chapter

seven networking

connecting computing devices

objectives

After reading this chapter, you should be able to answer the following questions:

1. What is a network, and what are the advantages/disadvantages of setting up one? ***(pp. 309–310)***
2. What is the difference between a client/server network and a peer-to-peer network? ***(pp. 310–312)***
3. What are the main components of every network? ***(pp. 312–315)***
4. Which type of network is most commonly found in the home? ***(p. 315)***
5. What equipment and software do I need to build a network in my home? ***(pp. 319–322)***
6. Besides computers, what other devices would I connect to a home network? ***(pp. 322–326)***
7. Why are wireless networks more vulnerable than wired networks, and what special precautions are required to ensure my wireless network is secure? ***(p. 327)***
8. How do I configure the software on my computer and set up other devices to get my network up and running? ***(pp. 329–334)***
9. What problems might I encounter when setting up a wireless network? ***(pp. 334–335)***

multimedia resources

Active Helpdesk

- Understanding Networking **(p. 325)**

Sound Bytes

- Installing a Home Computer Network **(p. 325)**
- Securing Wireless Networks **(p. 327)**

Companion Website

The Companion Website includes a variety of additional materials to help you review and learn more about the topics in this chapter. Go to: ***pearsonhighered.com/techinaction***

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

how cool is this?

how cool is *this?*

As you have probably already experienced, wireless connectivity is not always free. Many businesses, such as Starbucks, **charge** customers for each device they want to connect, which can become expensive for groups of friends trying to surf the Internet while waiting to **catch a flight** at the airport. Connectify is free software that takes an existing Internet connection and turns it into a wireless hotspot. So if you are connected to the Internet on your notebook, the **Connectify** software turns your notebook computer into a wireless hotspot so that you and your friends can connect other WiFi-enabled devices such as a cell phone or **gaming** system through the same Internet connection. The hotspot you create features easy connectivity and encryption of data for solid **security**.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Networking Fundamentals

Now that we are into the second decade of the 21st century, most homes have more than one computing device that is capable of connecting to the Internet. A typical family, like the Diaz family (see Figure 7.1), might be engaged in the following: Carlos (the father) is watching a movie, which he downloaded yesterday on the large-screen HDTV in the living room while checking his Gmail

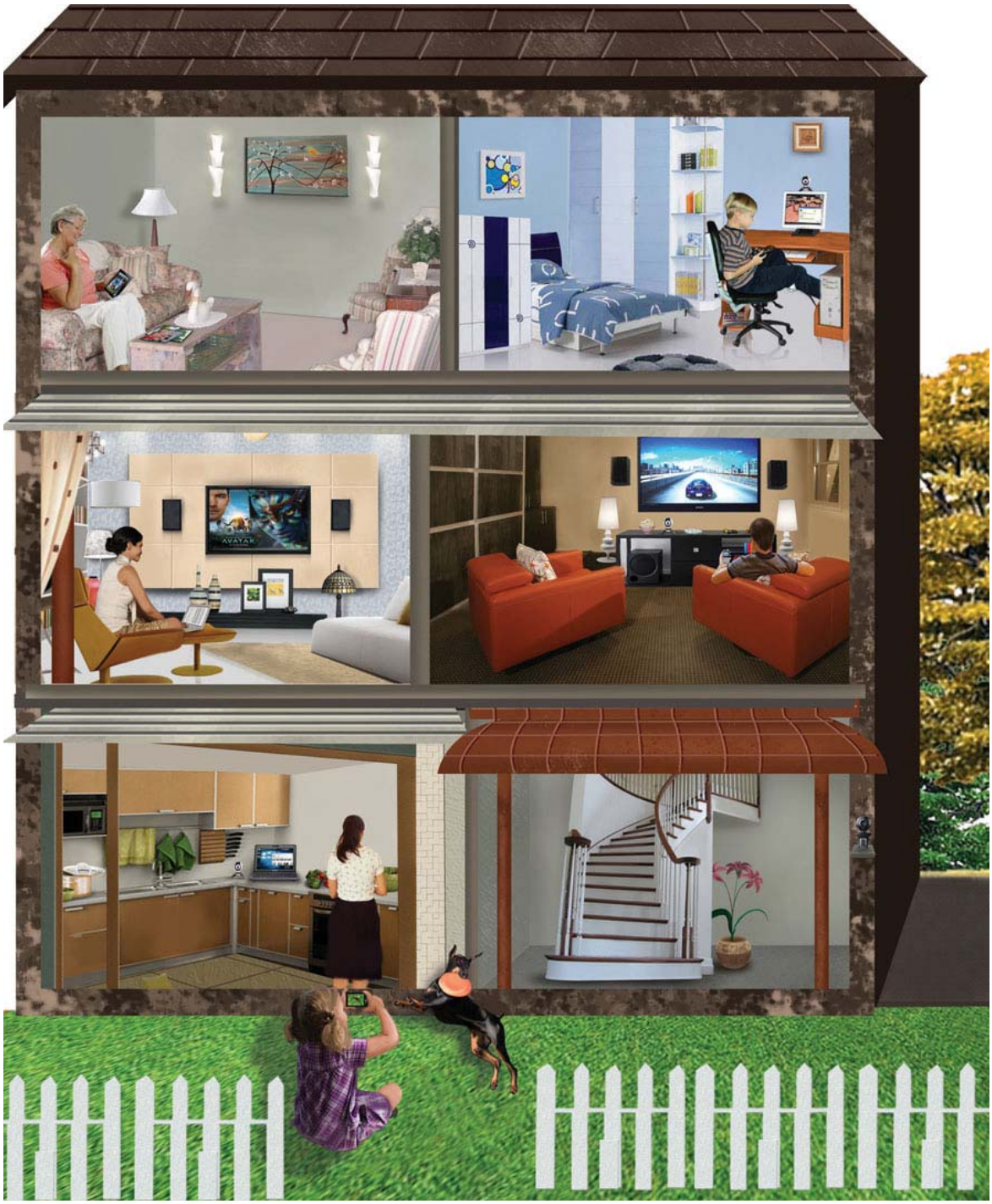


Figure 7.1

By setting up a home network, everyone in the family can connect their computers and others devices whenever and wherever they desire.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

on his smartphone. Camila (the mother) is in the kitchen fixing lunch while checking the weather forecast and watching YouTube videos. Antonio, their fifteen-year-old son, is in his bedroom playing an online game with his friends (via his PlayStation) and is uploading a video he made for a class project to a Web site at school. Adriana, Antonio's older sister, is in the den using her notebook computer to finish a report for school. She's also watching a Blu-ray disc of *Avatar*, which is one of her all-time favorite movies. Grandma Cecilia is in the family room viewing pictures from the family's last vacation and is uploading to Facebook the pictures that she took of her grandchildren during their trip to Disneyland last week. And Angel, the youngest daughter, is playing with Sparky in the backyard and uploading video that she took of him with her phone so that everyone can see it in the family room while they eat lunch. And because both Carlos and Camila work outside the home, they use webcams to monitor activities in the house, like ensuring their kids arrive home safely from school, while they are at work. What makes all this technology transfer and sharing possible? A home network!

What is a computer network? A computer **network** is simply two or more computers that are connected via software and hardware so that they can communicate with each other. You access networks all the time whether you realize it or not. When you use an ATM, get gasoline, or use the Internet (the world's largest network), you are interacting with a network. Each device connected to a network is referred to as a **node**. A node can be a computer, a peripheral (such as an all-in-one printer), a game console (such as a PlayStation or a Wii), a digital video recorder (such as a TiVo), or a communications device (such as a modem). The main function for most networks is to facilitate information sharing, but networks provide other benefits.

What are the benefits of networks? There are several benefits to having computers networked. Most home users want a network to facilitate resource sharing. For example, a network allows you to share the high-speed Internet connection coming into your home. Networks also allow you to share peripheral devices, such as printers. Figure 7.2a shows two computers that are not networked. Computer 1 is connected to the printer, but Computer 2 is not. To print files from Computer 2, users have to transfer them using a flash drive or another storage medium to Computer 1, or they have to disconnect the printer from Computer 1 and connect it to Computer 2. By networking Computer 1, Computer 2,

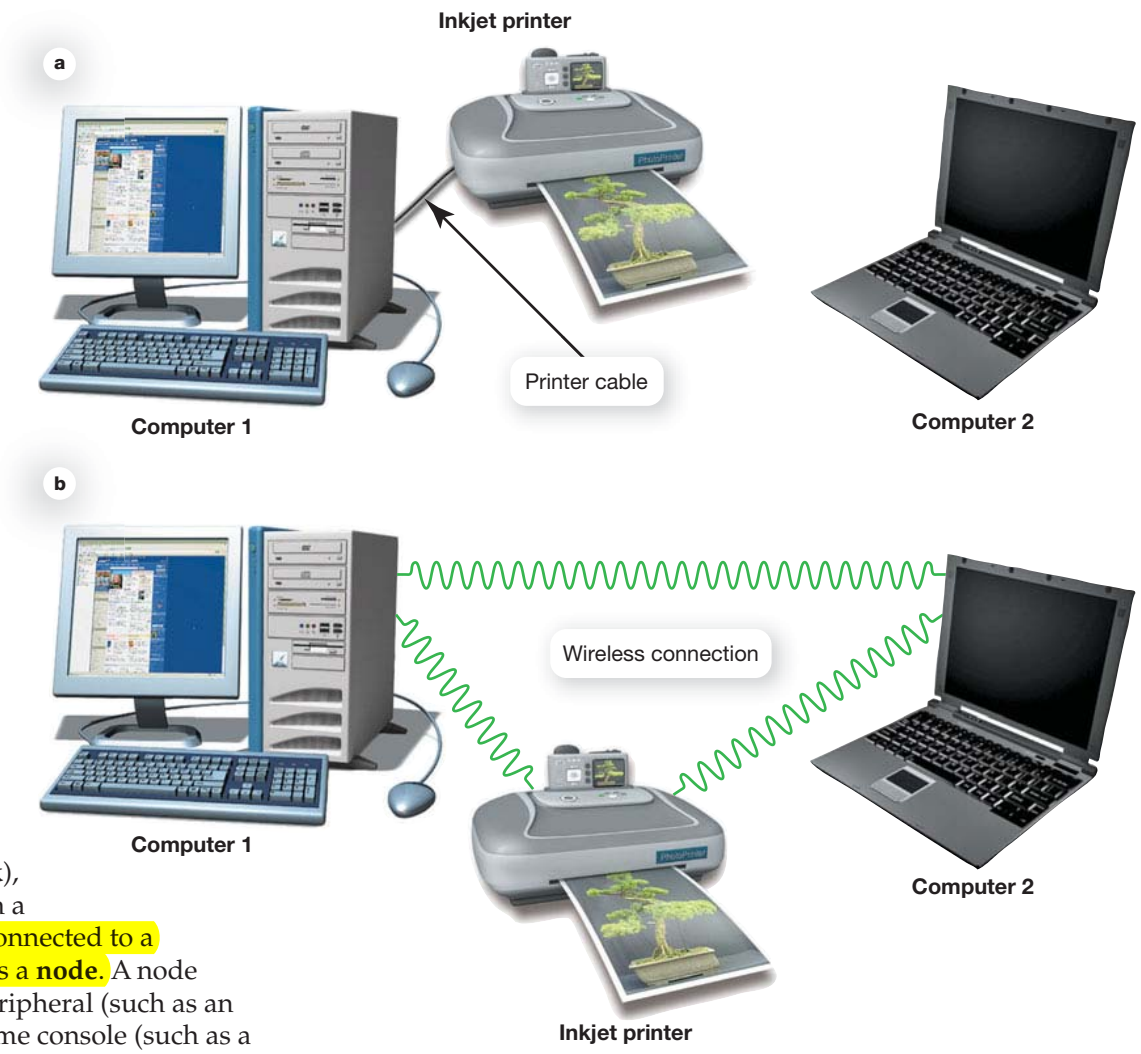


Figure 7.2
(a) Computers 1 and 2 are not networked, and Computer 2 cannot access the printer. (b) Networking allows sharing of the printer.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

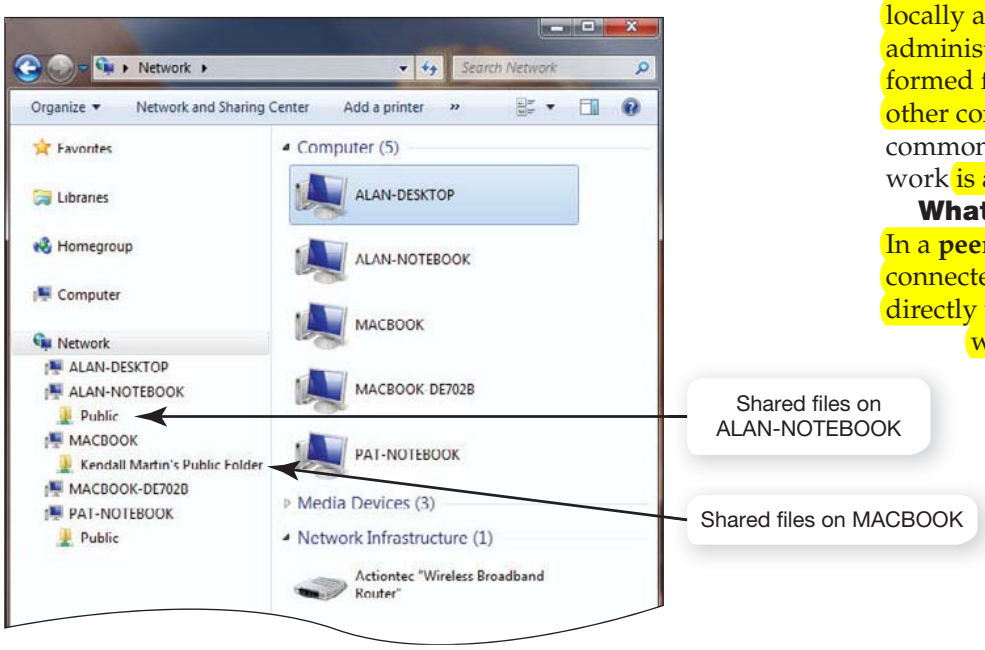
and the printer, as shown in Figure 7.2b, both computers can print from the printer without transferring files or attaching the printer to a particular computer. Using a wired or wireless network to share a printer saves the cost of buying one printer for each computer.

Besides peripheral and Internet connections, does networking facilitate any other types of resource sharing? You can also easily share files between networked computers without having to use portable storage devices such as flash drives to transfer the files. In addition, you can set sharing options in Windows or OS X that allow the user of each computer on the network to access files (such as music or videos) stored on any other computer on the network, as shown in Figure 7.3.

This Windows network has five computers attached to it. ALAN-DESKTOP, ALAN-NOTEBOOK, and PAT-NOTEBOOK are running the Windows operating system. The two MACBOOKs are running OS X. The Public folders enable file sharing because the user of any computer on the network can access the Public folder's contents. And note the final advantage of networking: computers running different operating systems (such as Windows and OS X) can communicate on the same network.

Are there disadvantages to setting up a network? Networks involve the purchase of additional equipment to set them up, so cost is one disadvantage. Also, networks need to be administered, at least to some degree. **Network administration** involves tasks such as: 1) installing new computers and devices, 2) monitoring the network to ensure it is performing efficiently, 3) updating and installing new software on the network, and 4) configuring, or setting up, proper security for a network. Fortunately, most home networks do not require a great deal of administration after their initial configuration, and the benefits of using a network usually outweigh the disadvantages.

Figure 7.3
Windows Explorer showing five networked computers set up for sharing.



Network Architectures

The term **network architecture** refers to the design of a network. Network architectures are classified according to the way in which they are controlled and the distance between their nodes.

Describing Networks Based on Network Administration

What different types of control do I have over my network? A network can be administered, or managed, in either of two main ways: locally or centrally. Local administration means that the configuration and maintenance of the network must be performed on each individual computer attached to the network. A peer-to-peer network is the most common example of a locally administered network. Central administration means that tasks can be performed from one computer and affect the other computers on the network. The most common type of centrally administered network is a client/server network.

What is a peer-to-peer network? In a **peer-to-peer (P2P) network**, each node connected to the network can communicate directly with every other node on the network. Thus, all nodes on this type of network are peers (equals). When printing, for example, a computer on a P2P network doesn't have to go through the computer that's connected to the printer. Instead, it can communicate directly with the printer. Figure 7.2b, shown earlier, shows a very small peer-to-peer network.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

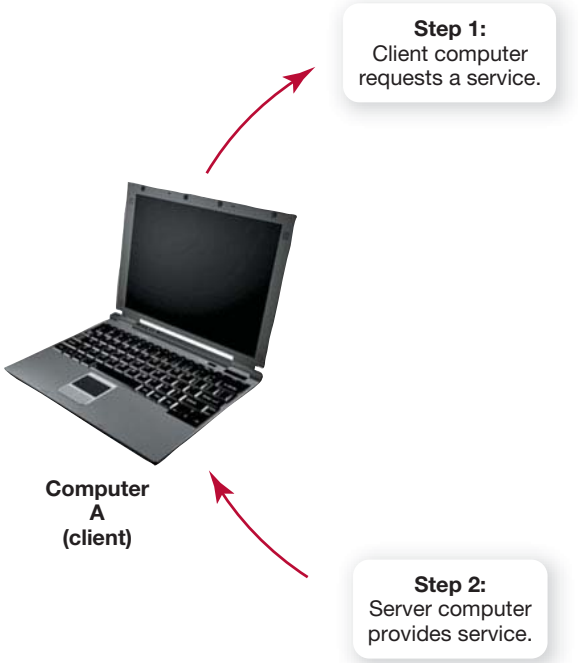


Figure 7.4

In a client/server network, a computer acts either as a client making requests for resources or as a server providing resources.

Because they are simple to set up, P2P networks are the most common type of home network. Very small schools and offices may also use P2P networks. However, most networks that have 10 or more nodes are client/server networks.

What are client/server networks? A **client/server network** contains two different types of computers: clients and servers. A **client** is a computer on which users accomplish specific tasks (such as construct spreadsheets) and make specific requests (such as printing a file). The **server** is the computer that provides information or resources to the client computers on the network. The server on a client/server network also provides central administration for network functions such as printing. Figure 7.4 illustrates a client/server network in action.

As you learned in Chapter 3, the Internet is an example of a client/server network. When your computer is connected to the Internet, it is functioning as a client computer. When it accesses the Internet through an Internet service provider (ISP), your computer connects to a server computer maintained by the ISP. The server "serves up" resources to your computer so that you can interact with the Internet.

Are client/server networks ever used as home networks? Although client/server networks can be configured for home use, P2P networks are more often used in the home because they cost less than client/server networks and are easier to configure and maintain. However, specialized types of servers (such as servers for sharing files) are now appearing on P2P networks in the home.

Nowadays, the individuals in most homes are accumulating vast amounts of media files from digital cameras, camcorders, video downloads, and music downloads. Because users often want to share this media, specialized home network servers such as the Acer Aspire easyStore servers featuring Windows Home Server are now available for home networks. A **home network server** is designed to store media, share media across the network, and back up files on computers connected to the network (see Figure 7.5). All computers connected to the network can access the server.

Figure 7.5

At only 8 inches high, the Acer Aspire easyStore server can perform a variety of tasks to simplify media management on a home network.

Even though a server may now be attached to a home network, that does not change the architecture of a home network from a P2P network to a client/server network. Except for the specialized functions of the home network server, all network administration tasks (such as installation

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

of software and changing of configuration settings) must still be performed locally, and all the nodes on the network are still peers to each other.

Describing Networks Based on Distance

How does the distance between nodes define a network? The distance between nodes on a network is another way to describe a network. A **local area network (LAN)** is a network in which the nodes are located within a small geographic area. Examples include a network in a computer lab at school or at a fast-food restaurant. A **home area network (HAN)** is a network located in a home. HANs are used to connect all of a home's digital devices, such as computers, peripherals, phones, gaming devices, digital video recorders (DVRs), and televisions.

