact 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.8). 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.

Each of the five business client/server models that follows has a different way of
parceling out the three tasks of presentation processing, logic processing, and data man-
agement. See Figure E.9 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 of
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 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.10).

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.
Figure E.10
Model 3: Client/Server Implementation for Employee Pay Raises
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 workstation.
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.

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 achieve two goals: make information available to those who need it and keep departmental information and processing local to the appropriate office.

CLIENT/SERVER: A PHYSICAL VIEW

There are more physical implementations of client/server networks than cars on the road. However, conceptually, large networks work on the same principle as little ones. You still need network cards, hubs, switches, and/or routers, communications media, and network operating systems on all the computers in the network. However, this is not to say that large networks are simple to build and maintain: they most definitely are not. The number of considerations goes up exponentially with the size of the network.

For a client/server network, you need a special operating system for the servers. You may have to install special network processors like multiplexors that collect transmissions from several communications media and send them over a single line that operates at a higher capacity. You also have to consider the type of topology (how the computers and servers are arranged in relation to each other) and what sort of protocol to use. A communications protocol (protocol) is a set of rules that every computer follows to transfer information. You may have heard of TCP/IP (Transport Control Protocol/Internet Protocol), which is the protocol that computers connected to the Internet have to use to be able to talk to the other computers. It’s quite a simple concept—if the computers don’t all speak the same language they can’t communicate. The electronic data interchange (EDI) of basic business documents that you learned about in Chapters 2 and 5 uses ANSI X.12 protocol. So a network that accesses the Web and conducts EDI transactions will need both protocols.

Figure E.11 shows a typical Ethernet configuration for a medium-sized business. A router connects the company’s network to the ISP which provides Internet access. A hub or switch serves to connect the smaller company networks to the server or servers,
which will have control over the organizational databases, and there might also be a wireless network connection for people with laptops. One or more servers are also available to all the computers in the network. One server would most likely provide Internet and e-mail services.

An enterprisewide network might span many states or even be scattered all over the world. Such a network would most likely have mainframes and older, legacy networks that must be tied to the more modern network. Parts of the network would need high-bandwidth or high-capacity communications media (which we’ll discuss later). There would probably be multiple servers on such a large network, probably one for each of the smaller networks.

**LANs, MANs, WANs, and Communications Media**

Many, many types of networks exist today. Previously in this module we discussed peer-to-peer and client/server networks. A peer-to-peer network is one in which all the computers are equal and share information and hardware. A client/server network has one or more computers that provide services to the others. However, this isn’t the only way you can categorize computer networks. You can also classify networks by geographic distance.
**ON YOUR OWN**

**HOW IS A SERVER DIFFERENT FROM A CLIENT COMPUTER?**

Compare a high-end desktop 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 backup 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 looking for information, although they’re only two of the many, many sites selling servers.

**CLASSIFICATION OF NETWORKS BY GEOGRAPHIC DISTANCE**

There are three basic types of networks in this category: LANs, MANs, and WANs. A **local area network (LAN)** covers a limited geographic distance, such as an office, building, or a group of buildings in close proximity to each other. A **municipal area network (MAN)** covers a metropolitan area.

**Wide area networks (WANs)** cover large geographic distances, such as a state, a country, or even the entire world. A wide area network is essentially a network of smaller networks. The Internet is the biggest WAN on the planet. When a company’s LAN is connected to the Internet, the LAN becomes part of a WAN.

An example of a company WAN is Metropolitan Life Insurance Company, which uses a WAN to connect its LANs. At Met Life, a central server makes the organization’s pension database available to employees who work all over the country. The database has information on all current and prospective clients, as well as information about competitors. Each LAN also has its own server with a database of client and product information for that particular area. As updates are made at each LAN site the LAN servers communicate those updates to the central WAN server. Likewise, the central server updates all appropriate information on the LAN site servers nightly. When Met Life sales associates are on the road, they can dial into the central server to receive whatever updates they need.

