Chapter 1

Planning the Lay of the LAN

In This Chapter

- Deciding to create a home network
- Homing in on the right operating system
- Understanding how networks work
- Figuring out what hardware you need
- Purchasing kits or individual components

A *network* is a system of two or more computers that are connected in some manner (you have lots of choices about the "manner") and the commonly used term for a network is *LAN,* which stands for Local Area Network. Each computer on the network has access to the files and peripheral equipment (such as printers or modems) on all the other computers on the network. You create those connections with the following elements:

- Hardware in each computer that permits the computer to communicate.
- A cable or a wireless technology that sends data between the computers (using the hardware you installed).
- Software (called a *driver*) that operates the hardware. (I cover drivers in Chapter 6.)

Believe it or not, installing the hardware and software you need on each computer is not complicated at all. Start with the first computer and go through the process one step at a time. After you finish setting up that first computer, you'll see how logical and simple the tasks are.

In fact, anyone who knows how to turn on a computer and use the keyboard and mouse can create a network in an amazingly short amount of time. Many people who installed their own home networks found it so easy and satisfying

that they helped neighbors, friends, and relatives. Some have gone on to neighborhood fame and fortune as part-time consultants to other households who want home networks. They never give away the secret that all of this is extremely easy to do.

In this chapter, I explain some reasons you might want to set up a network in your home, explain your software and hardware alternatives, and tell you more about how different networks *work.* I also discuss some of the technology that's available for your network.

The particulars and the installation steps for all the different types of networking hardware and software are found throughout this book — look for the appropriate chapter titles or check the index to find the particular pages you need.

Why Would I Want a Home Network?

I believe that anyone who has more than one computer in the house should definitely have a network. That belief has its roots in the fact that I'm generally lazy and miserly, and I believe everyone should do everything in the easiest and cheapest way. Here's a list of just some of the ways a home network can benefit your whole household:

- **You can work anywhere in the house, even in bed if you want to.** Suppose that you have an important presentation for your boss, and it's due tomorrow morning. But it's Sunday morning, and you're having your second cup of coffee in your bedroom. It would be so cozy and comfy to use your laptop, in bed, to finish the presentation. Then you realize that when you were working on the presentation *yesterday,* you were sitting at the kitchen computer, slaving away at the presentation while eating a turkey sandwich. You don't have to leave your cozy bed and stumble downstairs to find the most recently saved version of the document — you can open the file that's on the kitchen computer right on the laptop in your bedroom.
- **Your kids won't argue as much.** Sally doesn't have to stop using the computer in the den because Bobby needs to retrieve his homework assignment from it. Bobby can go to the computer in the basement and open the file that's on the computer in the den right on the computer in the basement. There's no need to copy the file to a floppy disk; it's as available and handy as it would be if it were residing on the basement computer.

- **You can put an end to the demands for the computer that has the Internet connection.** Because you can set up your network so that everyone in the household can be on the Internet at the same time, those arguments about whose turn it is to surf the Net are a thing of the past.
- **You can buy yourself an expensive piece of jewelry with the money you save on peripherals.** Okay, not quite, but you will save money because you won't have to buy a printer and modem every time you buy a computer because everyone shares those tools across the network. Even better, the sharing is simultaneous, so you can avoid "It's my turn!" arguments.
- **You can become a god (or goddess).** Another benefit of setting up a home network is that when you install it, you become the *network administrator* (that's what the people who installed the network at your office are called). You may even get to invent usernames and passwords. You'll be in charge of decisions about whether Mom can see Bobby's files or Bobby can see Mom's files. All of this knowledge and power makes you a computer geek. Because I think that being called a computer geek is a compliment, I offer my congratulations to you.

Network Operating Systems (Nothing to Do with Surgery)

You don't have to start creating your network with computers that already contain the hardware and software required for networking because you can easily install that stuff yourself (with the help of this book). However, you must have computers that already run on an operating system that can participate in a network environment.