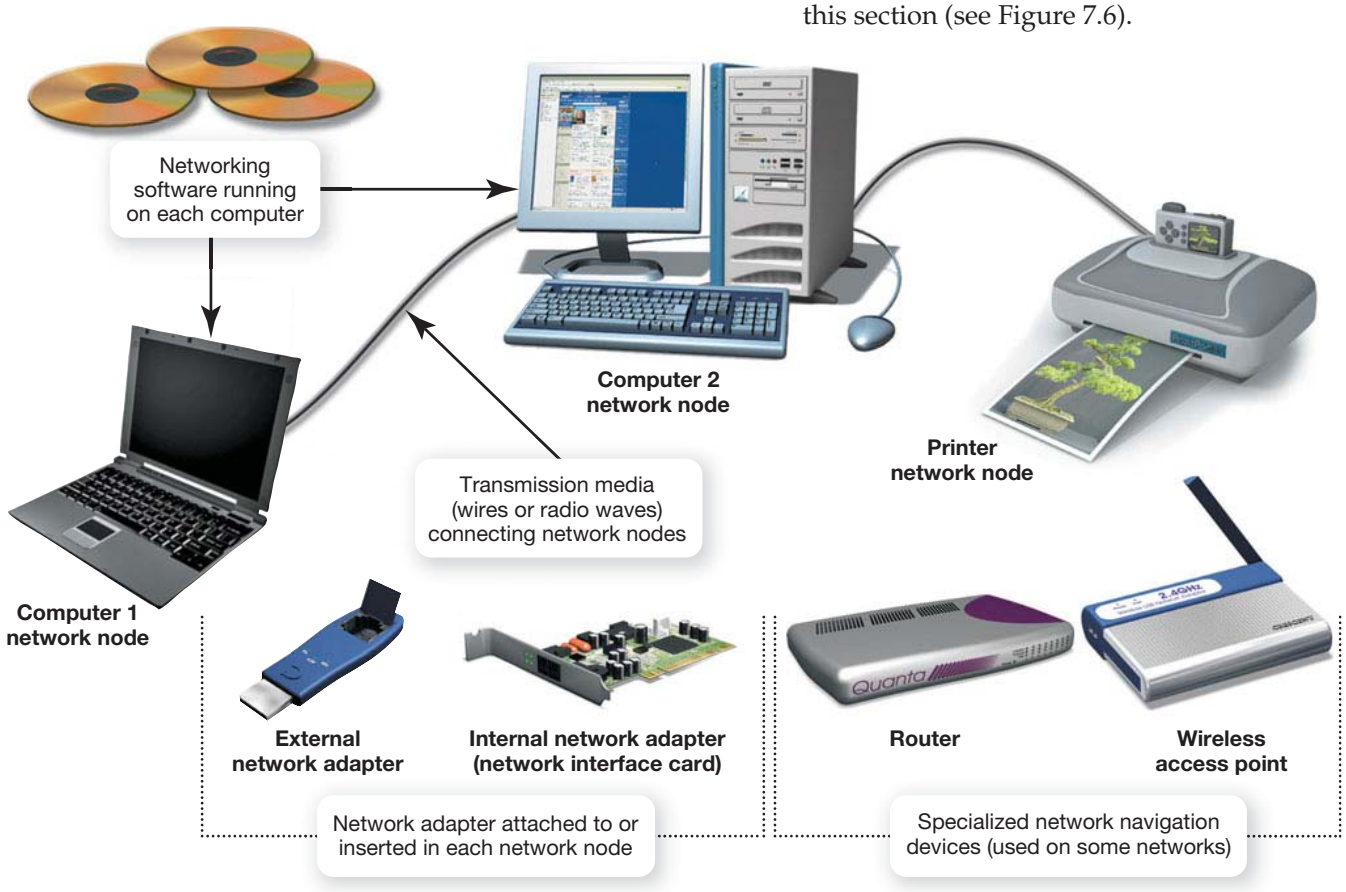
Is it possible to connect LANs? A **wide area network (WAN)** is made up of LANs connected over long distances. Say a school has two campuses (east and west) located in different towns. Connecting the LAN at the east campus to the LAN at the west campus by telecommunications lines would allow the users on the two LANs to communicate. The two LANs would be described as a single WAN.

Are wireless networks that cover large areas like cities considered WANs? Technically, wireless networks like the one deployed in Minneapolis, which provides Internet access to city residents and visitors, are WANs. However, when a network is designed to provide access to a specific geographic area, such as an entire city, the network is usually called a **metropolitan area network (MAN)**. Many cities in the United States are now deploying MANs to provide Internet access to residents and provide convenience for tourists.

Network Components

To function, all networks must include (1) a means of connecting the nodes on the network (cables or wireless technology), (2) special devices that allow the nodes to communicate with each other and to send data, and (3) software that allows the network to run. We discuss each of these components in this section (see Figure 7.6).

Figure 7.6
Network components.



ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Transmission Media

How are nodes on a network connected? All network nodes are connected to each other and to the network by transmission media. **Transmission media** establishes a communications channel between the nodes on a network and can either be wireless or wired.

Wireless networks use radio waves to connect nodes. With the proliferation of portable devices being connected to home networks, a network with at least some wireless connectivity is preferred in most homes.

Wired networks use various types of cable (wires) to connect nodes. **Twisted-pair cable** is made up of copper wires that are twisted around each other and surrounded by a plastic jacket. Normal telephone cable is a type of twisted-pair cable, although phone cable won't work for connecting a home network and a slightly different type of twisted-pair cable is used. **Coaxial cable** consists of a single copper wire surrounded by layers of plastic. If you have cable TV, the cable running into your TV or cable box is most likely coaxial cable. **Fiber-optic cable** is made up of plastic or glass fibers that transmit data at extremely fast speeds. Verizon's FiOS service uses fiber-optic cable to run very fast data connections directly up to your home, although fiber-optic cable is not usually run inside the home. On a FiOS network, twisted-pair or coaxial cable is still used inside the home to transport the network signals.

> "All computers sold today contain network adapters."

Does it matter what type of media you use to transfer data? The media you choose depends on the requirements of a network's users. Using wireless media is critical when portable computing devices (such as smartphones) need to be connected to a network. However, higher speed connections (than can be achieved by wireless connectivity) are required for certain types of network activities, such as downloading large files such as movies. Different types of transmission media transmit data at different speeds.

Data transfer rate (also called **bandwidth**) is the maximum speed at which data can be transmitted between two nodes on a network. **Throughput** is the actual speed of data transfer that is achieved. Throughput is always less than or equal to the data transfer rate. Data transfer rate and throughput are usually measured in megabits per second (Mbps). (A megabit is 1 million bits.) Twisted-pair cable, coaxial cable, and wireless media usually provide enough bandwidth for most home networks.

Network Adapters

How do the different nodes on the network communicate? **Network adapters** are devices connected to or installed in network nodes that enable the nodes to communicate with each other and to access the network. All desktop and notebook computers (and many peripherals) sold today contain network adapters installed *inside* the device. This type of adapter is referred to as a **network interface card (NIC)**. Different NICs are designed to use different types of transmission media. Most NICs included in computing devices today are built to use wireless media but many can use wired media as well. Your notebook computer most likely has a wireless NIC in it that allows you to connect to wireless networks (home, school, or the coffee shop). But most notebooks also have a port on the side that accommodates cable for a wired connection to a network.

Why would I ever consider using a wired connection with my notebook computer? Wired connections can sometimes provide greater throughput than current high-speed wireless networks. Here are some common reasons why wireless signals may have decreased throughput:

- Wireless signals are more susceptible to interference from magnetic and electrical sources.
- Other wireless networks (such as your neighbor's network) can interfere with the signals on your network.
- Certain building materials (such as concrete and cinderblock) and metal (a refrigerator) can decrease throughput.
- Throughput varies depending on the distance from your networking equipment.

Wireless networks usually use specially coded signals to protect their data whereas

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

ETHICS IN IT

Sharing Your Internet Connection with Your Neighbors: Legal? Ethical? Safe?

With the advances in wireless equipment, signals can travel well beyond the walls of your home. This makes it possible in an apartment or single family home (where homes are close together) for a group of neighbors to share a wireless signal and potentially save money by splitting the cost of one Internet connection among them. However, before jumping into this venture, you need to weigh a few issues carefully.

You probably aren't legally prohibited from sharing an Internet connection, but you should check on the state and local laws. Most laws are designed to prohibit piggybacking, which is using a network without the account holder's consent. However, if you are giving neighbors permission to share your connection, you probably don't violate any piggybacking laws.

Of course, your ISP might not permit you to share your Internet access with anyone. You probably have a personal account that is designed for one household. The terms of your agreement with the Internet provider might prohibit you from sharing your connection with people outside your household. If you aren't allowed to share the type of account you have now, your ISP probably offers a type of account (such as a small business account) that will allow you to share a connection, but it will most likely be more expensive. The ISPs know that the more people that share an account, the more likely that account is to use bandwidth; so they price their accounts accordingly. You might be able to share a personal account without being detected by your ISP, but that certainly would be unethical because you should be paying for a higher level of access. Therefore, make sure to check with your ISP to determine that you have the right type of account.

The next thing you need to consider is whether the shared access should be open to all neighbors, or just to the neighbors that are contributing to the cost of the Internet connection. You could leave the connection open (like the connections at Panera Bread) and let anyone who finds it log on and surf. You might consider this a very ethical action, because you are providing free Internet access for anyone who needs it. You could register your free hot spot with a service like JiWire, and then people would know where it is. However, your neighbors who are helping pay the cost might have a different viewpoint and not want to fund free surfing for everyone. Make sure you work this out before proceeding.

If you are going to host a free and open hot spot, you still need to make sure that you set it up safely. You want to maintain a secure network for you and your neighbors while still allowing the occasional visiting surfer to use the connection. There are WiFi sharing services (see Figure 7.7) such as Fon (**fon.com**), Whisher (**whisher.com**, now owned by **wifi.com**), and WeFi (**wefi.com**) that can provide you with special hardware (a router) or software that allows you to configure your hot spot so your network remains secure.

While offering free access to anyone will earn you lots of good karma, additional risks exist because you don't know what mischief or criminal activities someone might engage in while connected to the Internet through your account. Think very carefully before you proceed down the sharing path, and make sure you set your hot spot up to protect your internal network.

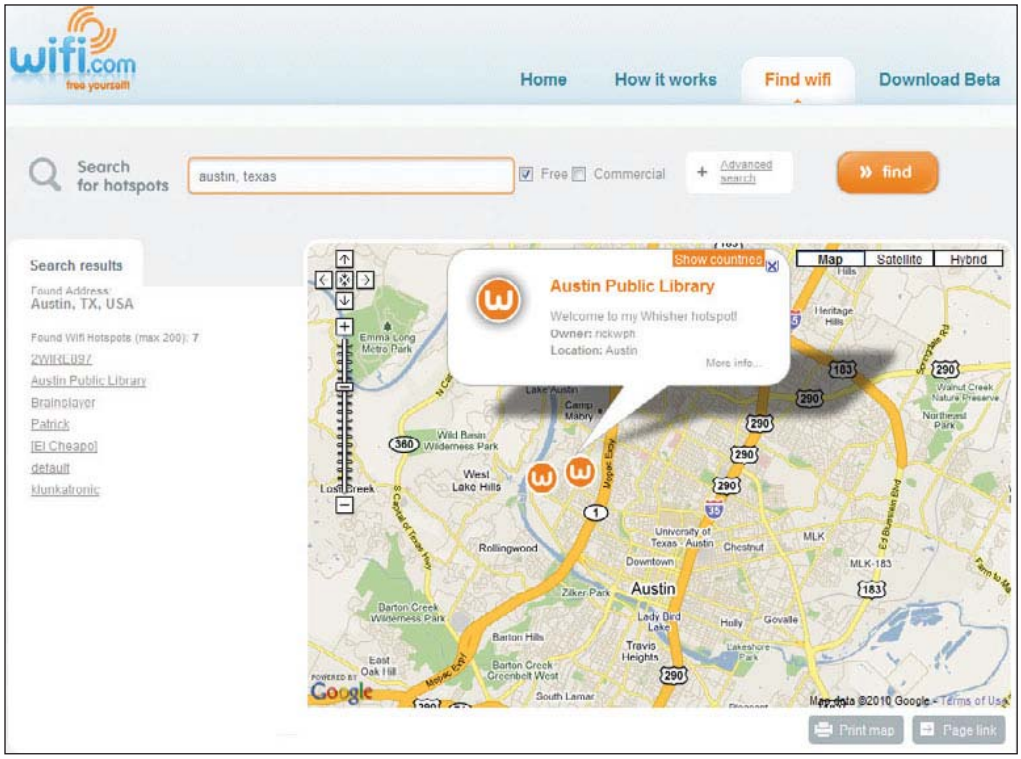


Figure 7.7

At Wifi.com you can search and find free hot spots hosted by other Whisher users.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

wired connections don't protect their signals. This process of coding signals can slightly decrease throughput, although once coded, data travels at usual speeds.

Therefore, in situations where you want to achieve the highest possible throughput (transferring a large video), you may want to connect your notebook (or other portable device) to your home network using a wire (at least temporarily). We'll discuss this type of connection in more depth when we talk about home Ethernet networks later in this chapter.

Network Navigation Devices

How is data sent through a network? **Network navigation devices** facilitate and control the flow of data through a network. Data is sent over transmission media in bundles. Each bundle is called a **packet**. For computers to communicate, these packets of data must be able to flow between network nodes. Network navigation devices, which are themselves nodes on a network, enable the transmission of data between other nodes on the network that contain NICs.

> "Home networks need operating system software that supports P2P networking."

What network navigation devices will I use on my home network? The two most common navigation devices are routers and switches. A **router** transfers packets of data between two or more networks. For example, if a home network is connected to the Internet, a router is required to send data between the two networks (the home network and the Internet). A **switch** is a "traffic cop" on a network. Switches receive data packets and send them to their intended nodes on the same network (not between different networks). All routers sold for home use have switches integrated into them. We discuss routers for home networks in more detail later in the chapter.

SOUND BYTE Installing a Home Computer Network

Installing a network is relatively easy if you've seen someone else do it. In this Sound Byte, you'll learn how to install the hardware and configure Windows for a wired or wireless home network.

Networking Software

What software do home networks require? Home networks need operating system (OS) software that supports P2P networking. The Windows, OS X, and Linux operating systems all support P2P networking. You can connect computers running any of these OSs to the same home network (we also cover configuring software for home networks later in the chapter).

Is the same software used in client/server networks? Client/server networks are controlled by centralized servers that have specialized **network operating system (NOS)** software installed on them. This software handles requests for information, Internet access, and the use of peripherals for the rest of the network nodes. As opposed to P2P networks, the nodes on a client server network do not communicate directly with each other but communicate through a server. Communicating through a server is more efficient in a network with a large number of nodes, but requires more complex NOS software than is necessary for P2P networks. Examples of NOS software include Windows Server 2008 R2 and SUSE Linux Enterprise Server.

Home Ethernet Networks

Now that you understand the basic components of a home network, you are probably wondering where to start on installing your home network. In the following sections, we'll discuss the most common types of networks found in the home and how to get the fastest data transfer rates from your home network. We'll also explore the various types of cabling used in wired networks.

Ethernet Home Networks

What type of peer-to-peer network should I install in my home? The vast majority of home networks are Ethernet networks. An **Ethernet network** is so named because it uses the Ethernet protocol as the means (or standard) by which the nodes on the network communicate. The Ethernet protocol was developed by the Institute of

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

BITS AND BYTES — Wake Up Your Computer Remotely

Having your computer on a home network with a shared Internet connection makes it possible to access your computer and its files even when you aren't at home. But if your computer is asleep, you need some way to "wake it up." Otherwise, you can't access it through the Internet. Fortunately for Mac users, there is an application called iNet WOL (Wake on LAN) designed to do this (see Figure 7.8). iNet WOL is compatible with the iPhone, iPod Touch, and iPad. The application allows you to use your portable device to wake up your computer via the Internet. Once your computer is awake, you can then use your remote access software to access it. Think of iNet WOL as an alarm clock for your computer.

Figure 7.8
The application iNet WOL (Wake on LAN) lets you use your iPhone to wake up your computer from a remote location.

Electrical and Electronics Engineers (IEEE). This nonprofit group develops many standard specifications for electronic data transmission that are adopted throughout the world. Each standard the IEEE develops is numbered, with 802.11 (wireless) and 802.3 (wired) being the standards for Ethernet networks. The Ethernet protocol makes Ethernet networks extremely efficient at moving data. Ethernet networks use both wireless and wired transmission media.

What is the current wireless standard for Ethernet networks? The current standard that governs wireless networking for Ethernet networks is the **802.11n standard**, which was ratified in 2009. Establishing standards for networking is important so that devices from different manufacturers will work well together. The 802.11 standard is also known as **WiFi**. Four standards are currently defined under the 802.11 WiFI standard: 802.11a, 802.11b, 802.11g, and 802.11n. Since 802.11n features the fastest data transfer rates, it is now the most desirable choice for home networks. Devices using older standards (such as 802.11g) will still work with 802.11n networks, but they will operate with slower data transfer rates. This accommodation of current devices being able to use previously issued standards in addition to the current standards is known as **backward compatibility**.

How do 802.11n wireless devices work? Wireless routers and network adapters contain transceivers. A **transceiver** is a device that translates the electronic data that needs to be sent along the network into radio waves and then broadcasts these radio waves to other network nodes. Transceivers serve a dual function because they also receive the signals from other network nodes. Devices that use the 802.11n standard achieve higher throughput by using a technology known as Multiple Input Multiple Output (MIMO).

Devices using wireless standards developed prior to the 802.11n standard only utilized one antenna for transmitting and receiving data. Devices that use **Multiple Input Multiple Output (MIMO)** technology are designed to use multiple antennas for transmitting and receiving data. The multiple antennas break the data into multiple data streams and allow for faster transmission of the data. 802.11n devices can achieve throughput of up to 300 Mbps under ideal conditions. But as mentioned previously, many factors can reduce the throughput of a wireless connection.

Throughput Speeds

How can I tell how fast the wireless connection to my network is on my computer? You can install various utilities, such as Net Meter (available at **download.com**), on your computer that will measure your throughput. Net Meter (see Figure 7.9) shows you the throughput you are achieving on your computer's wireless connection to your network over a period of time. Hopefully, you'll achieve throughput in the range of 50 to 200 Mbps on your wireless network, which should be sufficient

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

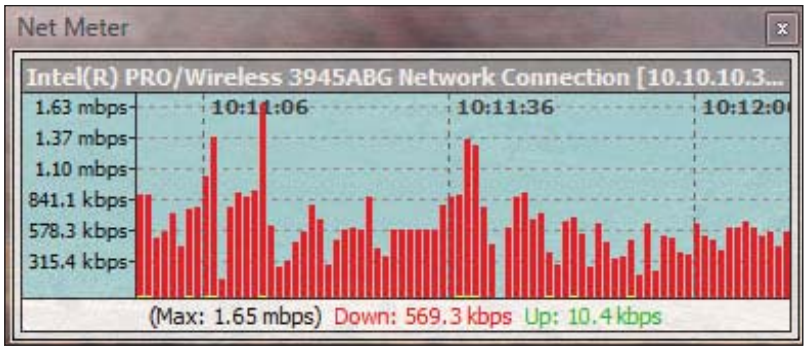


Figure 7.9

Net Meter shows this computer is achieving a rather slow maximum connection of 1.65 mbps on a shared wireless network at a hotel.

for most applications (even watching video). However, if you don't achieve acceptable throughput, you might want to consider a wired Ethernet connection.

What kind of throughput is achievable with wired network connections? Up to one gigabit per second (1,000 Mbps) of throughput is possible using the **gigabit Ethernet** standard, which is the most commonly used wired Ethernet standard deployed in devices designed for home networks. Wired Ethernet networks use cables to transmit data as opposed to the radio waves used on wireless networks. Because cabling is much less susceptible to interference, a wired connection can achieve higher rates of throughput.

Network Cabling

What type of cable do I need to connect to a wired Ethernet network? The most popular transmission media option for wired Ethernet networks is **unshielded twisted-pair (UTP) cable**. UTP cable is composed of four pairs of wires that are twisted around each other to reduce electrical interference. You can buy UTP cable in varying lengths with RJ-45 connectors (Ethernet connectors) already attached. RJ-45 connectors resemble standard phone connectors (called RJ-11 connectors) but are slightly larger and have contacts for eight wires (four pairs) instead of four wires (see Figure 7.10). You must use UTP cable with RJ-45 connectors on an Ethernet network because a phone cable will not work.

Do all wired Ethernet networks use the same kind of UTP cable? Figure 7.11 lists the three main types of UTP cable you would consider using in home-wired Ethernet networks—Cat 5E, Cat 6, and Cat 6a—and their data transfer rates. Although Cat 5E cable is the cheapest and is sufficient for many home networking tasks it was designed for 100 Mpbs wired Ethernet networks that were popular before gigabit Ethernet networks became the popular standard for home networking. Therefore, you should probably not install Cat 5E cable although it is still available in stores. Since **Cat 6 cable** is designed to achieve data transfer rates that support a gigabit Ethernet network, it is probably the best choice for home networking cable. Cat 6a cable is designed for Ultra-Fast Ethernet (10 gigabit Ethernet) networks that run at

BITS AND BYTES

Blazingly Fast Wireless Connections on the Horizon

Although most people want wireless connectivity throughout their home, wired connections still provide the best throughput. But a joint effort between the Wireless Gigabit Alliance and the WiFi Alliance aims to change this. The next generation of wireless standards is called Wi-Gig and will be designed to provide up to 7 Gbps of throughput. This speed will blow away current WiFi standards (with a current theoretical maximum transfer rate of 600 Mbps) and wired gigabit connectivity. Whereas WiFi currently operates in the 5 GHz and 2.4 GHz bands, Wi-Gig will operate in the 60 GHz band, which is currently unlicensed by the FCC. This should prevent many of the interference issues that WiFi users currently experience. But don't start looking in the stores for this equipment just yet; this standard will take several years to develop.