**TELECOMMUNICATIONS MEDIA: THE PATHS THAT CARRY INFORMATION**

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 follow:

<table>
<thead>
<tr>
<th>Wired</th>
<th>Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twisted-pair cable</td>
<td>Microwave</td>
</tr>
<tr>
<td>Coaxial cable</td>
<td>Satellite</td>
</tr>
<tr>
<td>Optical fiber</td>
<td>Infrared</td>
</tr>
</tbody>
</table>
BANDWIDTH

Before discussing the various types of communications media we should first address bandwidth. Bandwidth, or capacity of the communications medium, refers to the amount of information that a communications medium can transfer in a given amount of time. You measure the capacity of a communications medium in bits per second (bps), thousands of bits per second (Kbps), millions of bits per second (Mbps), or billions of bits per second (Gbps). For example, if a particular communications medium has a maximum capacity of 16 megabits per second (Mbps), up to 16 million bits of information can be transferred in a single second. Bandwidth is comparable to the size of a drinking straw: The fatter the straw, the more liquid you can drink in a given period of time.

WIRED COMMUNICATIONS MEDIA

Wired communications media are those that tie devices together with cables of some kind. Twisted-pair cable, coaxial cable, and optical fiber are the types of cabling or wired media you’d find in computer networks.

TWISTED-PAIR CABLE

Twisted-pair cable comes in several varieties. The Cat 5, which we discussed in connection with home networks previously 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 Kbps, while a better type (Cat 3) provides up to 10 Mbps. However, distance, noise on the line, and interference tend to limit the reliability of most types of twisted-pair cabling. For example, a crackle that changes a credit card number from 5244 0811 2643 741 to 5244 0810 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 cable provides a much higher bandwidth than ordinary phone cable, meaning it carries more information in a given time period, and is suitable for distances of up to 100 yards. It’s the most widely used cabling for data transfer in today’s LANs. Cat 5 is relatively inexpensive and is fairly easy to install and maintain. 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 FIBERS

The fastest and most efficient medium for wired communication is optical fiber, which uses a very thin 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 cable’s advantages are size (one fiber has the diameter of a human hair); capacity (exceeding 1,400 Mbps); much greater security; and 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. However, optical fiber is very expensive and very difficult 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 people are in motion. For whatever reason, if wired communications media don’t fit your needs, wireless may be the answer. Wireless communications radiate information through 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 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 OMNIDIRECTIONAL MICROWAVE FOR SHORT DISTANCES

Infrared is the oldest type of wireless communication. Infrared is a wireless communications medium that uses light waves to transmit signals or information. Your TV remote control uses infrared. You can use infrared to connect hand-held devices, such as pocket PCs, to peripheral devices such as printers. Wireless keyboards and mice are usually connected to your PC with an infrared link. Infrared communication is totally line-of-sight, meaning that if anything blocks the path of the signal, it won’t work. Infrared transmission has very limited bandwidth (typically 1 Mbps).

Another method of short-distance wireless communications is omnidirectional (all directions) microwave transmission. Microwave transmission is a type of radio transmission. You can choose one of two systems: Bluetooth or WiFi, both of which you saw earlier in this module. To add wireless access to your network, you’d connect a wireless access point to the wired network, which would then act as a receiver for messages coming into the network and a transmitter for messages going out to the wireless device. The wireless device has a companion receiver and transmitter, and can access the network as if it were cable connected.

DIRECTIONAL MICROWAVE FOR MEDIUM DISTANCES

Microwaves can 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 travels in a straight line and does not 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.12). 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 several dishes on them). Microwave signals have difficulty getting through walls or trees or other solid objects, so there must be a clear path from sender to receiver.

**SATELLITES FOR LONG DISTANCE**

*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.13). 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, Kmart 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 office; 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.

**Communications Service Providers**

You can set up your own cabling, routers, switches, multiplexors, protocols, and so on and have your own communications network, or you can get a third party to provide it for you. Which strategy you take determines network ownership. Network ownership determines

- Rights to the network
- Cost
- Availability
- Services provided
- Speed
- Security

Small networks within an office building are almost always private. That means that the company buys, installs (or contracts out the installation), and maintains the network. Therefore that company has exclusive rights to the use of the network.

The following discussion deals with networks that cover a large geographic area and require *communications service providers*, third parties who furnish the conduit for information. You can support your network with a public network, a private network, a value-added network, or a virtual private network (see Figure E.14 on the next page).