For this book, I assume that all the computers in your home run Windows XP or Windows Vista. As a result, you won't see specific instructions for performing tasks on any other (earlier) versions of Windows. However, if you happen to have a computer running Windows 98SE or Windows 2000, the instructions in this book should work for you, it's just that you may have to figure out how to open the dialog boxes and windows I refer to because sometimes the menus are different.

Check out the Introduction of this book for other assumptions I've so flippantly made about you.

Network Types — Just Like Personality Types

You can configure networks to operate in any of several *modes,* or *configuration types.* Like personality types, some network configuration types are interested in controlling computer users; other network types are more relaxed about controls. You can choose a mode for your current needs and then easily change your network to another mode if the circumstances warrant. The basic hardware and configuration stuff that goes into creating a network (all of which I cover in this book) are the same for all network types, so your choices depend mostly on how you want to communicate among computers.

Client/server networks for control freaks

Networking schemes that operate in *client/server* mode are almost always found only in businesses. These schemes include a main computer (a *server*) that controls users and holds files and peripherals shared by all the other computers (called *clients* or *workstations*).

One of the most important reasons to install a client/server network is *user authentication,* which is a security feature. The server on a client/server network checks to see if a SuzieQ user is who she says she is and controls whether she can join the network. If she's eligible, the server continues to control her network tasks, determining what she can do. For example, perhaps she can read files but not delete them. The good news is that if you set up the network, you can control *everything.* (Heh, heh, heh.)

All the client computers are connected in a way that gives them physical access to the server. Everyone who works at a client computer can use files and peripherals that are on his or her individual computer (the local computer) or on the server. Look at Figure 1-1 to see the communication between computers in a client/server environment.

Even though all the computers are connected to each other, each client usually communicates with the server. However, you can configure the network so that the users on client computers can also access the other client computers on the network.

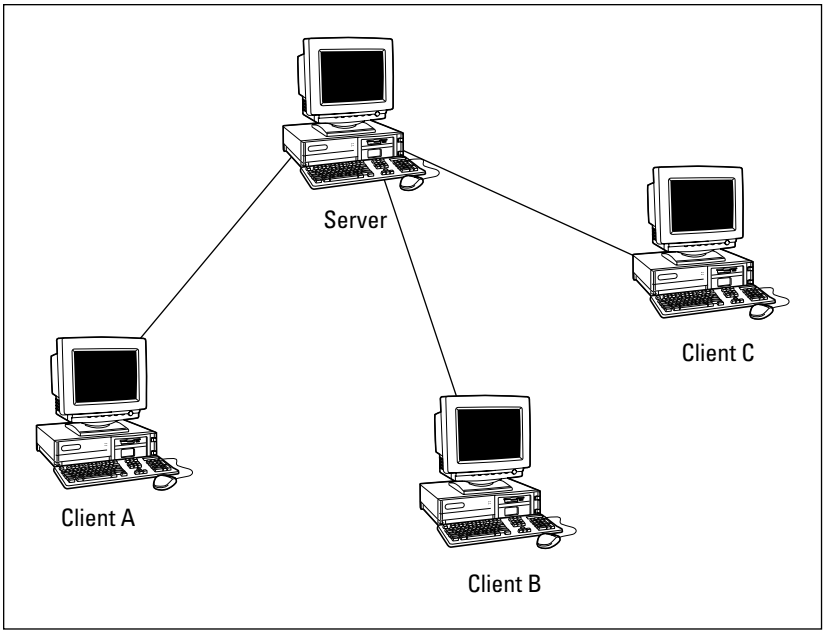

Figure 1-1: In a client/server network, all the client computers have to check in with the server.

Large client/server networks (usually found in the workplace) frequently have multiple servers, and each server has a specific job. For example, one server is used for authenticating users, one manages everyone's e-mail, one contains the accounting software, and yet another has the word processing software. The common network operating systems used for servers on client/server networks are Windows 2000, Windows Server 2003, Novell NetWare, and UNIX/Linux. These kinds of networks may be a *little* more than you need — unless you're thinking of running an enormous enterprise-like business out of your home.