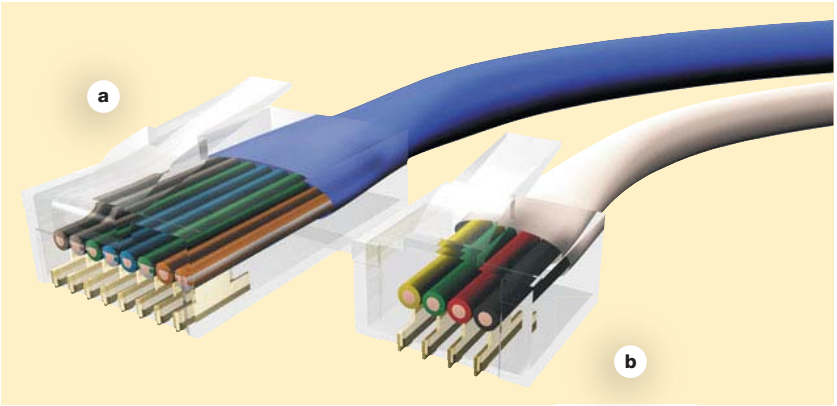


Figure 7.10

(a) An RJ-45 (Ethernet) connector, which is used on UTP cables; and (b) a typical RJ-11 connector, which is used on standard phone cords.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

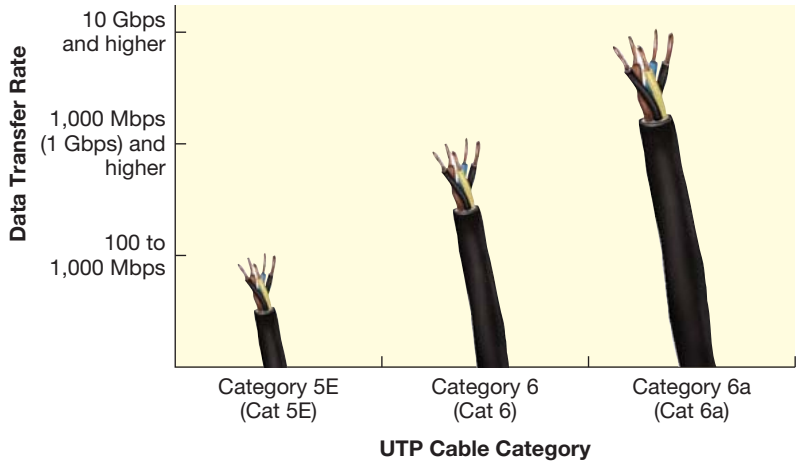


Figure 7.11
Data Transfer Rates for Popular Home Network Cable Types

speeds as fast as 10 Gbps. Installing a 10 gigabit Ethernet network in the home is probably unnecessary because today's home applications don't require this rate of data transfer

What precautions should I taken when running UTP cable? UTP cable is no more difficult to install than normal phone cable but there are a few things to avoid. Do not put sharp bends into the cable when running it around corners because this can damage the copper wires inside and lead to breakage. Also, run the cable around the perimeter of the room (instead of under a rug, for example) to prevent damage to wires from foot traffic.

How long can an Ethernet cable run be? Regardless of the type of Ethernet cable you use, runs for UTP cable can't exceed 100 meters (328 feet) or the signal starts to degrade. Even for short cable runs, you should use continuous lengths of cable. Although two cables can be spliced together with a connecting jack, this creates a point of failure for the cable, because connectors can loosen in the connecting jack and moisture or dust can accumulate on the contacts.

Fortunately, you don't have to choose between a wired or a wireless network. Ethernet networks can handle your wired and wireless needs on the same network. This gives you the best of both worlds (portability and high throughput).

Wired and Wireless on One Network

Can I have wired and wireless nodes on one Ethernet network? Yes, one Ethernet network can support nodes with both wireless and wired connections. Most people will want to connect portable devices (such as notebooks and smartphones) that are constantly being moved around the home wirelessly to their network. However, many of the devices that are connected to a network (such as televisions, DVRs, and Blu-ray players) usually stay in one location. Although these devices probably feature wireless connectivity also, it may be desirable to hook them up to wired connections to take advantage of faster throughput achieved by wired connectivity. Routers sold for home networks facilitate wired and wireless connections. Figure 7.12 shows an example of a network with a wireless/wired router attached.

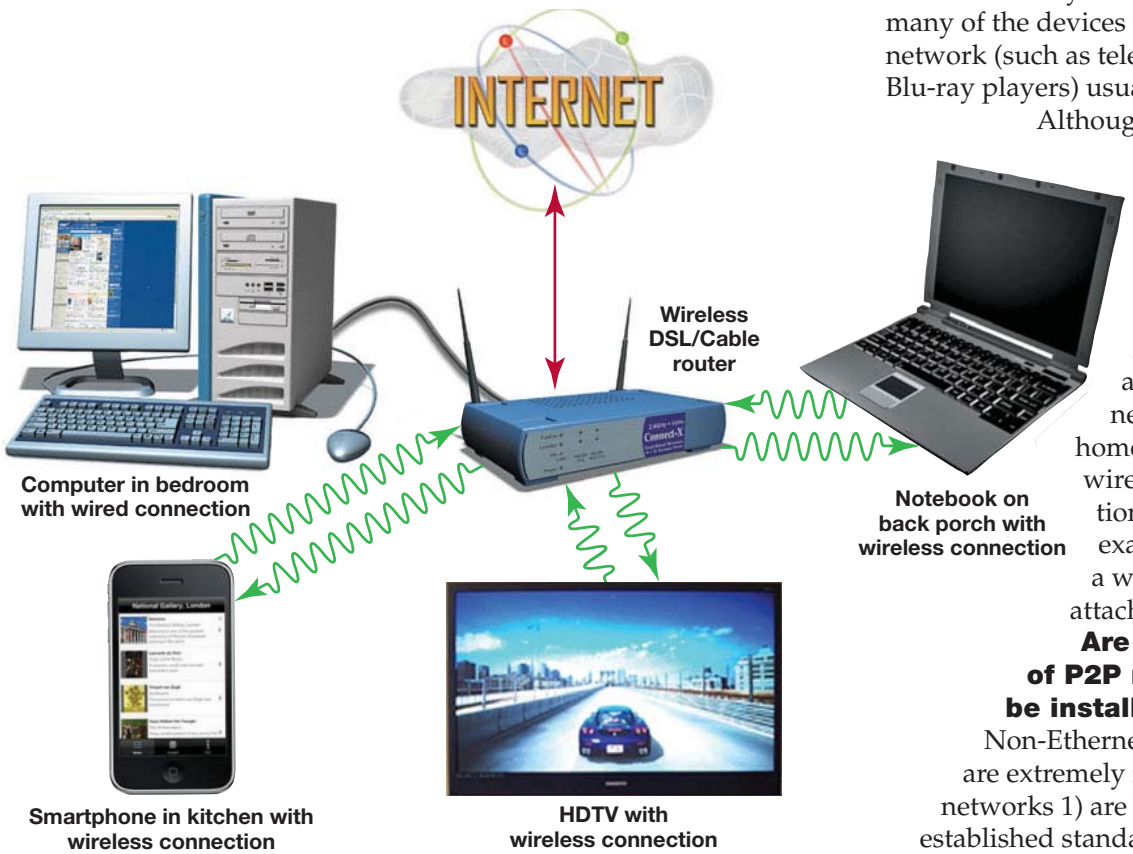


Figure 7.12
Wired and wireless connections in the same home network.

Are there other types of P2P networks that can be installed in the home? Non-Ethernet networks in the home are extremely rare. Because Ethernet networks 1) are based on a well-established standard, 2) feature easy

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

set-up, 3) provide good throughput for home networking needs, and (4) are cost effective, manufacturers of home networking equipment have overwhelmingly embraced Ethernet networks.

Does the type of operating system I'm using affect my choice of a home networking standard? Windows, OS X, and Linux built in P2P networking software will all support connection to an Ethernet network. Therefore, an Ethernet network is appropriate for all computers using these three operating systems.

Home Ethernet Equipment

By now you should have enough information to decide what nodes on your network need be connected wirelessly and which devices would benefit from wired connections. In this section, we'll explore the various types of equipment (such as a router) that you need to obtain to configure your home network. And we'll explore what devices your nodes need to contain to enable them to connect to your network.

Routers and Switches: Moving Data Around Your Network

What equipment do I need for a home Ethernet network? Ethernet networks need network navigation devices to make them work and therefore the first piece of equipment to consider is a router. Recall that routers are designed to transfer packets of data between two (or more) networks—in this case, your home network and the Internet. A router is essential on a home network to allow sharing of an Internet connection. For an Ethernet network to function properly, data must also be transmitted efficiently around the network. A switch is the device that is used on Ethernet networks to route the data between nodes on the same network.

Because both a router and a switch are needed on home Ethernet networks, the manufacturers of home networking equipment make devices that are a combination of routers and switches. In most instances, these devices are called *routers* or *broadband routers*. But despite the name, these devices do include integrated switches. Although manufacturers do make routers with only wired capabilities, for the vast majority of home networks, people buy routers with wireless capabilities.

What do switches do on an Ethernet network? Data is transmitted through the transmission medium of an Ethernet network in packets. Imagine the data packets on an Ethernet network as cars on a road. If there were no traffic signals or rules of the road (such as driving on the right-hand side), we'd see a lot more collisions between vehicles, and people wouldn't get where they were going as readily (or at all). Data packets can also suffer collisions. If data packets collide, the data in them is damaged or lost. In either case, the network doesn't function efficiently. The routers you buy for home networks have a switch integrated into them, so you won't need to buy a standalone switch for your home network.

As shown in Figure 7.13, a switch in an Ethernet network acts like a traffic signal (or a traffic cop) by enforcing the rules of the

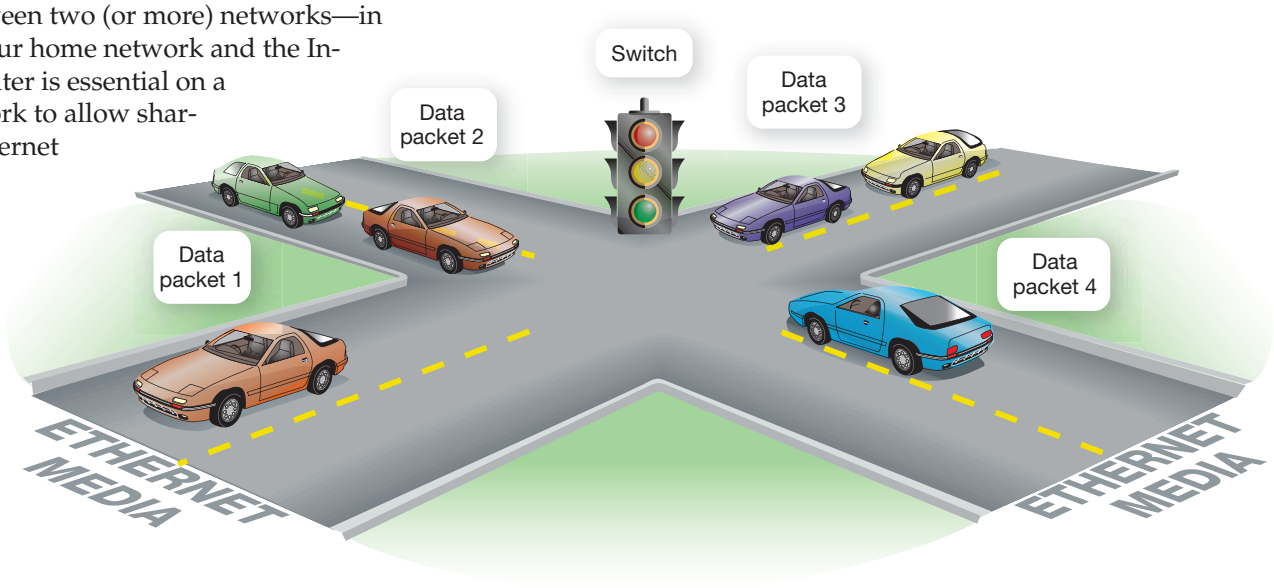


Figure 7.13
A simplified explanation is that switches (working in conjunction with NICs) act like traffic signals or traffic cops. They enforce the rules of the data road on an Ethernet network and help prevent data packets from crashing into each other.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

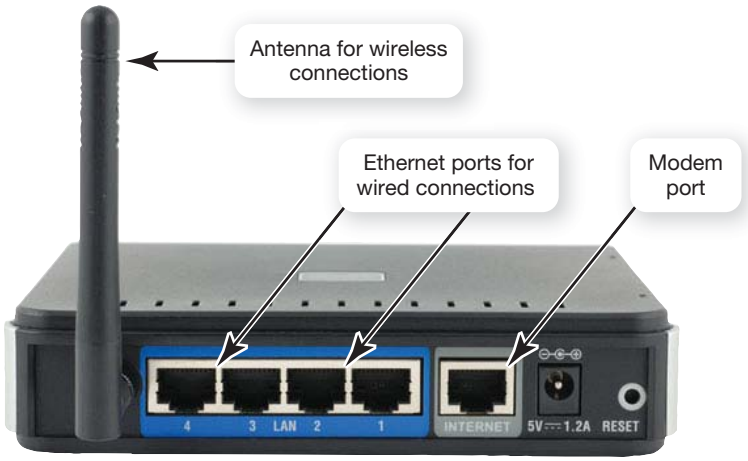


Figure 7.14
Rear view of typical wireless/wired router.

data road on the transmission media. The switch keeps track of the data packets and, in conjunction with network interface cards, helps the data packets find their destinations without running into each other. The switch also keeps track of all the nodes on the network and sends the data packets directly to the node for which they are headed. This keeps the network running efficiently.

In the next section, we'll explore connecting your computing devices to your router.

Connecting Devices to Routers

How many computers and other devices can be connected to a router in a home network? Most home wireless routers can support up to 253 wireless connections at the same time. This number is a theoretical maximum, however—most home networks probably have fewer than ten wireless devices connected to the network. But regardless of how few or how many devices your home network has, those wireless devices share bandwidth when they are connected to a router. Therefore, the more devices actively transmitting data that you connect to a single router, the smaller the portion of the router's bandwidth each device receives.

To look at this another way, consider you have a pizza which represents your router's bandwidth. You can cut the pizza into six or eight pieces (that is, you can connect either six or eight devices to the network). If you cut the pizza into eight pieces, each person who gets a slice receives a smaller portion of pizza than they would if you had cut the pizza into six pieces. (that is, when you connect eight devices to the network, each device has less bandwidth than it would have if only six devices were connected to the network).

Does my wireless router support wired connections? Most home wireless routers have three or four Ethernet ports on the back of the router to support wired connections via twisted-pair cable (see Figure 7.14). If you have a lot of devices (such as a game console, HDTV, and a notebook) in your home that may be used simultaneously, you might want to consider connecting some of them via a wired connection to increase allocated bandwidth to each wireless device. This will help increase the throughput to each wireless device.

If you find that you need additional ports for plugging in wireless connections to your network, you can buy a standalone switch and plug that into one of the ports on your router. This will give you additional ports for making wired connections to your network. Do not mistakenly buy another router (with an embedded switch) and try adding that to your network because the two routers will cause conflicts as they fight for control over network navigation.

Where do I obtain a router for my home network? You can purchase a router at any store (such as Best Buy) or online stores (**tigerdirect.com**, **newegg.com**) that carry home networking equipment. Also, since networks are so common in homes now, many ISPs offer home subscribers a device that combines a broadband modem and a wireless router. ISPs typically charge either a one-time or a monthly fee for this combination device. If you already have broadband access in your home, you at least have a modem. Check with your ISP if you are not sure whether you also already have a device that contains a router.

How do I know if my router supports wireless networking? If you do have a router provided by your ISP, make sure to ask what wireless networking standard the router supports. If it does not support 802.11n but supports and older standard such as 802.11g, you should consider having your ISP provide you with a new router. You want to have a router that supports the fastest wireless networking standard (802.11n) so that you can achieve the highest possible throughput on your wireless nodes. If all of your wireless devices have 802.11n network adapters, but your router supports 802.11g, you will not

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

achieve the best throughput available to you because 802.11g devices feature much slower transfer rates than 802.11n devices (about four to six times slower).

Where do I place the router on my network? Your router should be connected directly to your broadband modem (see Figure 7.15). The connection is usually an Ethernet cable (Cat 6 cable) running from an Ethernet port on your modem to the modem port on your router.

Are wireless routers for Windows and OS X networks different? All routers that support the 802.11n standard should work with computers running Windows or OS X. However, Apple has designed routers that are optimized for working with Apple computers. So if you are connecting Apple computers to your network, you may wish to consider using an Apple AirPort router. (Windows machines can also connect to the AirPort routers.) The Apple AirPort Extreme (Figure 7.16) is a good choice for a home network. It supports up to 50 simultaneous wireless connections and has three gigabit Ethernet ports for wired connections.

How do I set up my router so that I can use it to connect to the Internet? First, contact your ISP and find out about any special settings that you may need to configure your router to work with your ISP. Next, access your router from Internet Explorer (or another Web browser) by entering the router's IP address or default URL. You can usually find this information in the documentation that came with the router. You'll also need a username and password to log on to the router. You'll probably find these, too, in the documentation that came with the router.

Many routers feature their own wizard (different from the Windows Networking wizards) that takes you through special configuration screens. A sample screen from a router is shown in Figure 7.17. The documentation that came with your router will provide a URL to use to log on to the router. If you're unsure of any information that needs to be entered to configure the router (such as whether IP addresses are assigned dynamically—meaning you are assigned a new IP address by your ISP each time you connect to the Internet), contact your ISP and ask for guidance.

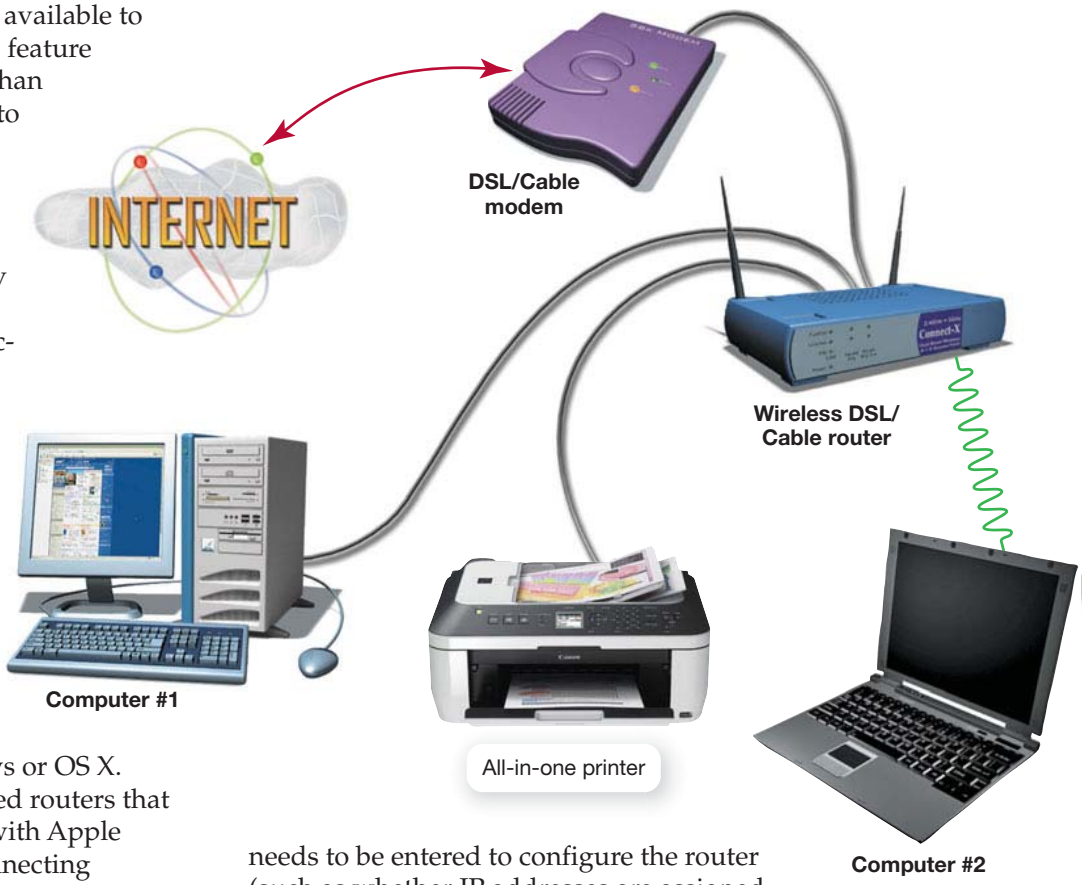


Figure 7.15
A small network with a wireless router attached.

After ensuring that your router is set up properly, you are ready to begin connecting your computing devices to your network. You now need to ensure that all your nodes have the proper equipment to enable them to connect to your network.