A *public network* is a network on which your organization competes for time with others. The telephone system is a public network. You’re not guaranteed that you’ll
always be able to get a line when you want to make a call—as you may have found out if you unsuccessfully tried to call your mother on Mother’s Day. When all the lines are busy you get a recorded message to that effect. And when you dial into the Internet, you’re competing with others for access, and you’ll find that the speed of getting to Web sites varies greatly.

A **private network** consists of the communications media that your organization owns or exclusively leases to connect networks or network components. You can lease dedicated lines from a communications service provider.

A **value-added network (VAN)** is a semipublic network that provides services beyond the movement of information from one place to another. The “value-added” part of this type of network is what makes it attractive. For example, if you need EDI (electronic data interchange) capabilities to automate the exchange of standard business documents between your organization, your suppliers, and your customers, you might hire a communications service provider to set up a network and provide EDI capability. VAN providers also offer security, auditing, and translation services between different versions of EDI systems.

General Electric Information Services offers VAN services. If you buy their VAN, all you have to do is develop an interface between (1) your system and GE’s VAN and (2) your customers’ and suppliers’ systems and GE’s VAN. GE will do the rest. You saw in Chapter 5 how VANs aid electronic commerce.

Of course, you could do all this yourself. You could build a private network and develop software to handle the conversions that you’ll need for EDI. However, most companies don’t adopt this strategy: It’s too complex and expensive.

A **virtual private network (VPN)** uses software to establish a secure channel on the Internet for transmitting data. Your information travels with information from other organizations. A VPN promises that your information will be secure even though it travels over the Internet. VANs also guarantee secure information transmission, but the cost of a VPN is usually lower. Practically every national phone service provider (Baby Bells, AT&T, and so on) offers domestic VPN services.

### Comparison of Types of Network Ownership

<table>
<thead>
<tr>
<th>Cost</th>
<th>Availability</th>
<th>Services</th>
<th>Speed</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pay-as-you-go</td>
<td>Compete for time and use</td>
<td>Moves information only</td>
<td>Slower than private network</td>
<td>Little or none guaranteed</td>
</tr>
<tr>
<td><strong>Private</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pay for all of it <strong>Or</strong></td>
<td>No competition for use</td>
<td>Can have additional services</td>
<td>Faster than public networks</td>
<td>Higher than that of public networks</td>
</tr>
<tr>
<td>Pay flat fee for leased line</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value-Added Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pay-as-you-go</td>
<td>Little or no competition for use</td>
<td>VAN provider offers additional services</td>
<td>Faster than public networks</td>
<td>Much better than public networks</td>
</tr>
<tr>
<td><strong>Virtual Private Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flat fee per month plus usage fee</td>
<td>Compete for use</td>
<td>VPN owner provides some additional services</td>
<td>Slower than equivalent public network</td>
<td>Better than public networks</td>
</tr>
</tbody>
</table>

**Figure E.14**

Comparison of Types of Network Ownership
If you need to transmit information further abroad, you can use an international virtual private network (international VPN). These are virtual private networks that depend on services offered by phone companies of various nationalities. Two current examples are Phoenix and Worldpartners. Phoenix is an alliance between Deutsche Telekom AG (Germany), France Telecom, and Sprint. Worldpartners is the largest international VPN and consists of AT&T, Kokusai Denshim Denwa (Japan), Singapore Telecom, and Unisource, which is itself an alliance of telecommunications providers from Spain, the Netherlands, Sweden, and Switzerland.

KEY CONSIDERATIONS FOR COMMUNICATIONS MEDIA

Communications media technology is vitally important in a network. To determine the most appropriate communications medium, you must consider the capacity, reliability, cost, and distance that your network covers as well as the mobility of your network users.
1. **Identify and describe the four basic concepts on which networks are built.** The four basic concepts on which almost all networks are built are:
   - **Network interface cards (NICs)** in each computer
   - A connecting device like a **hub, switch, or router**
   - At least one type of communications media
   - Network operating system software

2. **List the components you need to set up a small peer-to-peer network at home.** To set up a **peer-to-peer network** at home, you’d need:
   - **Ethernet cards** (as the NICs) in each computer
   - A home router to connect computers and other devices together
   - **Cat 5** cables to transmit information
   - Windows operating system on each computer

3. **Compare and contrast the various Internet connection possibilities.** There are five ways 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 communications. It’s the slowest type of connection.
   - Phone line and **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 with your cable TV connection and doesn’t use the phone line at all. It’s also broadband.
   - Satellite antenna (dish) and **satellite modem**, which provides broadband Internet access.
   - Wireless Internet connection and a wireless device like a notebook computer or a PDA. Access with a notebook computer is usually fast, but access with any hand-held device that uses cell phone technology is slow.