Peer-to-peer networks are more relaxed about controls

Peer-to-peer networks permit all the computers on a network to communicate with each other. In Figure 1-2, you can see a typical peer-to-peer network communication structure.

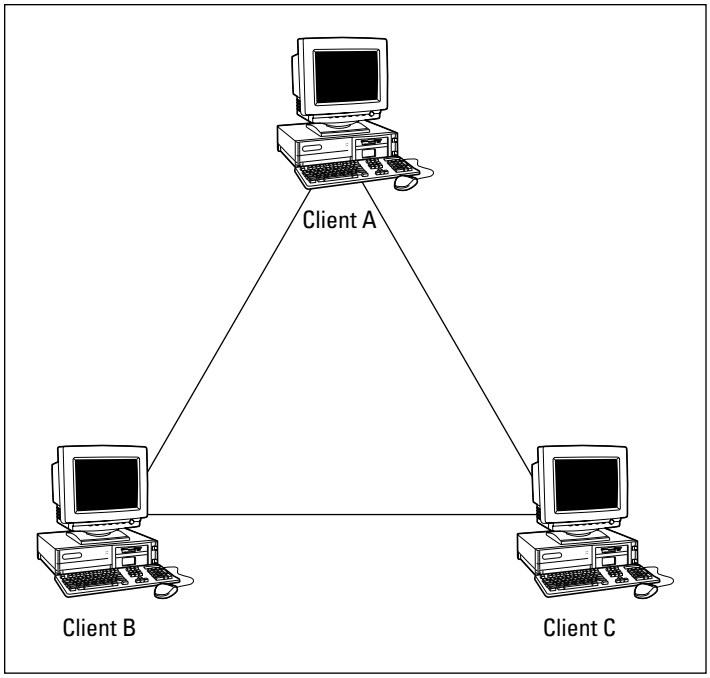

Figure 1-2: Everybody talks to everybody in a peer-to-peer network.

Windows has built-in support for peer-to-peer networks. In fact, this book is really about creating a peer-to-peer network in your home.

With a peer-to-peer network, as long as your network is composed of computers running Windows XP and Windows Vista, you can impose all the security features you want to. You can control files, Windows utilities, and all the other uses of a computer that might be dangerous for some users to access.

Mixed networks fit all types

Just so that you don't think the computer world is rigid, I'll point out that some networks are both client/server and peer-to-peer at the same time. Users log on to the network server and then use it to access software and store the documents that they create. Because the peer-to-peer network is built into the operating system, users can also transfer files from other clients and access printers connected to other clients. A mixed network is the best-of-all-worlds scenario for many businesses.

The Nuts and Bolts of Hardware

To create a network, the primary hardware device that you need is a *network adapter,* also called a *network interface card (NIC).* A NIC must be installed in each computer on the network. It's actually the NICs (not the computer boxes) that are connected to create a network. NICs are traditionally connected via cable. I say *traditionally* because wireless solutions are also available for small networks, and you may prefer to take that route.

Also, even though the term NIC is still commonly used, not all network interface devices are cards anymore. Today, you can connect a network interface adapter device to a *Universal Serial Bus (USB).* However, because of the widespread use of the jargon *NIC,* I use that term generically throughout the book.

The only rule for creating a network is that you must have a NIC in each computer. Beyond that, you have enough choices to make your head spin. I'll try to slow the spin rate by explaining the options before I drag you into the actual installation process (which you can find in Chapter 2).

NICs come in lots of flavors, and when you buy NICs, you must match them to two important elements:

- The type of network interface device that your computer accepts.
- The type of network cabling that you want to use. (See the section, "Connections: Cables, wires, and thin air," later in this chapter.)

Network connection types

Computers have one or more NICs built right into a chip on the motherboard. These built-in devices are called *embedded network cards* or *embedded network controllers.*

Although motherboard NICs are the most common type of network connections, you have several other options available.