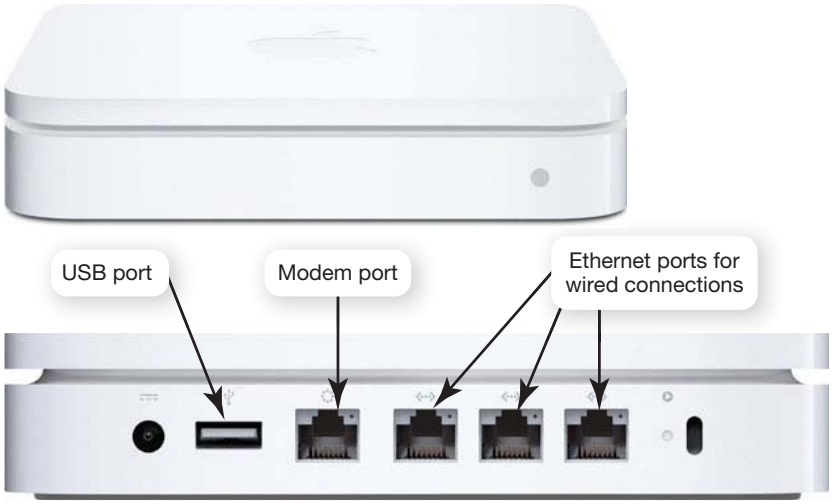


Figure 7.16
The AirPort Extreme router is often used for home networks with Apple computers.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Figure 7.17

Although setups differ from router to router, you will need basic information such as the logon information and the type of IP addressing to configure the router to work with your network and your ISP.

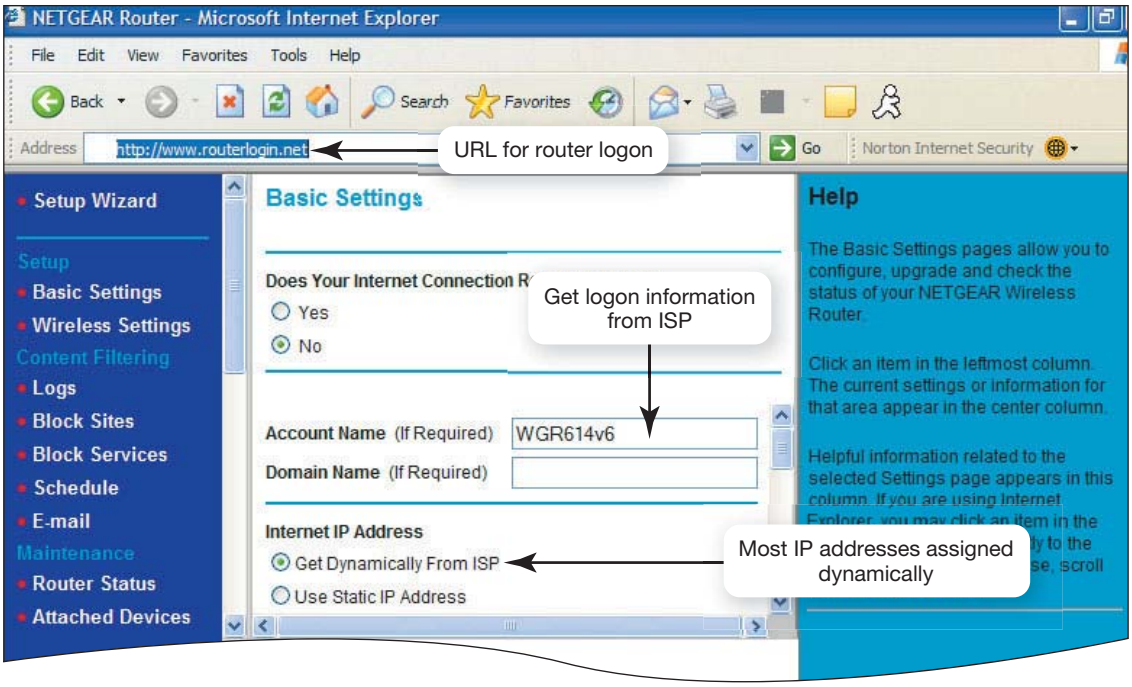


Figure 7.18

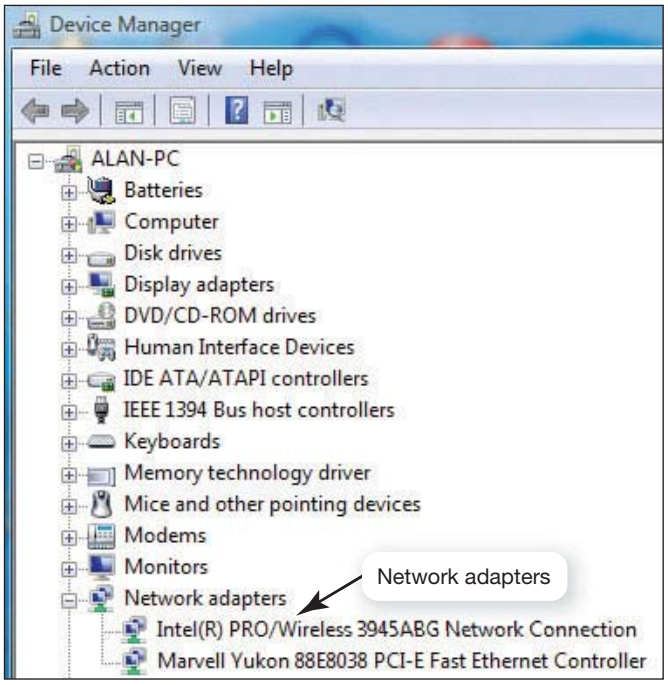
This Windows device manager shows a wireless and a wired network adapter installed in a notebook.

>To access Device Manager: Click the **Start Button**, select **Control Panel**, click on the **Hardware and Sound Group**, then click on **Device Manager**.

Connecting Network Nodes

What equipment do my computers need to communicate with wireless media on an 802.11n wireless network? Your computers need to have wireless network interface cards (NICs) installed in them. Notebooks and netbooks sold over the last several years most likely contain 802.11n NICs. For older computers, as long as they have wireless Ethernet adapters that are compatible with a previous standard (802.11g or 802.11b) they will be able to connect to your 802.11n router. However, the throughput will be at the lower 802.11g and b data transfer rates.

How can I tell what network adapters are installed in my computer? To see which network adapter(s) are installed in your Windows computer and to check whether the adapter is working, you should use the Device Manager utility program (see Figure 7.18). The installed adapters will be shown and then you search for information on the Internet to determine the adapter's capability if you aren't sure which wireless standard it supports.



Connecting Other Devices to Networks

Because sharing peripherals is a major benefit of installing a network, many peripheral devices, such as scanners and printers, now come with built-in Ethernet adapters. Also, many home entertainment devices (such as televisions, Blu-ray players, and gaming systems), portable devices (such as smartphones, and iPod Touches and iPads), and power monitoring devices to reduce energy consumption in the home are also designed to attach to home networks. Such devices are usually described as being "network-ready."

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

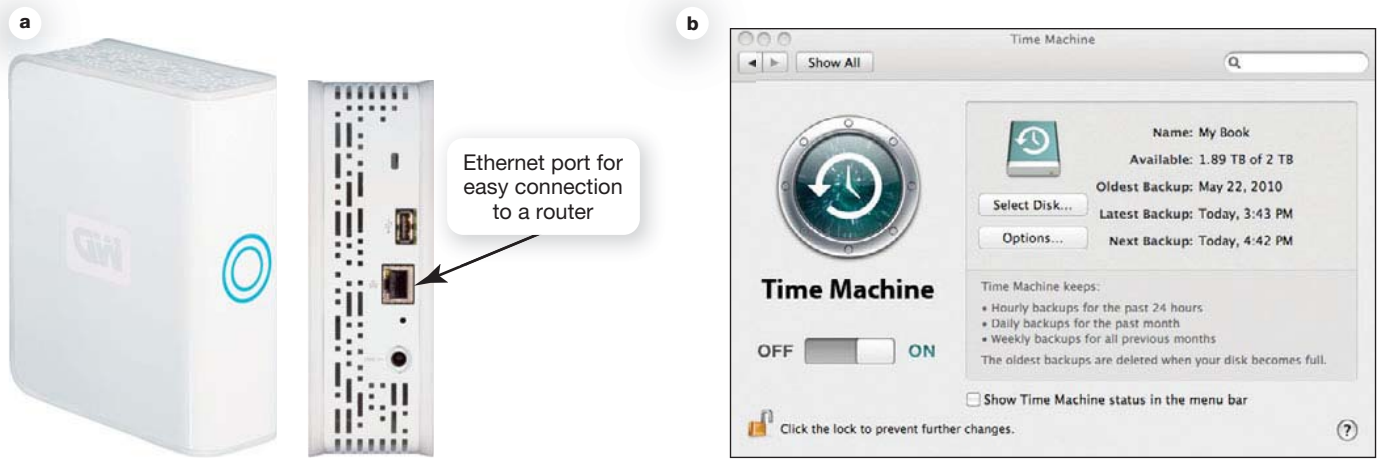


Figure 7.19

(a) The My Book drives from Western Digital feature NAS devices that can store 2 TB of data in a device the size of a small book. (b) Time Machine in conjunction with an external hard drive provides easy backups of Macs on a network.

Network-Ready Devices

What is a network-ready device? A **network-ready device** (or Internet ready) can be connected directly to a router instead of to a computer on the network. Network-ready devices usually contain wireless and/or wired network adapters inside them. A few devices (such as TiVo or the Xbox 360) still have external network adapters that connect to the device via a USB port but these eventually should be phased out in favor of internal adapters. The eventual goal may be to have all electronic devices in your home be nodes on your network.

Why should I connect my peripherals to my home network? There is an advantage to connecting peripherals wirelessly to your network. If a printer were connected directly to another computer (via a cable) on the network instead of being a node on the network, that computer would need to be switched on so other computers could access the printer. With a network-ready printer, only the printer needs to be powered on for any computer on the network to print to it.

What can I attach to my network to facilitate file sharing and back up of data? **Network attached storage (NAS) devices** are specialized computing devices designed to store and manage your data. People are generating tremendous quantities of data today with digital cameras and camcorders, as well as buying music files, and these files need to be stored and shared. Although data can always be stored on individual hard drives in computers on a network, NAS devices provide for centralized data storage and access.

Popular for years on business networks, NAS devices are now being widely marketed for home networks. You can think of them as specialized external hard drives. NAS devices, like the My Book series from Western Digital (see Figure 7.19a), connect directly to the network through a router or switch. Specialized software can then be installed on computers attached to the network to ensure that all data saved to an individual computer is also stored on the NAS as a backup. We'll discuss backing up your data in more detail in Chapter 9.

For Apple computers, the Time Capsule is a wireless router combined with a hard drive for facilitating backups of all computers connected to the network. The Time Capsule looks very similar to the AirPort router and it works in conjunction with the Time Machine backup feature of OS X (see Figure 7.19b). If you buy a Time Capsule, you won't need to buy an AirPort router (or other router) as the Time Capsule fulfills this function on your network also. When the Time Capsule is installed on your network, Macs connected to the network will ask the user if they want to use the Time Capsule as their source for Time Machine backups. The Time Capsule is another type of NAS device.

Besides external hard drives, are their other NAS devices I could use on my network? A more sophisticated type of NAS device is a home network server. Home network servers are specialized devices that are designed to provide a specific set of services to computers on a home network. Home servers do not convert a home peer-to-peer network into a client/server network because these servers only perform only a limited set of functions

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

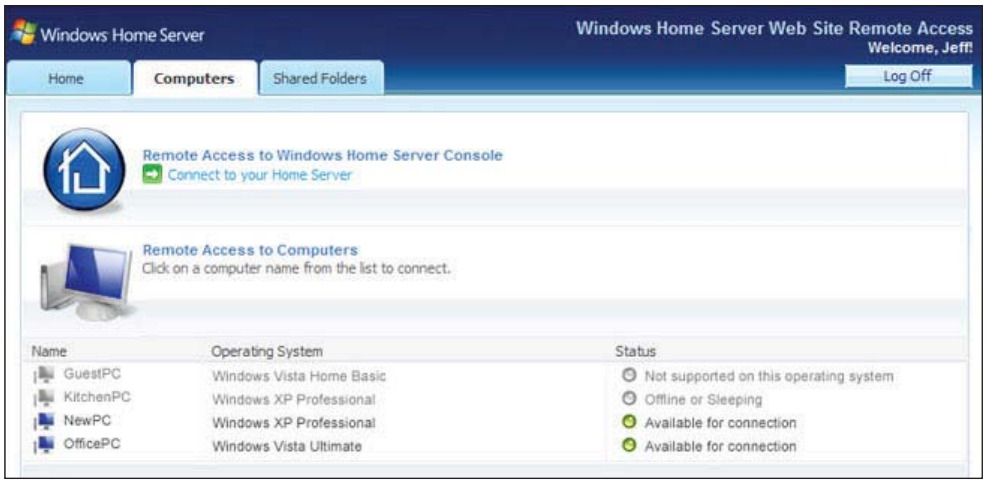


Figure 7.20
Windows Home Server remote access interface.

instead of all the functions performed on client/server networks.

Home network servers, like the Acer Aspire easyStore server (shown earlier in Figure 7.5), are often configured with Windows Home Server and connect directly as a node on your network. Home servers have the functionality of NAS devices and often handle the following tasks:

- Automatically back up all computers connected to the network.
- Act as a repository for files to be shared across the network (such as music and video files).
- Function as an access gateway to allow any computer on the network to be accessed from a remote location via the Internet (see Figure 7.20).

And you can access the media stored on your Windows Home Server through your Xbox 360 as long as the Xbox is also connected to your home network.

Figure 7.21
Searching for the right remote? New software apps make it easy to just use your phone instead.

Digital Entertainment Devices on a Network

Why should I connect my digital entertainment devices to my network? The main reason is to access and share digital content. When you attach devices to the Internet, you can purchase (or even obtain for free) more content for you to enjoy such as movies, videos, or music files. You can also use gaming devices to play multiplayer games with players all over the world. The content you access is either downloaded or streamed to your entertainment devices. Viewing Netflix movies delivered over the Internet on your computer is an example of streaming media.

When media is *streamed*, it is sent directly to a device (such as a computer or HDTV) without being saved to a hard drive. This requires a lot of bandwidth so a broadband connection is required to effectively view streaming media. Media can also be *downloaded* (saved) to a hard drive for viewing at a later time. Although the Amazon Video on Demand service now offers streaming movies, they still offer the ability to download content to your computer or your TiVo so you can view it later.

What types of digital entertainment devices can I use to view streaming or downloaded media? Network-ready televisions and home theater systems allow for direct connection to your home network (wireless or wired). These devices are configured to receive streaming media directly from the Internet. Waiting for a DVD to come in the mail from Netflix is so passé when you can have it available immediately on your television through your home network!

However, many people prefer to own media and buy it on permanent formats such as Blu-ray discs. Blu-ray disc players, such as the Sony 3D Blu-ray disc players offer not only high-definition resolution but also the capability to display 3D video. These Blu-ray players feature integrated wireless connectivity for connection to your network as well as the ability to receive

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

streaming media from various Internet providers. You can even view videos from YouTube and listen to Pandora Internet Radio right through your Blu-ray player.

In terms of controlling your devices such as televisions and Blu-ray players, more companies are developing applications that enable your handheld devices (such as PSPs or iPhones) to act as remote controls. The BD Remote app by Sonoran Blue (see Figure 7.21) for the iPhone allows you to control Sony Blu-ray players.

Digital video recorders (DVRs), like the TiVo Premiere, are often used in the home to record high-definition television programs. Connecting your TiVo to your network makes it possible to receive downloads of movies directly to your TiVo from services such as Amazon Video on Demand. And some home network servers, like the Hewlett Packard MediaSmart servers, now work in conjunction with TiVo devices to provide additional storage for your TiVo devices. The TiVo Desktop software (see Figure 7.22), which you download from **tivo.com**, allows you to transfer shows recorded on your TiVo to your computer or to portable devices such as an iPod, iPhone, BlackBerry, or PSP.

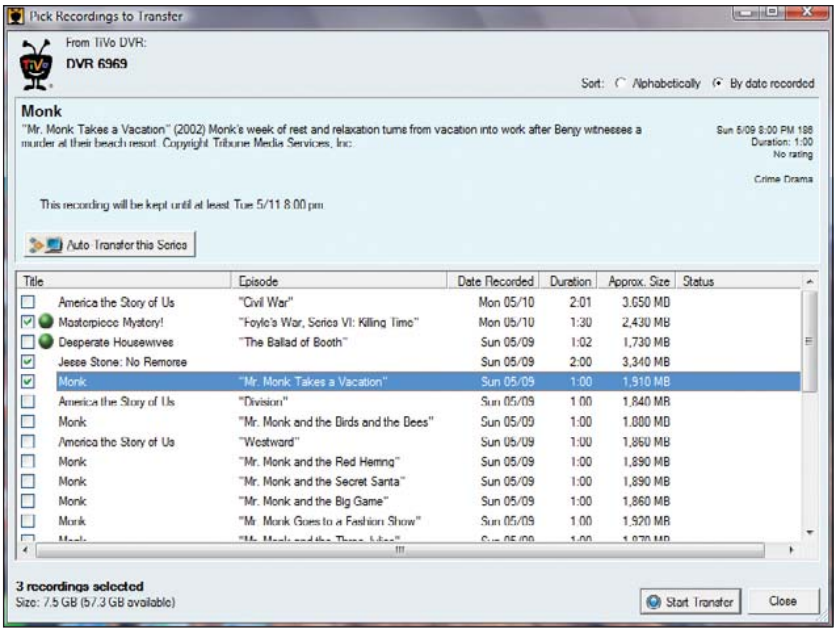


Figure 7.22
The TiVo Desktop software facilitates transfer of recorded shows to portable devices so you can enjoy your content on the go.

Can I connect my gaming consoles to my home network? Current gaming systems, like the PlayStation 3, offer much more than just games as they can function as a total entertainment platform when connected to your network (and therefore to the Internet). The PlayStation 3 (PS3) has a built-in Blu-ray drive and can play Blu-ray discs as well as DVDs and music files. You can download movies, games, and videos directly to the PlayStation. It can also be used to share media across your network and import photos or video from cameras and camcorders. And if you have a PSP, you can use an application called Remote Play (see Figure 7.23) to access features of your PlayStation from your PSP. You can use the PSP to turn your PlayStation on and off, access music and video files, access photos stored on your PlayStation, play games, and browse the Internet. Media is transmitted from your PlayStation and displayed on the PSP screen.

Figure 7.23
The Remote Play feature of the PSP and the PlayStation 3 (PS3) allows users to access PS3 features, like the PlayStation Store, directly from their PSP.

Specialized Home Networking Devices

What if I don't need the full functionality of a PC, but I still want to access Internet content? The launch of the Apple iPad signaled a resurgence of Internet appliances. The main function of an **Internet appliance** is easy access to the Internet, social networking sites, e-mail, video,

ACTIVE HELPDESK Understanding Networking

In this Active Helpdesk call, you'll play the role of a helpdesk staffer, fielding calls about home networks—their advantages, their main components, and the most common types—as well as about wireless networks and how they are created.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Figure 7.24

Quick access to information and entertainment is the key feature of Internet appliances.

news, and entertainment. These devices fall into a category somewhere between smartphones and full-blown computers. They are light on calculation, but high on easy content delivery. Devices such as the Sony Dash Personal Internet viewer (see Figure 7.24) are popular in kitchens and bedside tables where access to Internet radio stations, short videos, and quick information updates (like Facebook updates and current weather conditions) are needed. Originally, Internet appliances were marketed toward older computer users since these devices feature easy operation and a shallow learning curve. But the Apple iPad is propelling this category of devices into the hands of much younger users. We discuss the Apple iPad in more detail in Chapter 8.

Figure 7.25

Sending pictures directly to an electronic frame from your phone is possible when the frame is connected to your network.

How can I use my home network to enhance photo sharing? Digital picture frames that display an array of changing digital photos have become quite popular with the rise in digital photography. Now digital picture frames such as the eStarling TouchConnect (see Figure 7.25) come with built-in wireless adapters for easy connection to home networks. Featuring a touch screen interface, this frame can access photos stored on your network or on an online photo-sharing site and display them. You can set up an e-mail address for the picture frame so that friends and family can e-mail pictures directly to the frame as soon as they are taken. Wouldn't it be nice to come home to new photos of your friend's trip to Cancun tonight?

How can I use my home network to enhance my home security? Monitoring cameras, both for indoor and outdoor use, are now available for the home and feature wireless connectivity. The cameras can connect to your network and be monitored by software like the Logitech Digital Video Security System (Figure 7.26). Security monitoring software allows you to view real-time images from the cameras at your home. The software can be configured to alert you via e-mail or text message when the cameras detect movement. Some systems also allow you to receive alerts when there is a lack of movement. This can be useful for monitoring an aging relative (who may need help if they stop moving) or for monitoring the arrival of children coming home from school at a certain time.