4. **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

---

**Summary: Student Learning Outcomes Revisited**

1. **Capacity or Bandwidth** determines (1) how much information can travel over the communications medium at once, and (2) how fast the information can travel. Twisted-pair cable has the lowest capacity, and optical fiber the highest.

2. **Reliability** is a measure of how much you can depend on your network. If you need a network with the greatest reliability, you probably won’t choose wireless communications because wireless networks are the most susceptible to outside interference.

3. **Cost** is always a very important consideration in the building and maintenance of a network. Your choice of capacity and reliability will usually affect the cost.

4. **Distance** is a consideration in what medium you choose. Infrared, for example, works only over small distances, whereas optical fiber and satellite work well over great distances.

5. **Mobility** may be important to your organization. If so, you may want to investigate wireless communications so that connectivity becomes mobile.
• Where the data management component (DBMS) and information (database) are located

**Physical View:** The basic concepts on which larger networks are based are the same as those on which small networks are built. However, there are a lot more considerations, such as network processors, communications media, protocols, and so on to consider.

5. Define local area networks (LANs), municipal area networks (MANs), and wide area networks (WANs). A **local area network (LAN)** covers a limited geographic distance, such as an office, office building, or group of buildings in close proximity to each other. A **municipal area network (MAN)** covers a metropolitan area. A **wide area network (WAN)** covers large geographic distances, such as a state, a country, or even the entire world.

6. **Compare and contrast the types of communications media.** Communications media are the paths, or physical channels, in a network over which information travels. 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 satellite, microwave, and infrared. Satellite is for long distance. Microwave has short and medium distance versions, and infrared is for very short distances only.

---

**Key Terms and Concepts**

Bandwidth, 19  
Bluetooth, 6  
Broadband, 7  
Cable modem, 8  
Cat 5 (Category 5), 4  
Client/server network, 11  
Coaxial cable (coax), 19  
Communications medium, 18  
Communications protocol (protocol), 16  
Communications satellite, 21  
Communications service provider, 21  
Computer network, 2  
Digital Subscriber Line (DSL), 8  
Ethernet card, 3  
Firewall, 4  
H Lanspring, 10  
Home PNA (Phoneline Networking Alliance), 6  
Infrared, 20  
International virtual private network (international VPN), 23  
Local area network (LAN), 18  
Microwave, 20  
Municipal area network (MAN), 18  
Network hub, 3  
Network interface card (NIC), 3  
Optical fiber, 20  
Palm, 10  
Palm Operating System (Palm OS), 11  
Peer-to-peer network, 3  
Personal digital assistant (PDA), 10  
PNA adapter card, 6  
Pocket PC, 10  
Pocket PC OS (Windows CE), 11  
Private network, 22  
Public network, 21  
Repeater, 20  
Router, 4  
Satellite modem, 9  
Switch, 3  
Telephone modem (modem), 7  
Value-added network (VAN), 22  
Virtual private network (VPN), 22  
Wide area network (WAN), 18  
WiFi (Wireless Fidelity or IEEE 802.11b), 5  
Wired communications medium, 18  
Wireless network access point (wireless access point), 5  
Wireless communications media, 18  
Wireless Internet service provider (wireless ISP), 10
Short-Answer Questions

1. What is a computer network?
2. What is a peer-to-peer network?
3. How is a peer-to-peer different from a client/server network?
4. What is an Ethernet card?
5. What does a network hub do?
6. How does an Ethernet network work?
7. What is Cat 5 cable used for?
8. What is Bluetooth?
9. What do you need to have a dial-up connection to the Internet?
10. How is a DSL Internet connection different from a telephone modem connection?
11. What is a satellite modem?
12. How is client/server model 1 different from client/server model 2?
13. What is a local area network?
14. What does WiFi do?
15. What are communications service providers?