USB Connectors

Most of today's computers come with a USB port (in fact, most come with a bunch of USB ports), and you can buy NICs that plug into a USB port. The best part of a USB connection is that you don't even have to open your computer because USB ports are external. Look for USB port connectors that look like those shown in Figure 1-3.

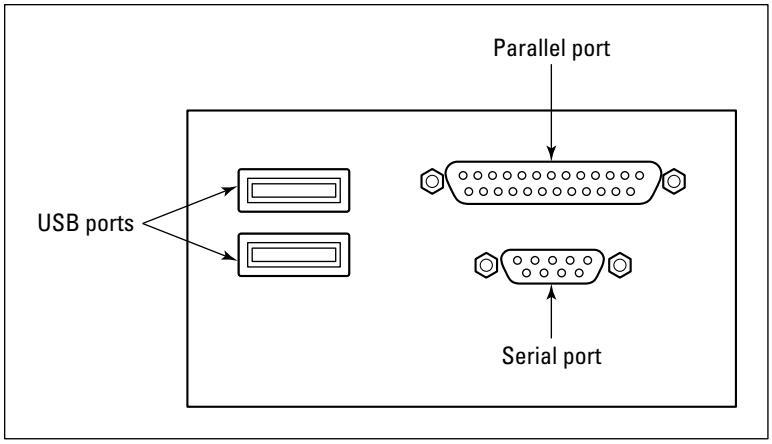

Figure 1-3: USB ports are identical in every computer.

USB connectors are available for all types of network cabling and wireless connections.

NIC Controller Cards

Another way to add a NIC to a computer is to install a card inside the computer, using a PCI slot (your computer has several PCI slots available for installing controllers). Follow the manufacturer's instructions for installing the hardware and drivers.

Connections: Cables, wires, and thin air

You have one more decision to make before you go shopping for your hardware — you have to choose a cabling system. Your decision affects not only the type of cable you buy, but also the type of NICs you buy. The NIC has a device that accepts the cable connector, so the NIC must be built specifically for the cable you choose.

You have several choices for cabling your computers into a network:

- Ethernet cable
- Telephone wires already in your house
- Electrical wires already in your house
- None (wireless connections)
- Mixed (using more than one type)

In the following discussions, I mention the speeds at which cable types transfer data among computers. Network speeds are rated in *megabits per second (Mbps).* A *megabit* is a million binary pulses, and the best way to put that into perspective is to think about a modem. The fastest telephone modems are rated to transmit data at the rate of 56,000 bits per second (56 kilobits per second, or 56 Kbps).

Don't pooh-pooh the notion of speed; it is important. Everyone who uses computers changes his or her definition of the word *fast.* If you started using computers years ago, think about how fast the computer seemed at first, and then how impatient you became whenever you had to wait for a task to complete. Soon after, you bought a faster computer. Then you got over the feeling that this was the fastest machine you'd ever seen, and impatience set in again. Waiting a long time for a file to open in an application or for a file to be copied from one machine to another can drive you nuts.

Ethernet cable

Ethernet cable is the connection type of choice. It's fast, accurate, pretty much trouble-free, and simply the best. Ethernet can transfer data across the network at up to 1000 Mbps, depending on the rated speed of the NICs and the hub or switch. The commonly sold NICs and Ethernet cable operate at 100 Mbps. Most Ethernet equipment can determine the speed of individual devices on the network and automatically drop or raise the speed to match the device's capabilities.

Ethernet is the cable that you find in business networks. The commonly used variety of Ethernet cable is *twisted-pair cable* or *Category 5 UTP cable* (nicknamed *CAT-5*). Although Ethernet cable looks like telephone wire, it's not the same thing. Ethernet cable is designed to transmit data rather than voice. Using Ethernet cable requires the purchase of a *concentrator,* a device that collects all the Ethernet connections in one place. Concentrators are usually sold as devices called *hubs* or *switches.* All the network computers are connected to the concentrator, which distributes the data among the connected computers, as shown in Figure 1-4.

The connector at the end of the cable looks like the connector at the end of your telephone cable, but it's actually slightly fatter. The 10Base-T cable connectors are *RJ-45 connectors* (telephone connectors are *RJ-11 connectors*).