Figure 7.26

Logitech security products can help you remotely monitor your home's security.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

As time goes on, many more types of entertainment devices and home gadgets will eventually be connected to your home network.

Securing Wireless Networks

All computers that connect to the Internet (whether or not they are on a network) need to be secured from intruders. This is usually accomplished by using a **firewall**, which is a hardware or software solution that helps shield your network from prying eyes. We discuss firewalls at length in Chapter 9. Wireless networks present special vulnerabilities; therefore, you should take additional specific steps to keep your wireless network safe. It is important to configure your network security before setting up and connecting all the nodes on your network.

Why is a wireless network more vulnerable than a wired network? With a wired network, it is fairly easy to tell if a **hacker** (someone who breaks into computer systems to create mischief or steal valuable information) is using your network. However, wireless 802.11n networks have wide ranges that may extend outside of your house. This makes it possible for a hacker to access your network without your knowledge.

Why should I be worried about someone logging onto my wireless network without my permission? Some use of other people's wireless networks is unintentional. Houses are built close together. Apartments are clustered even closer together. Wireless signals can easily reach a neighbor's residence. Most wireless network adapters are set up to access the strongest wireless network signal detected. If your router is on the east side of your house and you and your notebook are on the west side, then you may get a stronger signal from your neighbor's wireless network than from your own. **Piggybacking** is connecting to a wireless network (other than your own) without the permission of the owner. This practice is illegal in many jurisdictions but often happens inadvertently between neighbors.

Your neighbor probably isn't a hacker, but he might be using a lot of bandwidth—your bandwidth! If he's downloading a massive movie file while you're trying to do research for a term paper, he's probably slowing you down. In addition, when some less-than-honest neighbors discover they can log onto your wireless network, they may cancel their own Internet service to save money by using yours. Some neighbors might even be computer savvy enough to penetrate your unprotected wireless network and steal personal information, just as any other hackers would.

In addition, because computer criminal activities are traceable, hackers love to work their mischief from public computers (such as those in a library or college) so they can't be identified. If a hacker is sitting in her car outside your house and logging on to your wireless network, any cyberattacks she launches might be traced back to your IP address, and you might find law enforcement officials knocking on your door.

How is my wireless network vulnerable? Packets of information on a wireless network are broadcast through the airwaves. Savvy hackers can intercept and decode information from your transmissions that may allow them to bypass any standard protections, such as a firewall, which you have set up on your network. Therefore, to

BITS AND BYTES

Wireless Hot Spots: How to Find One on the Go

Wireless hot spots are places where you can connect to the Internet via a computing device with wireless networking capability (such as your notebook computer). Providers of wireless hot spots may provide free access, or they may charge a fee, which is usually based on connection time (such as a set fee per hour of access). So aside from randomly cruising around searching for a place to connect, how do you find out where the hot spots are? Directories have popped up on the Internet to help you locate hot spots in the areas in which you'll be traveling. Check out JiWire (**jiwire.com**), WiFi FreeSpot (**wififreespot.com**), and WiFi Hotspot List (**wi-fihotspotlist.com**) to locate a hot spot near you.

SOUND BYTE

Securing Wireless Networks

In this Sound Byte, you'll learn what "war drivers" are and why they could potentially be a threat to your wireless network. You'll also learn some simple steps to secure your wireless network against intruders.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

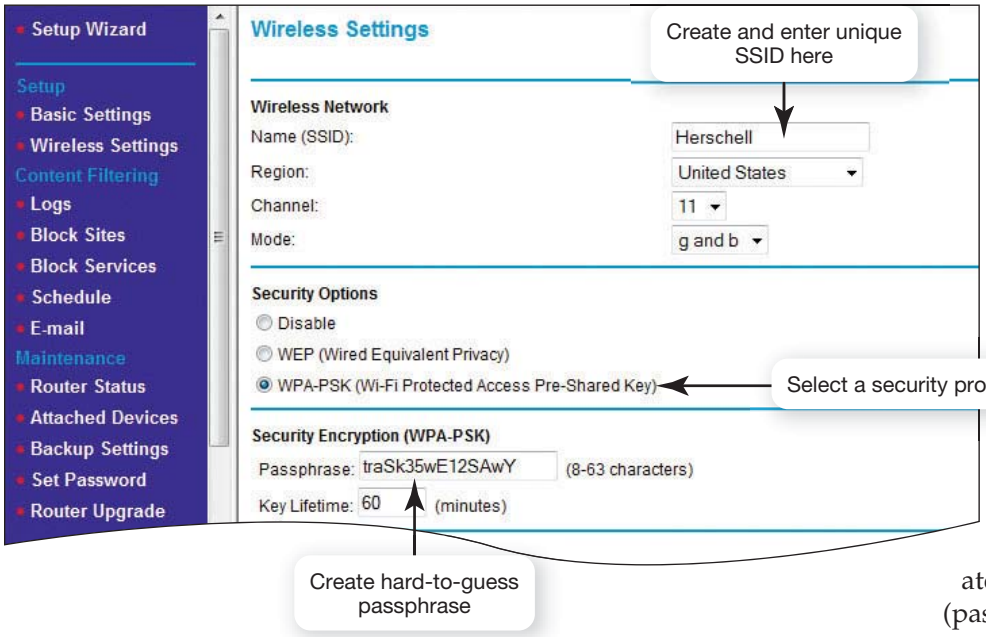


Figure 7.27

By running your router configuration wizard, you can configure the security protocols available on your router and change the SSID, which helps protect your wireless network.

secure a wireless network, you should take the additional precautions described in the Sound Byte "Securing Wireless Networks" and as summarized below:

1. **Change your network name (SSID).** Each wireless network has its own name to identify it, which is known as the **service set identifier** or **SSID**. Unless you change this name when you set up your router, the router uses a default network name that all routers from that manufacturer use (such as "Wireless" or "Netgear"). Hackers know the default names and access codes for routers. If you haven't changed the SSID, it's advertising the fact that you probably haven't changed any of the other default settings for your router, either.
2. **Disable SSID broadcast.** Most routers are set up to broadcast their SSIDs so that other wireless devices can find them. If your router supports disabling SSID broadcasting, turn it off. This makes it more difficult for a hacker to detect your network and nearly impossible for a neighbor to inadvertently connect to your network.
3. **Change the default password on your router.** Hackers know the default passwords of most routers, and if they can access your router, they can probably break into your network. Change the password on your router to something hard to guess. (Use at least eight characters that are a combination of letters, symbols, and numbers.)
4. **Turn on security protocols.** Most routers ship with security protocols such as Wired Equivalent Privacy (WEP) or WiFi Protected Access (WPA). Both use encryption (a method of translating your data into code) to protect data in your wireless transmissions. WPA is a much stronger protocol than WEP, so enable WPA if you have it; enable WEP if you don't. When you enable these protocols, you are forced to create a security encryption key (passphrase). When you attempt to connect a node to a security-enabled network for the first time, you'll be required to enter the encryption key. The encryption key or passphrase (see Figure 7.27) is the code that computers on your network need to decrypt (decode) data transmissions. Without this key, it is extremely difficult, if not impossible, to decrypt the data transmissions from your network. This prevents unauthorized access to your network because hackers won't know the correct key to use. The Windows 7 Connect to a network dialog box shows all wireless networks within range (see Figure 7.28a). Clicking on one allows you to connect to it, or prompts you for more information such as the SSID name and security key (see Figure 7.28b).
5. **Implement media access control.** Each network adapter on your network has a unique number (like a serial number) assigned to it by the manufacturer. This is called a **media access control (MAC) address**, and it is a number printed right on the network adapter. Many routers allow you to restrict access to the network to only certain MAC addresses. This helps ensure that only authorized devices can connect to your network.
6. **Limit your signal range.** Many routers allow you to adjust the transmitting power to low, medium, or high. Cutting down the power to low or medium could prevent your signal from reaching too far away from your home,

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

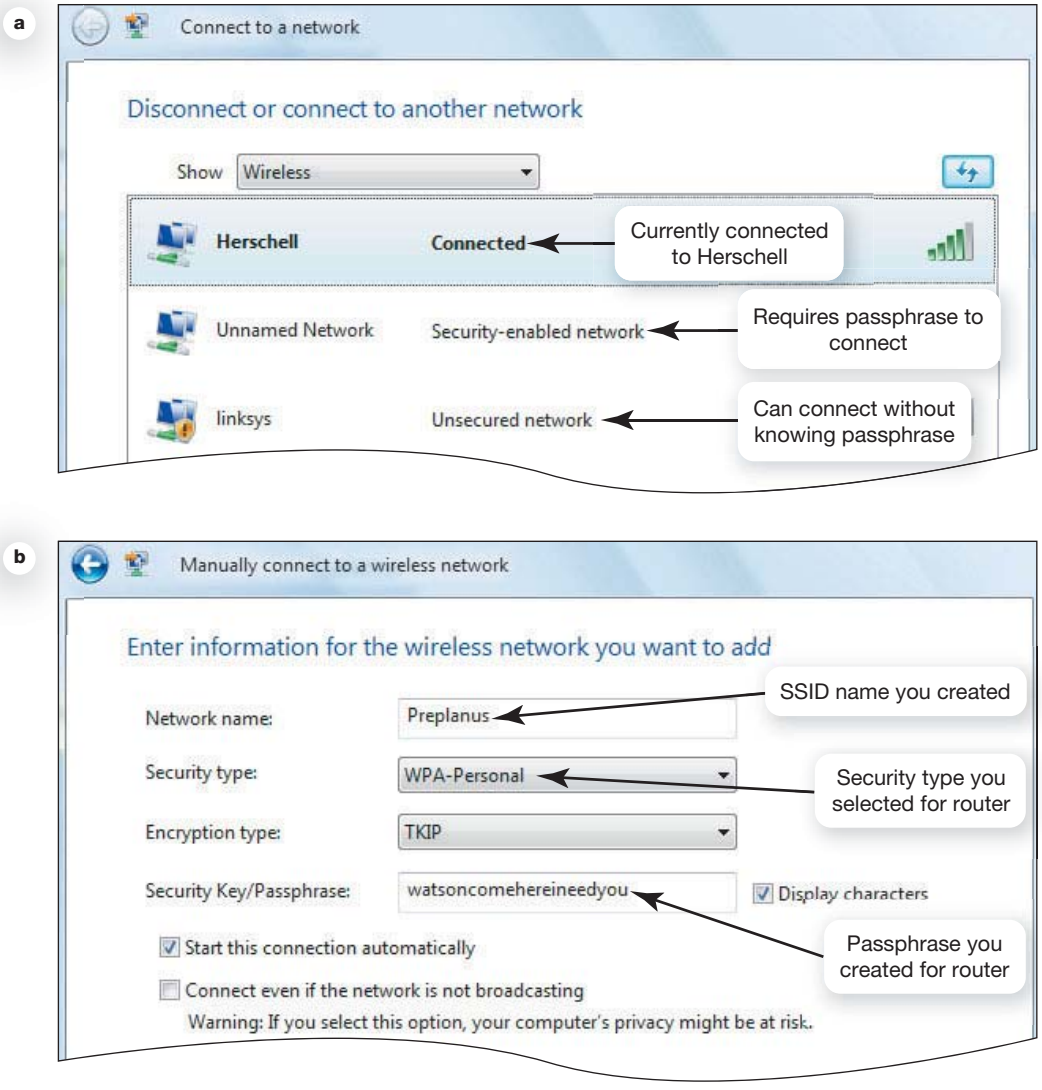


Figure 7.28

(a) The Windows 7 Connect to a network dialog box. (b) Manually connecting to a wireless network allows you to establish a connection if you know the network encryption key and the SSID name.

>You can access the **Connect to a network** dialog box by right-clicking the **Network Connection** icon on the taskbar and selecting **Connect to a network** from the shortcut menu. You can access the **Manually connect to a wireless network** dialog box by accessing the **Control Panel**, clicking on **Network and Internet**, selecting **Network and Sharing Center**, choosing the **Set up a new connection or network** option, and then clicking on **Manually connect to a wireless network**.

making it tougher for interlopers to poach your signal.

7. **Apply firmware upgrades.** Your router has read-only memory that has software written to it. This software is known as **firmware**. As bugs are found in the firmware (which hackers might exploit), manufacturers issue patches, just as the makers of operating system software do. Periodically check the manufacturer's Web site and apply any necessary upgrades to your firmware.

If you follow these steps, you will greatly improve the security of your wireless network. In Chapter 9, we'll explore many other ways to keep your computer safe from malicious individuals on the Internet and ensure that your digital information is secure.

Configuring Software for Your Home Network

Once you install the hardware for your network, you need to configure your operating system software for networking on your computers. In this section, you'll learn how to do just that using special Windows tools. Although configuration is different with Mac OS X, the setup is quick and easy. Linux is the most complex operating system to configure for a home network, though the difficulties are not insurmountable.

Windows Configuration

Is configuring software difficult? Windows makes configuring software relatively simple if you are using the same version of Windows on all of your

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

computers. The Windows examples in this section assume you are using Windows 7 on all of your computers. If you are using previous versions of Windows, there is plenty of information on the Internet regarding the connection of previous versions of Windows to a Windows 7 network. In Windows 7, the process of setting up a network is fairly automated by various software wizards. As you learned in Chapter 4, a wizard is a utility program included with software that you can use to help you accomplish a specific task. You can launch the Windows wizards from the Network and Sharing Center, which can be accessed via the Network and Internet group in the Control Panel. Before running any wizards, you should do the following:

> **"The HomeGroup feature in Windows 7 facilitates file and peripheral sharing."**

1. Make sure there are network adapters on each node.
2. For any wired connections, plug all the cables into the router, nodes, and so on.
3. Make sure your broadband modem is connected to your router and that the modem is connected to the Internet.
4. Turn on your equipment in the following order (allowing the modem and the router about one minute each to power up and configure):
   a. your broadband modem,
   b. your router, and
   c. all computers and peripherals (printers, scanners, and so on).

Other devices, such a televisions, Blu-ray players and gaming consoles can be added to the network after configuring the computers.

By completing these steps, you enable the wizards to make decisions about how best to configure your network. After you have completed these steps, open the Network and Sharing Center from the Control Panel (see Figure 7.29a). You can see the network to which you are currently connected on this screen. On the lower portion of the Network and Sharing Center screen, you can set sharing options for your network. Ensure that network discovery is shown as "on," because this allows your computer to locate other computers and peripherals on the network. You should also verify that the options for file and printer sharing and public folder sharing are shown as "on" to enable file and printer sharing with other computers. From the Network and Sharing Center, select the option to Set up a new connection or network to access the Windows networking wizards (see Figure 7.29b).

Select the Connect to the Internet wizard to configure your network to use your broadband modem to connect to the Internet for the first time. This wizard also configures your wired connections on your network (if any). On the information screen (see Figure 7.29c), enter the access information provided by your ISP. Enter a memorable name for your network and check the box to allow other people to use the Internet connection you are establishing. This will allow all users on the network to use the same connection.

After running this wizard, run the Set Up a Wireless Router wizard to configure your wireless connectivity. If you set up a secured wireless network (as detailed in the previous section), use the Manually Connect to a Wireless Network wizard to connect computers to the secure wireless network.

What if I don't have the same version of Windows on all my computers? Computers with various versions of Windows can coexist on the same network. Always set up the computers running the newest version of Windows first (Windows 7). Then consult the Microsoft web site for guidance on how to proceed for configuring computers with previous versions of Windows on a Windows 7 network.

How do I differentiate the computers on my network? When you set up your Windows computer, you gave it a name. Each computer on a network needs a name that is different from the names of all other computers on the network so that the network can identify it. This unique name ensures that the network knows which computer is requesting services and data and can deliver data to the correct computer.

For ease of file and peripheral sharing, Windows 7 created a feature known as HomeGroup. If you have all Windows 7 computers on your network, you simply all join the same HomeGroup. When you set up your first Windows 7 computer on your network, you can set a password for the HomeGroup.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

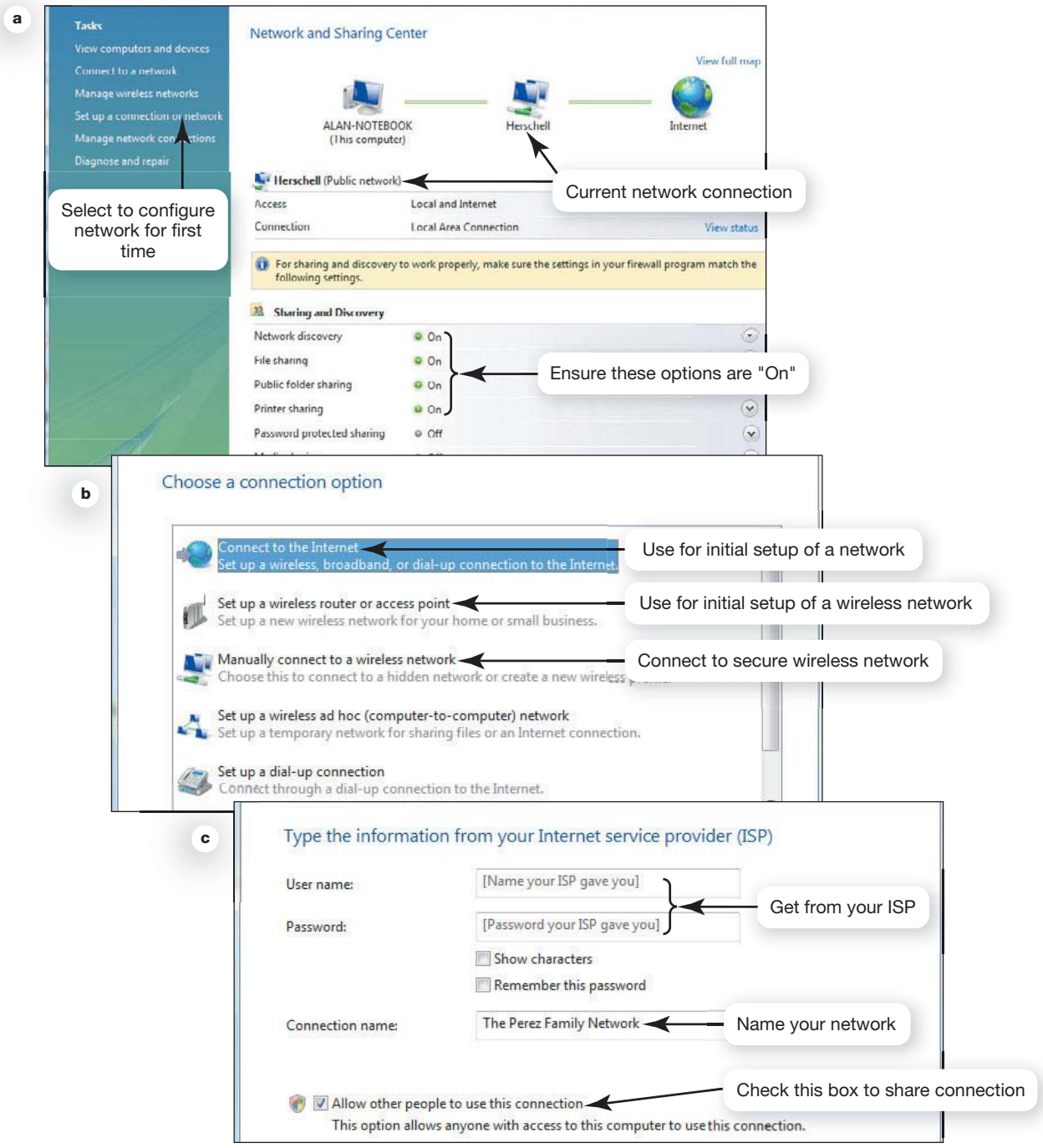


Figure 7.29

(a) The Windows Network and Sharing Center helps you configure your home network. Selecting the appropriate sharing options allow others to share resources on your computer. (b) Selecting the appropriate option provides access to wizards that will assist you. (c) Fill in the information provided by your ISP. The wizard will then set up your connection and connect your computer to the Internet.

>The Windows Network and Sharing Center is found in the Control Panel.

All other computers that subsequently are added to the network will need the password to join the HomeGroup. When you configure a HomeGroup, you have the option of deciding what files and peripherals on your computer will be shared with other computers on the network (see Figure 7.30).

How do Macs connect wirelessly to networks? Generally, connecting Macs to a wireless network is a much easier process than connecting with Windows computers. You set up the security for a router on a Mac network just as was illustrated in the previous section on securing

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

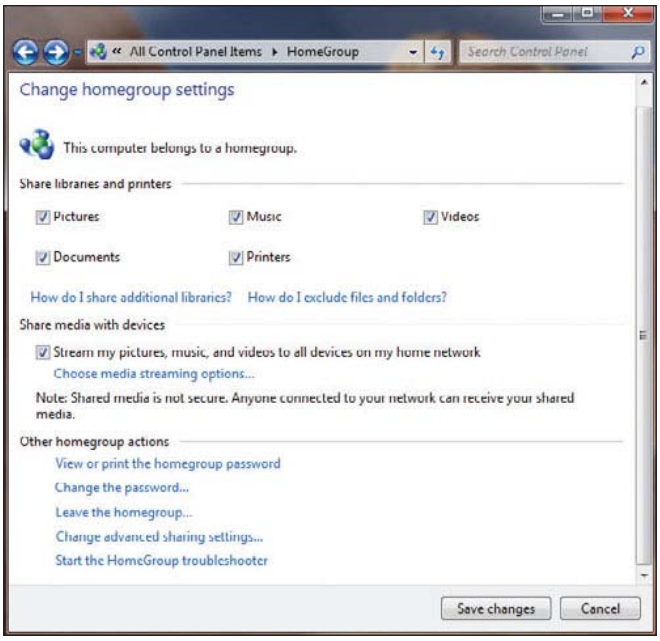


Figure 7.30

The Change HomeGroup settings screen allows you to configure sharing options for a particular computer.