Short-Question Answers

For each of the following answers, provide an appropriate question:

1. A network card in each computer, a connecting device, a communications medium, and a network operating system.
2. A network in which one or more computers are servers and provide service to the other computers which are called clients.
3. A wireless communications medium that uses a red light that’s below what your eye can see.
4. The amount of information that communications medium can transfer in a given amount of time.
5. A semipublic network that provides services beyond the movement of information from one place to another.
6. It’s a better constructed version of ordinary phone cable.
7. It’s used as a communications medium for phone networks.
8. It covers large geographic distances, such as a state, a country, or even the entire world.
9. A device that acts as a smart hub connection into a network and separates your network from any other network it’s connected to.
10. A standard for wirelessly accessing a local area network.
11. A device that uses your TV cable to deliver an Internet connection.
12. It uses a very thin glass or plastic tube through which pulses of light travel.
13. A network on which your organization competes for time with others.
14. It takes a message, strengthens it, and passes it along.
15. The paths, or physical channels, in a network over which information travels from one place to another.
Assignments and Exercises

1. INVESTIGATE CELL PHONE TECHNOLOGY  A wireless device that you may have used, or perhaps use all the time, is a cell phone. A cell phone is actually a radio (with a transmitter and a receiver) and uses radio waves of certain frequencies. There are different systems (called cellular access technologies) for cell phones: TDMA, GSM, CDMA. Go to the Web and find the answers to the following questions (hint: a good place to look is www.howstuffworks.com):
   A. What do the letters stand for?
   B. What’s the difference between systems?
   C. Why are they called “cell” phones?
   D. Why was this “cellular” method used in the first place?

2. FIND OUT ABOUT PERSONAL DIGITAL ASSISTANTS Many people have personal digital assistants (PDAs), which are hand-held computers that allow you to perform many computer tasks wirelessly. Some of the features of PDAs are calendar management, appointment management, mini spreadsheet and word processing capabilities, Web access, and sometimes even doubling as a cell phone. Do some research on PDAs and answer the following questions:
   A. What are three other features common in PDAs that were not listed above?
   B. What does the term synching mean?
   C. What are the two types of handwriting recognition systems used on PDAs?

3. 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? Can you get wireless Internet access in your area? Compare each available service on price and extras like a help line, or 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?

4. 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 hubs and routers on the Web. Also research Ethernet cards and cables. If you were to get a high-speed Internet connection, such as a cable modem or DSL modem, how much would it cost? Can you buy your own or would you have to rent the modems from the phone or cable company?

5. INVESTIGATE SATELLITE RADIO At the time of this writing there are two satellite radio stations: 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.

6. FIND OUT ABOUT FIREWALLS Go to the Web and find out about software and hardware that protects your computer and home network, respectively.
   A. If you only have one computer connected to the Internet, then a software firewall like Zone Alarm will most likely provide 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 antivirus software. Compare the firewall software on price and features. Some sites to try are as follows:
      • Symantec at www.Sarc.com
      • TREND Micro at www.TrendMicro.com
      • Virus List (a virus encyclopedia) at www.VirusList.com
      • McAffee at www.McAffee.com
   B. If you have a home network, then you’d be well advised to check into a hardware firewall. One place to look is at the LinkSys site (www.linksys.com) or any site that sells computer hardware.
NOTES

PHOTO CREDITS
P. 3, top, © Nance Trueworthy
P. 3, bottom, Photo courtesy of Kinesis Corporation
P. 4, top, © 2001 Linksys Group Inc. All rights reserved.
P. 4, bottom, © 2001 Linksys Group Inc. All rights reserved.
P. 5, top, © 2001 Linksys Group Inc. All rights reserved.
P. 5, bottom, Photo courtesy of Agere Systems Inc.
P. 6, © Microsoft
P. 11, Photo courtesy of Handspring.
P. 19, top, © Spencer Grant/Photo Edit
P. 19, bottom, © Spencer Grant/Photo Edit
P. 20, Courtesy of International Business Machines Corporation. Unauthorized use not permitted.