Telephone line cable

Telephone line cable is another option you can choose for wiring your home network. It transmits data at the rate of about 10 Mbps, which isn't nearly as fast as the speed of Ethernet cable. Telephone line networking is increasing in popularity, especially because most of the computer and device manufacturers have developed and accepted standards. Having standardized technology makes it easier to buy equipment; you know it all works together. You can find out more about the technology at `www.homepna.org`.

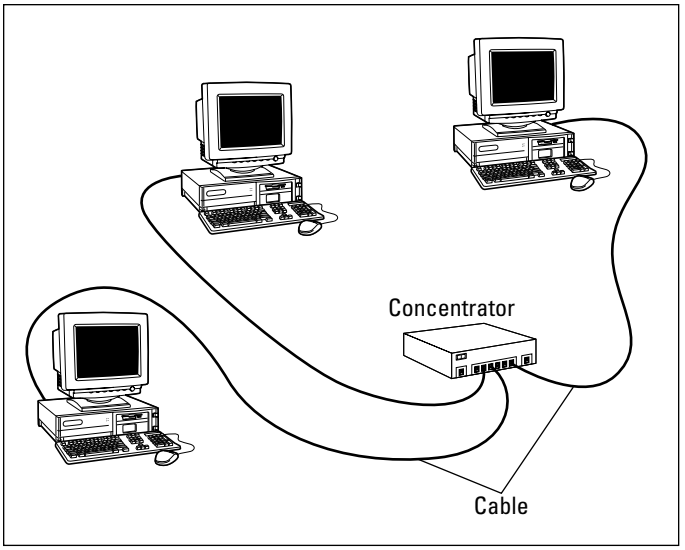

Figure 1-4: Each computer is connected to its own port in the concentrator.

To use telephone cable for home networks, you just connect a regular telephone cable between the telephone-cable NIC you install in your computer and the telephone wall jack. Telephone cable is inexpensive and available everywhere, including your local supermarket. The networking process uses a part of your telephone line that voice communication doesn't use, so your telephone lines are still available for normal household telephone use as well as for modem use.

You can use your wall jack for both a telephone and a network connection at the same time. You just have to adapt the wall jack so that it can do two things at once. Luckily, this is easy to do. You need to buy a *splitter* (the techy term is *modular duplex jack*), which is a little doohickey that you can buy for a couple of bucks just about anywhere — at an office supply store, one of those megastores, or even the supermarket. The splitter, shown in Figure 1-5, plugs into the wall jack to give you two places to plug in phone cables instead of just one. You plug the network cable into one connector and your telephone cable into the other connector. It doesn't matter which cable goes into which socket.

However, to avoid confusion, put some nail polish, a little sticky star, or some other add-on near the connector of your network connection cable so that you know which is which if you want to move the telephone.

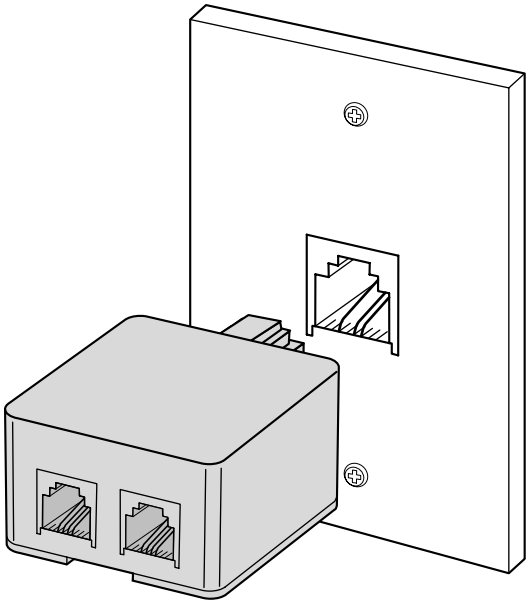

Figure 1-5: Insert a splitter to get double service from your telephone wall jack.