>The **Change HomeGroup settings** screen can be accessed by clicking the **Computer link** on the **Start** menu, then clicking the **HomeGroup** icon, and then clicking the **View HomeGroup settings** link.

your wireless network. Therefore, logging your Mac onto the network will require knowing the SSID and its passphrase. When you boot up your Mac, the wireless card should be on by default. The network login screen (see Figure 7.31) should appear with a list of available networks (that is, the ones the NIC in your Mac can detect). The locks next to the network names indicate a secure network, which will require a password. Enter the password for the network in the password box and click the Join button to connect to the network. For unsecure networks, the Join button can be clicked without entering anything in the password box.

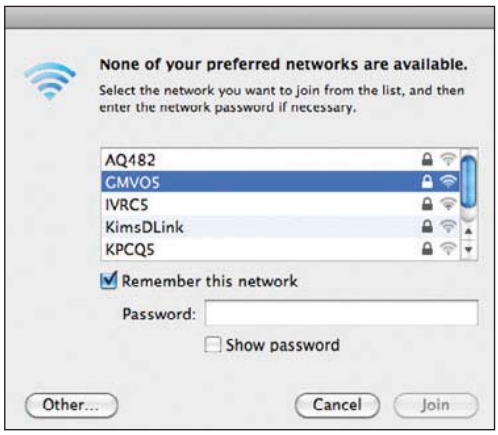


Figure 7.31

The OS X available wireless networks dialog box.

Why don't some networks appear as available? But networks with SSID broadcast turned off will not appear on the list of available networks. To join one of these secure networks, click the Other button on the available wireless network dialog box. This will cause the Enter the name of the network dialog box to appear (see Figure 7.32). Then just enter the SSID name for your network in the Network name box and the security passphrase in the password box. Clicking the join button will then connect you to the network. Checking the Remember this network check box will cause the computer to automatically connect to the network when it is available (that is, it becomes one of your preferred networks). You can have multiple preferred networks such as your home, school and local coffee shop networks.

Assuming you installed and configured everything properly, your home network should now be up and running, allowing you to share files, Internet connections, and peripherals. You are now ready to configure other non-computer devices to connect them to your network.

Wireless Node Configuration

How do I hook up devices like a TiVo or gaming console to my network? For a wired connection, you would simply plug a cable into the device and your router. For wireless connections, there is usually a set of steps to follow in the setup menu for the device you are configuring. Assuming you set up a secure wireless network as described in the security section of this chapter, you'll need to know the SSID name of your network and the security passphrase. Although each device's configuration steps will be slightly different, eventually, you will get to a screen where you need to input the SSID name and the

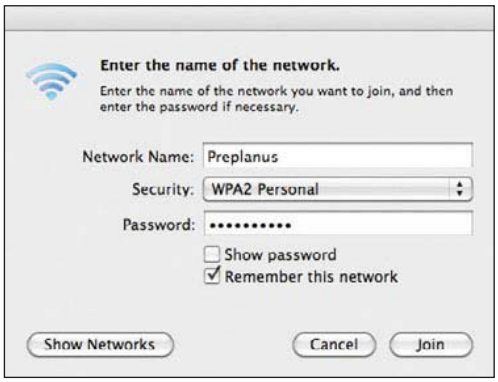


Figure 7.32

The OS X secure wireless networks dialog box.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

TRENDS IN IT

Careers: Cybercops on the Beat—Computer Security Careers

You probably have a lot of data on your home network such as music and video files. And you probably generate more data every day. But this pales in comparison to the data generated by most businesses. The vast quantities of data on business and government networks also require much higher levels of protection than the data on your home network. With billions of dollars spent on e-commerce initiatives every year, companies have a vested interest in keeping their information technology (IT) infrastructures humming along. The rise in terrorism has shifted the focus slightly—from protecting virtual assets and access, to protecting these plus physical assets and access points. The increased need for virtual and physical security measures means there should be a robust job market ahead for computer security experts.

The National Security Agency and the Office of Homeland Security are both encouraging information security professionals to be proficient in information assurance. As defined by the NSA, *information assurance* is "the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The five key attributes of secure information systems are as follows:

1. **Availability:** The extent to which a data-processing system is able to receive and process data. A high degree of availability is usually desirable.
2. **Integrity:** A quality that an information system has if the processing of information is logical and accurate and the data is protected against unauthorized modifications or destruction.
3. **Authentication:** Security measures designed to protect an information system against acceptance of a fraudulent transmission of data by establishing the validity of a data transmission or message, or the identity of the sender.
4. **Confidentiality:** The assurance that information is not disclosed to unauthorized persons, processes, or devices.
5. **Nonrepudiation:** A capability of security systems that guarantees that a message or data can be proven to have originated from a specific person and was processed by the recipient. The sender of the data receives a receipt for the data, and the receiver of the data gets proof of the sender's identity. The objective of nonrepudiation is to prevent either party from later denying having handled the data.

The Global Information Assurance Certification, or GIAC (**giac.org**), is an industry-recognized certification that provides objective evidence (through examinations) that security professionals have mastered key skills in various aspects of information assurance.

What skill sets will be most in demand for security professionals? In addition to information assurance technical skills (with an emphasis on network engineering and data communications), broad-based business experience is also extremely desirable. IT security professionals need to understand the key issues of e-commerce and the core areas of their company's business (such as marketing, sales, and finance). Understanding how a business works is essential to pinpointing and correcting security risks that could be detrimental to a company's bottom line. Because of the large number of attacks by hackers, security and forensic skills and related certifications also are in high demand. Working closely with law enforcement officials is essential to rapidly solving and stopping cybercrime.

Another important attribute of security professionals is the ability to lead and motivate teams. Security experts need to work with diverse members of the business community, including customers, to forge relationships and understanding among diverse groups. Security professionals must conduct skillful negotiations to ensure that large project implementations are not unduly delayed by security initiatives or pushed through with inadequate security precautions. Diplomacy is therefore a sought-after skill.

Look for more colleges and universities to roll out security-based degree and certificate programs as the demand for security professionals increases. These programs will most likely be appropriate for experienced networking professionals who are ready to make the move into the IT security field. If you're just starting to prepare for a career, consider a degree in network engineering, followed by network security training while you're working at your first job. A degree program that is also designed to prepare you for security certification exams is particularly desirable. Networking and security degrees, combined with passing grades on certification exams, should help you make a smooth transition into the exciting world of cybersecurity.

passphrase. The Xbox 360 configuration screens are shown in Figure 7.33.

Once all your devices are connected to your network, you might want to check your Internet connection speed to see what kind of throughput you are achieving. You can check your speed on any device on your network that can access the Internet with a browser.

How can I test my Internet connection speed? Your ISP may have promised you certain speeds of downloading and uploading data. How can you tell if you are getting what was promised? There are numerous sites on the Internet, such as **Speedtest.net** (see Figure 7.34) and **broadband.gov**, where you can test the speed of downloading files to your computer and uploading files to other computers. You can then see how your results compare to those of other users in your state and across the United States. Many factors

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

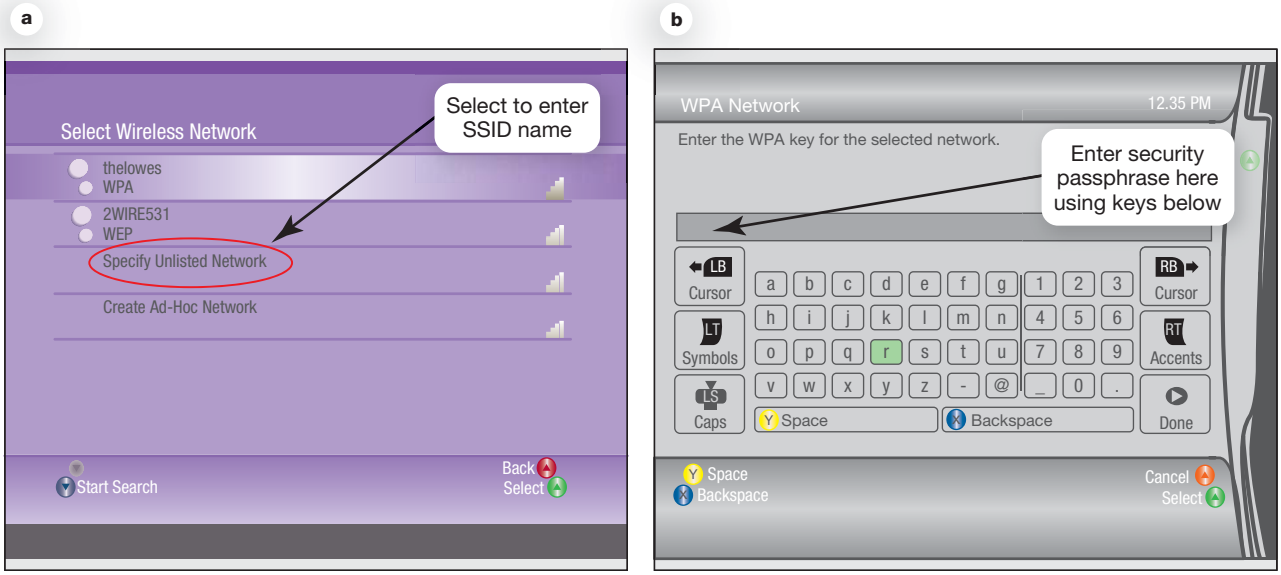


Figure 7.33

Xbox 360 wireless configuration screens. (a) The Xbox will detect available networks. Select the Specify Unlisted Network option to enter the SSID name of your network. (b) Enter the security passphrase on the appropriate security screen.

can influence your Internet speeds, so be sure to run the test at several different times during the day over the course of a week before complaining to your ISP about not getting your promised speed.

Troubleshooting Network Problems

What types of problems can I run into when installing wireless networks? The maximum range of wireless devices under the 802.11n standard is about 350 feet. But as you go farther away from your router, the throughput you achieve will decrease. Obstacles between wireless nodes also decrease throughput. Walls, floors, and large metal objects are the most common sources of interference with wireless signals. For example, placing a computer with a wireless network adapter next to a refrigerator may prevent the signals from reaching the rest of the network. Similarly, a node that has four walls between it and the Internet connection will

Figure 7.34

Speed test showing a download speed of 20.01 megabits, which is extremely fast for a home Internet connection.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

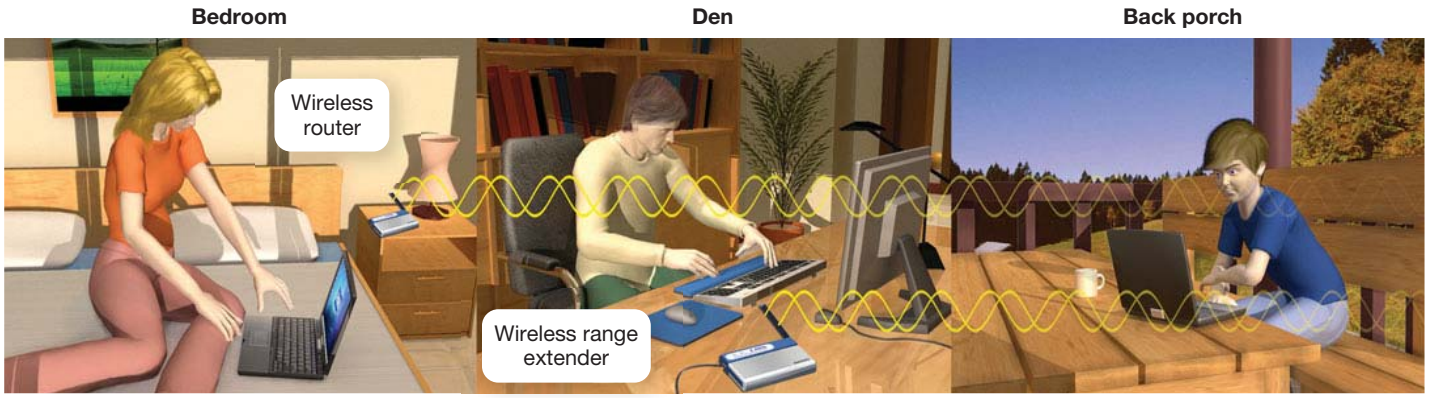


Figure 7.35

Because a wireless range extender is installed in the den, Notebook C on the back porch can now connect to the wireless network generated by the wireless router in the bedroom.

most likely have lower-than-maximum throughput.

What if a node on the network can't get adequate throughput? Repositioning the node within the same room (sometimes even just a few inches from the original position) can often affect communication between nodes. If this doesn't work, try moving the device closer to the router or to other rooms in your house. If these solutions don't work, you should consider adding a wireless range extender to your network.

A **wireless range extender** is a device that amplifies your wireless signal to get it out to parts of your home that are experiencing poor connectivity. As shown Figure 7.35, the notebook on the back porch can't connect to the wireless network even though the computer in the den can connect to the network. By placing a range extender in the den, where there is still good connectivity to the wireless network, the wireless signal is amplified and beamed farther out to the back porch. This improves the otherwise poor connectivity on the back porch and allows computer C to make a good connection to the network.

Hopefully, you'll now be able connect all your computing devices to your home network and achieve the throughput you need to move your date efficiently around your home network.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

chapter seven

summary

1. What is a network, and what are the advantages/disadvantages of setting up one?

A computer network is simply two or more computers that are connected using software and hardware so that they can communicate. Advantages of networks include allowing users to (1) share an Internet connection, (2) share peripheral devices, and (3) share files. A disadvantage is that the network must be administered.

2. What is the difference between a client/server network and a peer-to-peer network?

In peer-to-peer networks, each node connected to the network can communicate directly with every other node instead of having a separate device exercise central control over the network. P2P networks are the most common type of network installed in homes. Most networks that have 10 or more nodes are client/server networks. A client/server network contains two types of computers: a client computer on which users perform specific tasks and a server computer that provides resources to the clients and central control for the network.

3. What are the main components of every network?

To function, any network must contain four components: (1) transmission media (cables or radio waves) to connect and establish communication between nodes, (2) network adapters that allow the nodes on the network to communicate, (3) network navigation devices (such as routers and switches) that move data around the network, and (4) software that allows the network to run.

4. Which type of network is most commonly found in the home?

Ethernet networks are the most common networks used in home networking. Most Ethernet networks use a combination of wired and wireless connections depending upon the data throughput required. Wired connections usually achieve higher throughput than wireless connections.

5. What equipment and software do I need to build a network in my home?

All computing equipment that will connect to a network has to contain a network adapter. Network adapters allow computers to communicate (either wired or wirelessly) with network navigation devices such as routers and switches. Wired connections are usually made with Cat 6 twisted pair cable. A router is needed to share an Internet connection as it transmits data between two networks (the home network and the Internet).

6. Besides computers, what other devices would I connect to a home network?

Connecting peripherals such as printers directly to a network allow them to be easily shared by all users on the network. Network-attached storage (NAS) devices allow for the storage and sharing of data files such as movies and music as well as providing a central place for file backups. Connecting digital entertainment devices (such as gaming consoles) provides the ability to stream movies and other entertainment directly from the Internet.

7. Why are wireless networks more vulnerable than wired networks, and what special precautions are required to ensure my wireless network is secure?

Wireless networks are even more susceptible to hacking than wired networks because the signals of most wireless networks extend beyond the walls of your home. Neighbors may unintentionally (or intentionally) connect to the Internet through your wireless connection, and hackers may try to access it. To prevent unwanted intrusions into your network, you should change the default password on your router to make it tougher for hackers to gain access, use a hard-to-guess SSID (network name), turn off SSID broadcasting to make it harder for outsiders to detect your network, and enable security protocols such as WPA or WEP.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

8. How do I configure the software on my computer and set up other devices to get my network up and running?

Windows features software wizards that facilitate the setup of both wired and wireless networks. Plug in the modem, routers, and all cables, and then switch on the modem, router, and computers (in that order). Run the wizards, which should guide you through the process. Make sure each computer has a distinct name and ensure that all computers are in the same HomeGroup. Devices such as gaming consoles each have their own set-up procedures for connecting to wireless networks but usually require the same information as needed for connecting a computer to a secured wireless network.

9. What problems might I encounter when setting up a wireless network?

You may not get the throughput you need through a wireless connection and therefore you may need to consider a wired connection for certain devices. Distance from the router as well as walls, floors, and large metal objects between a device and the router can interfere with wireless connectivity. Wireless range extenders can amplify signals to improve connectivity in areas of poor signal strength.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

chapter seven

key terms

seven key terms

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Word Bank

- Cat 6 cable
- client/server
- data transfer rate
- hacker(s)
- home network server
- LAN
- network adapter(s)
- network-ready
- peer-to-peer (P2P)
- piggybacking
- router
- switch
- throughput
- twisted pair cable
- WAN
- wired
- wireless
- wireless range expander

Instructions: Fill in the blanks using the words from the Word Bank above.

Cathi needed to network three computers for herself and her roommates, Sharon and Emily. She decided that a(n) (1) _____ network was the right type to install in their dorm suite because a(n) (2) _____ network was too complex. Because they all liked to stream digital movies from the Internet, they needed high a(n) (3) _____ but doubted they would achieve the promised (4) _____ in any network they installed. Although they knew using (5) _____ media would provide the fastest Ethernet networks, they decided to use (6) _____ media so that they could use their notebooks wherever they were in their suite. Therefore they needed to buy a(n) (7) _____ with wireless capability that would allow them to share the broadband Internet connection that Sharon already had through a local ISP. This device would also double as a(n) (8) _____, preventing the need to purchase a separate device. Fortunately, all their computers already had (9) _____ installed, making it easy to connect the computers to the network. Cathi knew they would need to purchase some (10) _____ since the Xbox 360 they wanted to share only had a wired Ethernet adapter in it.

Cathi's roommate Emily wanted to know if they could hook into the (11) _____, or small network, that was already deployed for the students in the dorm. This student network was already hooked into the college's (12) _____, or large network, which spanned all three of the college's campuses. She knew they would need to be careful when connecting to the network, because some students from the dorm had accidentally been illegally (13) _____ on a network from the deli across the street. As the connectivity for notebooks in the lounge at the end of the hall was very poor, they needed to consider purchasing a(n) (14) _____ to extend the range of the wireless signal. As a final detail, Emily suggested they get a(n) (15) _____ printer that would plug right into the router and allow them all to print whenever they needed to do so.

Your grandmother has moved into a new retirement community. She is sharing a large living space with three other residents. All four retirees have their own notebook computers. Your grandmother has asked you to advise her and her roommates on an appropriate network to install so that they can share an Internet connection, a laser printer, and movies that they want to stream from Netflix via the Internet. And your grandmother is an avid photographer and has thousands of digital photographs on her computer. She is very concerned about forgetting to back up the photographs after she takes new ones and wants her family to be able to access her photos via the Internet.

Instructions: Using the preceding scenario, draft a networking plan for your grandmother and her roommates using as many of the keywords from the chapter as you can. Be sure that your grandmother, who is unfamiliar with many networking terms, can understand your suggestions.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

chapter seven self-test

self-test

Instructions: Answer the multiple-choice and true–false questions below for more practice with key terms and concepts from this chapter.

Multiple Choice

1. All of the following are advantages of installing a home network *except* sharing
   a. peripherals.
   b. an Internet connection.
   c. files.
   d. MAC addresses.
2. Which of the following is *not* a reason client/server networks are generally not installed in homes?
   a. Client/server networks can't handle streaming media, which is often required in home networks.
   b. Client/server networks are more difficult to install than peer-to-peer networks.
   c. Client/server networks provide more security than is needed for home networks.
   d. Peer-to-peer networks are less expensive to install than client/sever networks.
3. Which of the following is *not* required on some simple networks?
   a. Network adapters
   b. Networking software
   c. Network navigation devices
   d. Transmission media
4. Which network navigation device is required to move data between two networks?
   a. Repeater c. Router
   b. Switch d. Hub
5. If you need very fast throughput in a home network, you should use
   a. an 802.11n wireless Ethernet connection.
   b. a wired power-line network.
   c. a wired gigabit Ethernet connection.
   d. a client/server network.
6. Wireless range expanders
   a. are never used for home networks.
   b. are not needed with 802.11n networks.
   c. improve connectivity in remote areas of a home.
   d. turn devices with wired connections into wireless nodes.
7. Two or more networks connected over long geographic distances to form a single network is usually referred to as a
   a. LAN. c. HAN.
   b. MAN. d. WAN.
8. The throughput of a network
   a. is the same on all Ethernet networks.
   b. is usually higher on wireless networks.
   c. is the same in all areas covered by a wireless network.
   d. can vary depending upon the transmission media used.
9. The "name" of a particular wireless network is known as the
   a. NetID. c. SSID.
   b. HAN-ID. d. Wifi-ID.
10. The device used to move data around a single network is called a
    a. gateway.
    b. switch.
    c. router.
    d. repeater.

True–False

_____ 1. Actual data throughput is usually higher on wireless networks.

_____ 2. Ethernet networks require each node on the network to be equipped with its own network adapter.

_____ 3. WEP and WPA are popular wired network security protocols.

_____ 4. MANs cover a larger geographic area than HANs.

_____ 5. 802.11n wireless networks provide faster throughput than wired gigabit Ethernet networks.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

making the transition to... next semester

1. Dormitory Networking

Mikel, Dylan, Sanjay, and Harrison were sitting in the common room of their campus suite and complaining about their wireless network. They inherited the equipment from the last residents of the suite, and unfortunately their router uses the outdated 802.11g standard. They all have notebooks that have 802.11n network adapters, but their throughput is poor. Since they are often all surfing the Internet at the same time and trying to download movies, their network's performance has become unacceptable.

Since they all just sold last semester's books back to the bookstore for a total of $600, they decided this would be a good time to upgrade their network and peripherals. Dylan has an inkjet printer that gobbles up expensive cartridges, and Phil has a laser printer that just broke. The guys figure one good networked all-in-one printer should meet their needs since it would also provide them with photocopying capabilities. Mikel is concerned about backups for his computer. His external hard drive fell on the floor and no longer works reliably. He has a tremendous amount of photos and schoolwork on his computer that he is concerned about losing if his hard drive fails. Since the guys don't know much about networking, the four roommates have asked for your guidance. Consider the following keeping in mind their $600 budget:

a. Research network-ready laser printers on sites such as **hp.com**, **epson.com**, and **brother.com**. What network-ready all-in-one printer would you recommend? Why?
b. Research 802.11n wireless routers at sites such as **netgear.com**, **linksys.com**, and **dlink.com**. What router do you think will meet the roommates' needs? Why?
c. How would you recommend addressing Dave's backup concerns? Would you recommend a NAS device for the network, or do they have enough money left in their budget for a home network server? Research these devices and make an affordable recommendation. Check sites such as **tigerdirect.com** and **newegg.com** for competitive pricing.

2. Connecting Your Computer to Public Networks

You are working for a local coffee shop that offers free wireless access to customers. Your supervisor has asked you to create a flyer for patrons that warns them of the potential dangers of surfing the Internet in public places. Conduct research on the Internet about using public hot spots to access the Internet. Prepare a flyer that lists specific steps that customers can take to protect their data when surfing on publicly accessible networks.

3. Adding a Home Network Server for Backups to Your Network

You know that adding a home network server to your network would facilitate sharing of your digital media and would make backing up your computers easier. You need to consider the following questions when selecting an appropriate home network server:

1. What is the volume of shared media that you need to store? (In other words, how many music files, movies, and other media files do you have?)
2. What are the sizes of the hard drives of the computers on your network (for backup purposes)? What size hard drive would you need on a home network server to ensure you could back up all your computers as well as store your shared media?
3. Would you need to access files on the home network server when you are away from home or allow others (such as your cousins) to access them?

Research home network servers using sites such as **hp.com**, **acer.com**, and **lenovo.com** or use the term "home server" in a search engine. Select a server that is appropriate for your home network. Prepare a summary of your findings and include the reasons for your selection.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

making the transition to... the workplace

1. Wireless LAN for a Small Business

You are working for a local coffee shop. The owner of the shop thinks that adding a wireless network and providing free Internet access to customers would be a good way to increase business. The owner has asked you to research this idea and prepare a report of your findings. Consider the following:

a. Price out business Internet connectivity with local phone and cable providers. Which vendor provides the most cost effective solution for a coffee shop? Are there any limitations on bandwidth or the number of people that can access the Internet at one time through the business account connection?
b. What potential problems could you foresee with providing unrestricted free access to the Internet? What policies would you suggest to keep people from abusing the free Internet access? (An example of abuse is someone who sits all day and surfs for free without purchasing any coffee.)

2. Putting Computers to Work on Research Projects

Most computer CPUs only use a fraction of their computing power most of the time. Many medical research companies (such as those seeking cures for cancer and AIDS) could benefit from "borrowing" computer CPU time when computers are not being used or are being under utilized. Virtual supercomputers (which are really networks of computers) can be created using software installed on tens of thousands of computers. This type of computing is also known as *grid* or *distributed computing*. These virtual computing nets can be harnessed to solve complex problems when their owners are not using their computers. Assume that you are working for a business that has 100 computers and you would like to participate in a grid computing project. Investigate IBM's Worldwide Community Grid (**worldcommunitygrid.org**). Prepare a report for your boss that:

a. Describes the Worldwide Community Grid (WCG) and its objectives
b. Lists current projects that the WCG is working on.
c. Describes the process for installing the WCG software on the company's computers.
d. Suggests a strategy for publicizing the company's participation in the WCG project that will encourage your employer's customers to participate.

3. Testing Your Internet Connection Speed

Visit **speedtest.net** and **speakeasy.net/speedtest** and test the speed of your Internet connection at your home and in the computer lab at your school. Try to repeat the test at two different times during the day.

a. What did you find out about download speeds at your home? Are you getting as much speed as was promised by your ISP? Would this speed be sufficient for a home-based business? What type of business packages does your ISP offer, and what speeds could you expect when paying for a business package?
b. How does the connection speed at your school compare to the speed at your home? Where do you think you should have a faster connection—at your school or at your home? Why might the connection speed at your school be slower than you think it should be?

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

critical thinking questions

Instructions: Albert Einstein used *Gedankenexperiments*, or critical thinking questions, to develop his theory of relativity. Some ideas are best understood by experimenting with them in our own minds. The following critical thinking questions are designed to demand your full attention but require only a comfortable chair—no technology.

1. Protecting Your Wireless Home Network

Many people have installed wireless networks in their homes. Consider the wireless network installed in your home (or in a friend's home if you don't have wireless).

a. Is your network set up to provide adequate protection against hackers? If not, what would you need to do to make it secure?
b. Are there other wireless networks within range of your home? If so, are they set up with an adequate level of security, or can you connect to them easily? How would you go about informing your neighbors that their networks are vulnerable?

2. Adding Devices to Your Network

We discussed adding devices other than computers and computer peripherals to your network in this chapter. Consider the following for your home network:

a. Do you currently stream or download movies from Netflix, Amazon Video on Demand, or another service? If so, is your storage device sufficient or do you need more capacity? If you don't currently download this type of entertainment, would your family do so if you had a device that was attached to your network? What type of device (DVR, home server, etc.) do you think would be most appropriate for the type of media that you enjoy? How much media would you need to download and view in a month to make purchasing equipment worthwhile?
b. Do you have a need for a home security system? Would internal and external cameras be appropriate for monitoring your home? Are their people in your house (babysitters, housekeepers, contractors, etc.) on a regular basis that might need monitoring? Would you monitor these people in real time or make recordings for later review?

3. Evaluating Your Home Networking Needs

You might have a network installed in your home already, or perhaps you are still considering whether it is necessary to install one. Consider these issues:

a. Who uses computing devices in your home? How many computers (notebooks and desktops) are currently in your home? Are the computers networked? If not, should they be networked? What advantages would your family gain by networking its computers?
b. Which computer peripheral devices does your family own? Which family members need to use which peripherals? Are the peripherals network-ready or are they connected to individual computers? How easy is it to share these peripherals? Are there peripherals that your family doesn't own that would be beneficial? (Make sure to explain why.) How would you go about connecting new peripherals to your network?
c. Does your home network have network-attached storage or a home server? Would your family benefit from having this technology on your home network? What types of media do your family members routinely share? What other types would they share if they had the means?

4. Sharing a Home Internet Connection

Perhaps you have considered whether sharing a home Internet connection with your neighbors would save you money. Consider the following issues:

a. How many neighbors would be within range (say, within 350 feet of your router) of an 802.11n signal that came from your house or apartment? Do you think your neighbors would be amenable to sharing the cost of your Internet connection and your bandwidth? Why or why not?
b. Is it permissible to share an Internet connection with neighbors under your ISP's terms of use for the type of connection you purchased? If not, what type of plan would you need to upgrade to in order to share a connection with your neighbors? Would the increased cost of upgrading your connection still make it economically feasible to share a connection?

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

chapter seven team time

team time

Creating a Wireless Network

Problem

Wireless technology is being adopted by leaps and bounds, both in the home and in the workplace. Offering easy access free of physical tethers to networks seems to be a solution to many problems. However, wireless computing also has problems, ranging from poor reception to hijackers stealing your bandwidth.

Task

You are volunteering for a charity that installs wireless networks in homes for needy families. Many of these installations are done in older homes, and some recipients of the networks have reported poor connectivity in certain areas of their residences and extremely low bandwidth at other times. You have volunteered to research the potential problems and to suggest solutions to the director of the program.

Process

Break the class into three teams. Each team will be responsible for investigating one of the following issues:

1. **Detecting poor connectivity:** Research methods that can be used to find areas of poor signal strength, including signal sniffing software (**netstumbler.com**) and handheld scanning devices such as WiFi Finder (**kensington.com**). Investigate maximum distances between access points and network nodes and make appropriate recommendations. (Equipment manufacturers such as **netgear.com** and **linksys.com** provide guidelines.)
2. **Signal boosters:** Research ways to increase signal strength in access points, antennae, and wireless cards. Signal boosters are available for access points. You can purchase or construct replacement antennae or antenna enhancements. WiFi cards that offer higher power than conventional cards are now available.
3. **Security:** "War drivers" (people who cruise neighborhoods looking for open wireless networks from which to steal bandwidth) may be the cause of the bandwidth issues. Research appropriate measures to keep wireless network traffic secure from eavesdropping by hackers. In your investigation, look into the WiFi Protected Access (WPA) standard developed by the WiFi Alliance. Check out the security section of the knowledge center on the WiFi Alliance Web site to start (**wi-fi.org**).

Present your findings to your class and discuss possible causes of and ways to prevent the problems encountered at the residences. Provide your instructor with a report suitable for eventual presentation to the CEO of the charity.

Conclusion

As technology improves, wireless connectivity should eventually become the standard method of communication between networks and network devices. As with any other technology, security risks exist. Understanding those risks and how to mitigate them will allow you to participate in the design and deployment of network technology and provide peace of mind for your network users.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

In this exercise, you will research and then role-play a complicated ethical situation. The role you play may or may not match your own personal beliefs, but your research and use of logic will enable you to represent whichever view is assigned. An arbitrator will watch and comment on both sides of the arguments, and together the team will agree on an ethical solution.

Topic: Firing Employees for Expressing Views on Social Media Sites

The largest network, the Internet, provides the capability for vast social interaction. Social media sites such as Facebook, YouTube, and MySpace, as well as blogs and wikis, give everyone convenient ways to express their opinions. However, employers often are intolerant of employees who freely express negative opinions or expose inside information about their employers on social media sites. Given that most jurisdictions in the United States use the doctrine of employment at-will (that is, employees can be fired at any time for any reason, or even no reason), many employers are quick to discipline or terminate employees who express opinions with which the company disagrees. When such cases come to court, the courts often find in favor of the employers. It is clear that individual must exercise extreme care when posting work-related content.

Research Areas to Consider

- Ellen Simonetti and Delta Airlines
- Fired for blogging about work
- Free speech
- Joyce Park or Michael Tunison

Process

Divide the class into teams.

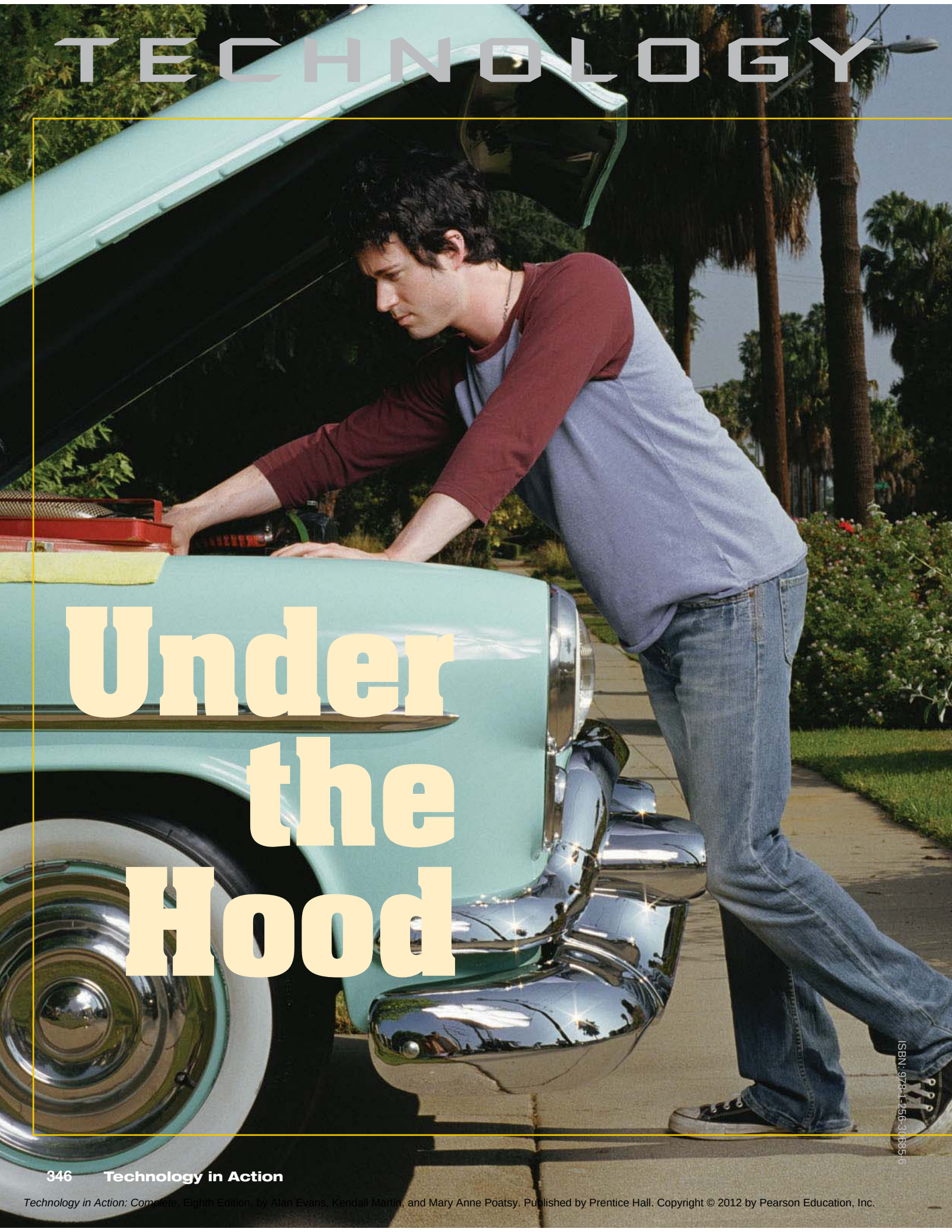
1. Research the areas cited above and devise a scenario in which someone has complained about an employee blogging about a sensitive workplace issue such as cleanliness at a food manufacturing facility or employee romances.
2. Team members should write a summary that provides background information for their character—for example: employee, Human Resources manager, or arbitrator — and details their character's behaviors to set the stage for the role-playing event. Then, team members should create an outline to use during the role-playing event.
3. Team members should arrange a mutually convenient time to meet for the exchange, either using the collaboration feature of MyITLab, the discussion board feature of Blackboard, or meeting in person.
4. Team members should present their case to the class, or submit a PowerPoint presentation for review by the rest of the class, along with the summary and resolution they developed.

Conclusion

As technology becomes ever more prevalent and integrated into our lives, more and more ethical dilemmas will present themselves. Being able to understand and evaluate both sides of the argument, while responding in a personally or socially ethical manner, will be an important skill.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.



Under the Hood

ISBN: 978-0-13-256-388-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

SOME PEOPLE ARE DRAWN TO UNDERSTANDING things in detail, but many folks are happy just to have things work. If you use a computer, you may not have ever been tempted to "look under the hood." However, without understanding the hardware inside, you'll be faced with some real limitations. You'll have to pay a technician to fix or upgrade your computer. This won't be as efficient as fine-tuning it yourself, and you may find yourself buying a new computer sooner than necessary. If you're preparing for a career in information technology, understanding computer hardware will affect the speed and efficiency of the programs you design. And what about all those exciting advances you hear about? How do you evaluate the impact of a new type of memory or a new processor? A basic appreciation of how a computer system is built and designed is a good start.

We'll build on what you've learned about computer hardware in other chapters and go under the hood, looking at the components of your system unit in more detail. Let's begin by looking at the building blocks of computers: switches.

Switches

The **system unit** is the box that contains the central electronic components of the computer. But how, exactly, does the computer perform all of its tasks? How does it process the data you input? The CPU performs functions like adding, subtracting, moving data around the system, and so on using nothing but a large number of on/off switches. In fact, a computer system can be viewed as an enormous collection of on/off switches.

ELECTRICAL SWITCHES

Computers work exclusively with numbers, not words. To process data into information, computers need to work in a language they understand. This language, called **binary language**, consists of just two numbers: 0 and 1. Everything a computer does, such as processing data or printing a report, is broken down into a series of 0s and 1s. **Electrical switches** are devices inside the computer that can be flipped between these two states: 1 and 0, signifying "on" and "off." Computers use 0s and 1s to process data because they are electronic, digital machines. They only understand two states of existence: on and off. Inside a computer these two possibilities, or states, are represented using the binary switches (or digits) 1 and 0.

You use various forms of switches every day. The on/off button on your DVD player is a mechanical switch: pushed in, it represents the value 1 (on), whereas popped out, it represents the value 0 (off). Another switch you use each day is a water faucet. As shown in Figure 1,

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

shutting off the faucet so that no water flows could represent the value 0, whereas turning it on could represent the value 1.

Computers are built from a huge collection of electrical switches. The history of computers is really a story about creating smaller and faster sets of electrical switches so that more data can be stored and manipulated quickly.

Vacuum Tubes

The earliest generation of electronic computers used devices called **vacuum tubes** as switches. Vacuum tubes act as computer switches by allowing or blocking the flow of electrical current. The problem with vacuum tubes is that they take up a lot of space, as you see in Figure 2. The first high-speed digital computer, the Electronic Numerical Integrator and Computer (ENIAC), was deployed in 1945. It used nearly 18,000 vacuum tubes as switches and filled approximately 1,500 square feet of floor space. That's about one-half the size of a standard high school basketball court! In addition to being large, the vacuum tubes produced a lot of heat and burned out frequently. Thus, vacuum tubes are impractical to use as switching devices in personal computers because of their size and reliability.

FIGURE 1
Water faucets can be used to represent binary switches.

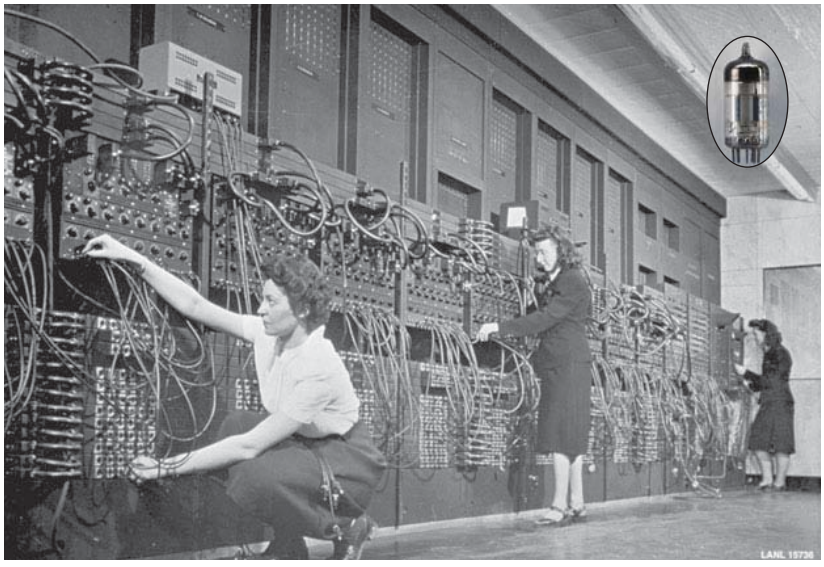
Since the introduction of ENIAC's vacuum tubes, two major revolutions have occurred in the design of switches, and consequently computers, to make them smaller and faster: the invention of the transistor and the fabrication of integrated circuits.

TRANSISTORS

Transistors are electrical switches that are built out of layers of a special type of material called a **semiconductor**, which is any material that can be controlled to either conduct electricity or act as an insulator (to prohibit electricity from passing through). Silicon, which is found in common sand, is the semiconductor material used to make transistors.