For shared Internet access, only one computer on the network needs to have a modem. If the computer that's hosting the shared Internet access has an external modem, follow these steps:

1. **Plug the splitter into the telephone wall jack.**
2. **Plug the modem, not the telephone, into the second side of the splitter (the network line is on the other side).**
3. **Plug the telephone into the appropriate connector on the modem.**

   Now you have three devices on your telephone jack: a network connection, a modem, and a telephone.

If the computer that's hosting the shared Internet access has an internal modem, you need a *Y-connector,* which is an adapter that looks like the capital letter *Y*. The bottom of the connector, where the two sides of the Y meet, plugs into the wall jack (to join the network). The two ends of the Y plug into the modem and the NIC (it doesn't matter which connector goes into which device). (There's no room on this setup for a telephone.)

If you have multiple telephone lines in your house, all the computers on your network must be connected through the same telephone line (telephone number). Computers can't communicate across different telephone lines. (Your regular telephone service can't do this either. For example, if someone is talking on line 1, you can't pick up a telephone connected to line 2 and eavesdrop, er, I mean, join the conversation.)

Here are a couple of drawbacks to using telephone wiring:

- Every computer must be near a telephone jack. Very few households have a telephone jack in every room, so this may limit your choices for computer placement.
- The maximum distance between any two computers is about 1,000 feet, but unless you live in the White House, that shouldn't be a major problem.

Electrical wires

You can network your computers with electrical line connections that work by plugging the manufacturer's network adapter device into the power outlet on the wall. The device has an attached cable that connects to the computer. Today, most of the electrical-wire network-connection hardware is designed for a USB port. Electrical-wire networking operates at about 10 Mbps. Some network equipment manufacturers use the term *powerline* instead of electrical wire.

I'm not kidding when I say *wall outlet device.* Plugging the network adapter into a power strip doesn't work.

Here's the other stuff you need to know about powerline networking:

- **Um, where do you plug it in?** If your house is like most houses, only one wall outlet is near the computer, and you're already using both plugs: one for the computer and one for the monitor. Most manufacturers of electrical line networking hardware supply a special power strip into which you can plug your computer and monitor. You can plug that power strip into the plug on the wall outlet that the network device isn't using.
- **How friendly do you want to be with your neighbor?** I could get into all the gory details about hubs and transformers and radio waves, but I'll cut to the bottom line: If your neighbor has a home network that's connected through electrical wires, your neighbor may be able to access your network because you probably share the same transformer. That's

either terribly convenient or terribly scary, depending on your relationship with your neighbor. But, to resolve this problem, the network equipment manufacturers provide software to help guard your system against unauthorized users. That software requires a separate installation and configuration process, which must be repeated whenever you add a computer to your network. It's quick and easy to install, so be sure to use it!

Wireless connections for the cable-phobic

Generally, people choose wireless connections because they're willing to give up the speed and reliability of Ethernet (or phone line or powerline) to avoid dealing with cable. This attitude comes from one of two motivations (or, in some cases, both of two motivations): They don't want to go through the effort of pulling cable through the house, or they hate the sight of the cable because it doesn't match their decorating scheme. When installing home networks, my experience has been that the man of the house loves the "fun" of pulling cable through the building, and the woman of the house says "ugh, ugly."

If you opt for wireless technology, you'll be working with *radio frequency (RF)* communication technology. Some manufacturers offer *infrared (IR*) network communication technology devices, but I don't recommend them. In fact, except for the next section that explains why I don't recommend them, I won't mention IR again in this book.

Infrared wireless connections

Infrared (IR) technology works by creating a direct signal, via a light beam, between computers. Your TV remote control (the frequently used technical jargon for that device is *clicker*) uses IR technology; you have a little red square on the remote control device and a red square on the television set or cable box. You point one little red square at the other square to use the device. This means you can't select a channel using the remote control if you're holding it while you're in the kitchen and the television set is in the living room.

Computer IR networking works the same way. The infrared connectors must "see" each other, which limits IR networks to those that have all the computers in the same room. Also, one computer can't make a straight-line connection with two other computers at the same time, so if your network has more than two computers, you have to buy additional IR hardware devices that collect and bounce the IR signals around the room.

One problem I've encountered during my tests of IR connections is that bright sunlight interferes with the signal. You need opaque window coverings if you want to go with IR connections unless you plan to use your computers only at night. On top of all of those inconveniences, IR connections are slow.

'Nuff said.

Radio frequency wireless connections

Radio frequency (RF) technology isn't new; it has been around for a long time. I used it when I was a child (many eons ago) for walkie-talkie conversations with friends in the neighborhood. You probably use it today to open and close your garage door or to connect windows on upper floors to your household security system. I used to use it to unlock my car door, but I learned to hate the beeps, and I set off my car alarm system so often that I had the whole system disabled.

Here are some things to consider about RF network connections:

- They require a network adapter that's specific to RF technology, which means the adapter has to be equipped with the devices necessary to transmit and receive RF signals. Today, all network device manufacturers make RF devices, and the NICs are available for motherboards (you have to install them in the PCI slots inside the computer), USB ports, and PC Cards for laptops.
- The RF signals can usually travel about 150 feet, passing through walls, ceilings, and floors. This distance should be sufficient for most home network schemes, but the actual distance that you can achieve may vary from manufacturer to manufacturer. If you need greater distance, you can often extend the signal by placing a special box called an *access point* in a central location.
- The only things that can stop the RF signal dead in its tracks are metal and large bodies of water. Although you may think that only means you can't use RF technology in your castle with an iron drawbridge and moat, think again. Putting the computer (with its RF technology device attached) under a metal desk can interfere with transmission. A wall that has a lot of metal plumbing pipes can also keep computers from communicating. The only problem with large bodies of water I can think of are those that crop up if you've installed a pond or swimming pool in your den, or if you're trying to communicate between two submarines or from an underwater office in a Sea World type of amusement park.

  When I was testing RF technology, several manufacturers assured me that the 150-foot limit applies only indoors and that most RF devices can achieve far greater distances with no walls or floors in their way. Uh huh, thanks. I'll appreciate that in the summer when I move all my computers onto my lawn or take them to a park. And, I've never seen an RF

network that achieved anywhere near 150 feet of signal; you can count on about a third of that distance.

- You may experience interference from cell phones, pagers, home alarm systems, microwave ovens, and other wireless devices frequently found in your neighborhood. If those RF devices are properly shielded, however, you shouldn't have any problems. The newer RF devices, based on newer RF technical standards, eliminate a lot of the annoyances of interference.
- Technically, anyone with a computer equipped with RF technology can "join" your network without your knowledge. A neighbor or stranger could come within 150 feet of your house with a laptop, find the right frequency, and copy any files he finds. For security, some manufacturers of RF networking kits have built in a clever design feature that slows malevolent outsiders who are trying to grab your frequency and get into your system — the frequency changes periodically.

  The RF signal that's sent and received across the network moves up and down within a given range (the technology is called *frequency hopping*), and this happens often enough to make it difficult to latch on to the current frequency — as soon as someone gets a bead on it, it moves.

  By the way, the idea of frequency hopping for security comes from an invention and a patent that are credited to composer George Antheil and actress Hedy Lamarr. (Is anyone besides me old enough to remember her?)

  Frequency hopping also acts as a performance enhancer. The speed is improved because you're effectively transmitting across a wider spectrum.

Saving Time, Trouble, and Money When You Buy Hardware

A slew of manufacturers make the equipment that you need to build your network, and you should make your purchasing decisions with an eye on both reliability and price.

Throughout the book, I mention some places to go for general research as you do your homework, as well as some places to buy equipment that I think provide good prices and service. None of these outlets knows that I'm telling you about this, so they aren't paying me any commission or giving me special treatment in exchange for telling you about them. I'm just one of those people who can't resist giving specific advice (which, as all parents know, doesn't

work well with children, but I don't expect readers to respond with "Oh, Motherrrrr," and leave the room). You may discover resources that I don't mention here, and my omission isn't significant. It just means that I didn't know about (or knew about but didn't remember) that resource.

Doing your homework: Just like being in school

Making decisions about hardware, cable types, and other networking gizmos without first doing some homework is foolish. You're going to live with your decisions for a long time. In fact, everybody in the household will have to live with your decisions, so to avoid listening to gripes later, get everyone to help in the decision-making process. Home networking is a hot topic, and computer experts have been testing technologies and reporting their findings. Use their expertise to gain knowledge and then discuss your findings with the rest of the family. You can find reviews of the pros and cons of networking schemes in the following places:

- **Start with any friends, relatives, or neighbors who are computer geeks.** All computer geeks are used to this treatment; people ask us for free advice at dinner parties, while we're in line at the movie theater, and almost anywhere else. Do what most people do — call the geek and pretend it's a social call. Then, after you ask, "How are you?" and before the geek has a chance to answer that question, ask your technical questions. (This is how most people interact with their computer-savvy friends.)
- **Paw through newsstands, especially those in bookstores.** You can find an enormous array of computer magazines on the shelves. Look for magazines that fit your situation. For example, a computer magazine named *Programming Tricks for C++* is probably less suitable than *Home PC Magazine.* Look for *PC World, PC Magazine,* and other similar publications. If the current issue doesn't have an article on home networking, check the masthead (the page where all the editors are listed) to see where you can call or write to ask for specific issues.
- **Search the Internet for articles and advice.** Type **home networking** into any search box, and you'll probably find that the number of results is overwhelming. If that approach seems onerous, try some of these popular sites that surely have the information you're seeking: `www.pcworld.com`, `www.zdnet.com`, or `www.cnet.com`. These sites all have search features, so you can find information easily. They also have reviews, technical advice, and "best buy" lists.

Plunking down the money: Tips for buying

After you decide which type of hardware and cabling you want to use for your home network, you need to buy the stuff. You can buy kits or individual components, and many people buy both. Your cost should be less than $60 per computer to create your network.

Most manufacturers offer kits, which is a way to buy everything you need at once. Here are some things to keep in mind before you buy a kit:

- **Most kits are designed for a two-computer network.** If you have a third computer, just buy the additional components individually. Some manufacturers make four-computer and five-computer kits.
- **Kits aren't necessary if one of your computers has a built-in network adapter.** Most computer manufacturers sell computers that are already set up with network hardware (usually with an Ethernet NIC).

In Table 1-1, I list some reliable manufacturers of networking products.

Table 1-1 Network Connection Manufacturers

Manufacturer	*Web Site*
3Com	www.3com.com
Belkin	www.belkin.com
D-Link	www.dlink.com
Intel	www.intel.com
Intellon	www.intellon.com
Linksys	www.linksys.com
Netgear	www.netgear.com

Even if you buy a kit, you may also have to buy individual components. Perhaps you have three computers, or maybe one of the Ethernet cables in the kit isn't long enough to reach the computer on the second floor. After you measure the distances, figure out where the available ports are, and do all the rest of your research, you may find that buying individual components is the

only approach you can take. A plan that doesn't match a kit isn't uncommon, and kits are really a convenience, not a money-saver. Most people find that buying individual components costs about the same as buying kits.

Every retail computer store sells hardware components for all types of network connections, and your city or town probably has many small independent computer stores in addition to major chains such as CompUSA. Most appliance retailers (Circuit City, Best Buy, and others) also carry computer networking equipment, and so do office-supply stores (Staples, Office Max, and others). Even some of the warehouse outlets carry networking equipment. On the Internet, visit `www.cdw.com` and `www.buy.com` to find good deals on networking hardware.

Be sure you know an online merchant's return policy before you purchase. And, be sure that the Web site is secure before you give out your credit card number. When you're on a secure Web site, the address bar displays `https://` instead of `http://` (the *s* is for *secure*). Furthermore, at the bottom of your browser window, you should see an icon that looks like a closed lock.