By itself, silicon does not conduct electricity particularly well, but if specific chemicals are added in a controlled way to the silicon, it begins to behave like a switch (see Figure 3). The silicon allows electrical current to flow easily when a certain voltage is applied; otherwise, it prevents electrical current from flowing, thus

FIGURE 2
Computers can be constructed using vacuum tubes (see inset). The difference in size achieved by moving from tubes to transistors allowed computers to become desktop devices.



ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

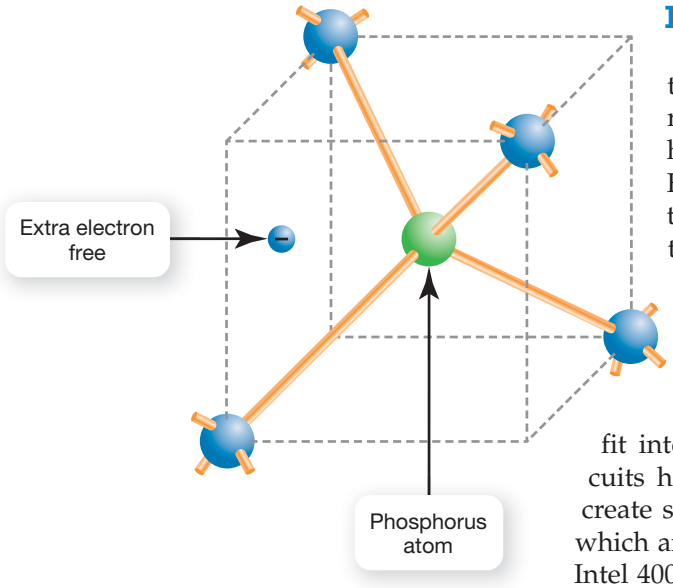


FIGURE 3
In "doping," a phosphorous atom is put in the place of a silicon atom. Because phosphorous has five electrons instead of four, the extra electron is free to move around.

behaving as an on/off switch. This kind of behavior is exactly what is needed to store digital information, the 0s (off) and 1s (on) in binary language.

Early transistors were built in separate units as small metal rods, with each rod acting as a single on/off switch. These first transistors were much smaller than vacuum tubes, produced little heat, and could quickly be switched from on to off, thereby allowing or blocking electrical current. They also were less expensive than vacuum tubes.

It wasn't long, however, before transistors reached their limits. Continuing advances in technology began to require more transistors than circuit boards could reasonably handle at the time. Something was needed to pack more transistor capacity into a smaller space. Thus, integrated circuits, the next technical revolution in switches, were developed.

Integrated Circuits

Integrated circuits (or **chips**) are tiny regions of semiconductor material such as silicon that support a huge number of transistors (see Figure 4). Along with all the many transistors, other components critical to a circuit board (such as resistors, capacitors, and diodes) are also located on the integrated circuit. Most integrated circuits are no more than a quarter inch in size.

Because so many transistors can fit into such a small area, integrated circuits have enabled computer designers to create small yet powerful **microprocessors**, which are the chips that contain a CPU. The Intel 4004, the first complete microprocessor to be located on a single integrated circuit, was released in 1971, marking the beginning of the true miniaturization of computers. The Intel 4004 contained slightly more than 2,300 transistors. Today, more than 2 billion transistors can be manufactured in a space as tiny as the nail of your little finger!

This incredible feat has fueled an industry like no other. In 1951, the Univac I computer was the size of a large room. The processor memory unit itself, which cost more than one million dollars to produce, was 14 feet long by 8 feet wide by 8.5 feet high and could perform about 1,905 operations per second. Thanks to advances in integrated circuits, the IBM PC released 30 years later took up just 1 cubic foot of space, cost $3,000, and performed 155,000 times more quickly. (For more information about computer history, see the Technology in Focus feature "The History of the PC" on page 34.)

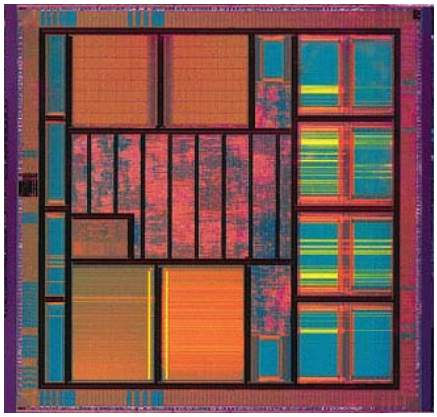


FIGURE 4
Integrated circuits use advanced fabrication techniques to fit millions of transistors into a quarter inch of silicon. This is an integrated circuit with areas marked out in black to show memory units, logic sections, and input/output blocks.

Computers use on/off switches to perform their functions. But how can these simple switches be organized so that they let you use a computer to pay your bills online or write an essay? How can a set of switches describe a number or a word, or give a computer the command to

ISBN-13: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

SOUND BYTE Where Does Binary Show Up?

In this Sound Byte, you'll learn how to use tools to work with binary, decimal, and hexadecimal numbers. (These tools come with the Windows operating system.) You'll also learn where you might see binary and hexadecimal values when you use a computer.

perform addition? Recall that to manipulate the on/off switches, the computer works in binary language, which uses only two digits, 0 and 1. To understand how a computer works, let's first look at the special numbering system called the *binary number system*.

THE BINARY NUMBER SYSTEM

A **number system** is an organized plan for representing a number. Although you may not realize it, you are already familiar with one number system. The **base 10 number system**, also known as **decimal notation**, is the system you use to represent all of the numeric values you use each day. It's called base 10 because it uses 10 digits, 0 through 9, to represent any value.

To represent a number in base 10, you break the number down into groups of ones, tens, hundreds, thousands, and so on. Each digit has a place value depending on where it appears in the number. For example, using base 10, in the whole number 6,954, there are 6 sets of thousands, 9 sets of hundreds, 5 sets of tens, and 4 sets of ones. Working from right to left, each place in a number represents an increasing power of 10, as shown here:

$$6{,}954 = 6 * (1{,}000) + 9 * (100) + 5 * (10) + 4 * (1)$$
$$= 6 * 10^3 + 9 * 10^2 + 5 * 10^1 + 4 * 10^0$$

Note that in this equation, the final number 1 is represented as 10^0 because any number raised to the zero power is equal to 1.

Anthropologists theorize that humans developed a base 10 number system because we have 10 fingers. However, computer systems, with their huge collections of on/off switches, are not well suited to thinking about numbers in groups of 10. Instead, computers describe a number in powers of 2 because each switch can be in one of two positions: on or off. This numbering system is referred to as the **binary number system**.

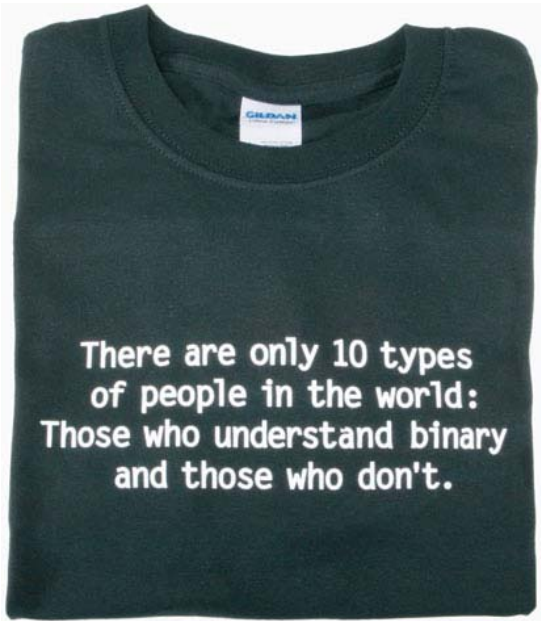


FIGURE 5
The joke here is that the base ten representation of 2 is written as 10 in binary.

The binary number system is also referred to as the **base 2 number system**. Even with just two digits, the binary number system can still represent all the values that a base 10 number system can (see Figure 5). Instead of breaking the number down into sets of ones, tens, hundreds, and thousands, as is done in base 10 notation, the binary number system describes a number as the sum of powers of 2. Binary numbers are used to represent every piece of data stored in a computer: all of the numbers, all of the letters, and all of the instructions that the computer uses to execute work.

Representing Integers

In the base 10 number system, a whole number is represented as the sum of ones, tens, hundreds, and thousands—that is, sums of powers of 10. The binary system works in the same way, but describes a value as the sum of groups of 1s, 2s, 4s, 8s, 16s, 32s, 64s, etc—that is, powers of 2: 1, 2, 4, 8, 16, 32, 64, and so on.

Let's look at the number 67. In base 10, the number 67 would be six sets of 10s and seven sets of 1s, as follows:

$$\text{Base 10: } 67 = 6 * 10^1 + 7 * 10^0$$

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

One way to figure out how 67 is represented in base 2 is to find the largest possible power of 2 that could be in the number 67. Two to the eighth power is 256, and there are no groups of 256 in the number 67. Two to the seventh power is 128, but that is bigger than 67. Two to the sixth power is 64, and there is a group of 64 inside a group of 67.

```
67 has  1 group of  64 That leaves 3 and
 3 has  0 groups of 32
        0 groups of 16
        0 groups of  8
        0 groups of  4
        1 group of   2 That leaves 1 and
 1 has  1 group of   1 And now nothing is left
```

So, the binary number for 67 is written as 1000011 in base 2:

```
Base 2: 67 = 64 + 0 + 0 + 0 + 0 + 2 + 1
           =(1 * 2^6) + (0 * 2^5) + (0 * 2^4) + (0 * 2^3) + (0 * 2^2) + (1 * 2^1) + (1 * 2^0)
           =(1000011) base 2
```

It is easier to have a calculator do this for you! Some calculators have a button labeled DEC (for decimal) and another labeled BIN (for binary). Using Windows, you can access the Scientific Calculator that supports conversion between decimal (base 10) and binary (base 2) by choosing Start, All Programs, Accessories; then clicking Calculator; and then clicking the View menu to select Programmer. Instead of the default setting of DEC (decimal), switch to BIN (binary) and enter your calculation.

A large integer value becomes a very long string of 1s and 0s in binary! For convenience, programmers often use **hexadecimal notation** to make these expressions easier to use. Hexadecimal is a base 16 number system, meaning it uses 16 digits to represent numbers instead of the 10 digits used in base 10 or the 2 digits used in base 2. The 16 digits it uses are the 10 numeric digits, 0 to 9, plus six extra symbols: A, B, C, D, E, and F. Each of the letters A through F corresponds to a numeric value, so that A equals 10, B equals 11, and so on (see Figure 6). Therefore, the

SOUND BYTE Binary Numbers Interactive

This Sound Byte helps remove the mystery surrounding binary numbers. You'll learn about base conversion among decimal, binary, and hexadecimal systems interactively, using colors, sounds, and images.

FIGURE 6 Sample Hexadecimal Values

Decimal Number	Hexadecimal Value	Decimal Number	Hexadecimal Value
00	00	08	08
01	01	09	09
02	02	10	A
03	03	11	B
04	04	12	C
05	05	13	D
06	06	14	E
07	07	15	F

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

value 67 in decimal is 1000011 in binary or 43 in hexadecimal notation. It is much easier for computer scientists to use the two-digit 43 than the seven-digit string 1000011. The Windows Calculator in Scientific view also can perform conversions to hexadecimal notation. (You can watch a video showing you how to perform conversions between bases using the Windows Calculator in the Sound Byte titled "Where Does Binary Show Up?")

Representing Characters: ASCII

We have just been converting integers from base 10, which *we* understand, to base 2 (binary state), which the computer understands. Similarly, we need a system that converts letters and other symbols that *we* understand to a binary state that the computer understands. To provide a consistent means for representing letters and other characters, certain codes dictate how to represent characters in binary format. Older mainframe computers use Extended Binary-Coded Decimal Interchange Code (EBCDIC, pronounced "Eb-sih-dik"). However, most of today's personal computers use the American National Standards Institute (ANSI, pronounced "An-see") standard code, called the **American Standard Code for Information Interchange** (**ASCII**, pronounced "As-key"), to represent each letter or character as an 8-bit (or 1-byte) binary code.

Each binary digit is called a **bit** for short. Eight binary digits (or bits) combine to create one **byte**. We have been converting base 10 numbers to a binary format. In such cases, the binary format has no standard length. For example, the binary format for the number 2 is two digits (10), whereas the binary format for the number 10 is four digits (1010). Although binary numbers can have more or fewer than 8 bits, each single alphabetic or special character is 1 byte (or 8 bits) of data and consists of a unique combination of a total of eight 0s and 1s.

The ASCII code represents the 26 uppercase letters and 26 lowercase letters used in the English language, along with many punctuation symbols and other special characters, using 8 bits. Figure 7 shows several examples of ASCII code representation of printable letters and characters.

Representing Characters: Unicode

Because it represents letters and characters using only 8 bits, the ASCII code can assign only 256 (or 2^8) different codes for unique characters and letters. Although this is enough to represent English and many other characters found in the world's languages, ASCII code cannot represent all languages and symbols, because some languages require more than 256 characters and letters. Thus, a new encoding scheme, called **Unicode**, was created. By using 16 bits instead of the 8 bits used in ASCII, Unicode can represent nearly 1,115,000 code points and currently assigns more than 96,000 unique character symbols (see Figure 8). The first 128 characters of Unicode are identical to ASCII, but because of its depth, Unicode is also able to represent the alphabets of all

FIGURE 7 ASCII Standard Code for a Sample of Letters and Characters

ASCII Code	Represents This Symbol	ASCII Code	Represents This Symbol
01000001	A	01100001	a
01000010	B	01100010	b
01000011	C	01100011	c
01011010	Z	00100011	#
00100001	!	00100100	$
00100010	"	00100101	%

Note: For the full ASCII table, see **asciitable.com**.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

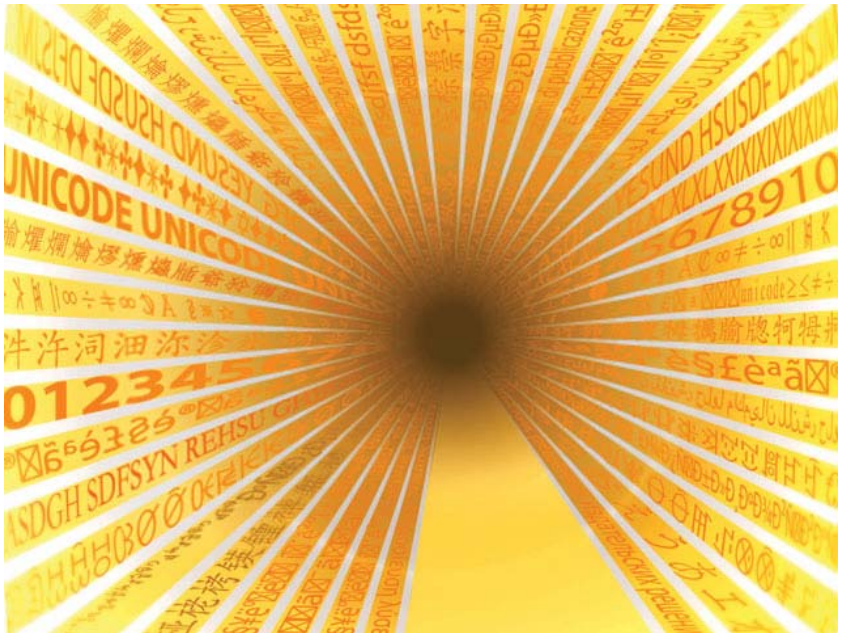


FIGURE 8
The written languages of the world require thousands of different characters, shown here. Unicode provides a system allowing digital representation of over 1,100,000 unique characters.

modern and historic languages and notational systems, including such languages and writing systems as Tibetan, Tagalog, Japanese, and Canadian Aboriginal syllabics. As we continue to become a more global society, it is anticipated that Unicode will replace ASCII as the standard character formatting code.

Representing Decimal Numbers

The binary number system also can represent a decimal number. How can a string of 1s and 0s capture the information in a value such as 99.368? Because every computer must store such numbers in the same way, the Institute of Electrical and Electronics Engineers (IEEE) has established a standard called the *floating-point standard* that describes how numbers with fractional parts should be represented in the binary number system. Using a 32-bit system, we can represent an incredibly wide range of numbers. The method dictated by the IEEE standard works the same for any number with a decimal point, such as the number –0.75. The first digit, or bit (the sign bit), is used to indicate whether the number is positive or negative. The next eight bits store the magnitude of the number, indicating whether the number is in the hundreds or millions, for example. The standard says to use the next 23 bits to store the value of the number.

Interpretation

All data inside the computer is stored as bits. Positive and negative numbers can be stored using signed integer notation, with the first bit (the sign bit) indicating the sign and the rest of the bits indicating the value of the number. Decimal numbers are stored according to the IEEE floating-point standard, and letters and symbols are stored according to the ASCII code or Unicode. All of these different number systems and codes exist so that computers can store different types of information in their on/off switches. No matter what kind of data you input in a computer—a color, a musical note, or a street address—that data will be stored as a string of 1s and 0s. The important lesson is that the interpretation of 0s and 1s is what matters. The same binary pattern could represent a positive number, a negative number, a fraction, or a letter.

How does the computer know which interpretation to use for the 1s and 0s? When your brain processes language, it takes the sounds you hear and uses the rules of English, along with other clues, to build an interpretation of the sound as a word. If you are in New York City and hear someone shout, "Hey, Lori!" you expect someone is saying hello to a friend. If you are in London and hear the same sound—"Hey! Lorry!"—you jump out of the way because a truck is coming at you! You knew which interpretation to apply to the sound because you had some other information—that you were in England.

Likewise, the CPU is designed to understand a specific language or set of instructions. Certain instructions tell the CPU to

ISBN-13: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

expect a negative number next or to interpret the following bit pattern as a character. Because of this extra information, the CPU always knows which interpretation to use for a series of bits.

The CPU Machine Cycle

Any program you run on your computer is actually a long series of binary code describing a specific set of commands the CPU must perform. These commands may be coming from a user's actions or may be instructions fed from a program while it executes. Each CPU is somewhat different in the exact steps it follows to perform its tasks, but all CPUs must perform a series of similar general steps. These steps, illustrated in Figure 9, are referred to as a CPU **machine cycle** (or **processing cycle)**.

1. FETCH: When any program begins to run, the 1s and 0s that make up the program's binary code must be "fetched" from their temporary storage location in random access memory (RAM) and moved to the CPU before they can be executed.

2. DECODE: Once the program's binary code is in the CPU, it is decoded into the commands the CPU understands.

3. EXECUTE: Next, the CPU actually performs the work described in the commands.

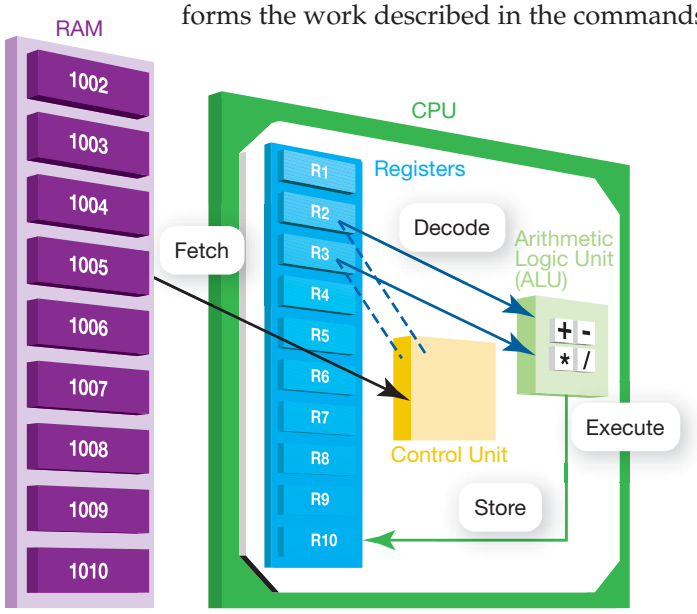


FIGURE 9
The CPU machine cycle.

Specialized hardware on the CPU performs addition, subtraction, multiplication, division, and other mathematical and logical operations at incredible speeds.

4. STORE: The result is stored in one of the **registers**, special memory storage areas built into the CPU, which are the most expensive, fastest memory in your computer. The CPU is then ready to fetch the next set of bits encoding the next instruction.

No matter what program you are running, be it a Web browser or a word processing program, and no matter how many programs you are using at one time, the CPU performs these four steps over and over at incredibly high speeds. Shortly, we'll look at each stage in more detail so that you can understand the complexity of the CPU's design, how to compare different CPUs on the market, and what enhancements you can expect in CPU designs of the future. But first, let's examine a few of the CPU's other components that help it perform its tasks.

THE SYSTEM CLOCK

To move from one stage of the machine cycle to the next, the motherboard uses a built-in **system clock**. This internal clock is actually a special crystal that acts like a metronome, keeping a steady beat and thereby controlling when the CPU will move to the next stage of processing.

These steady beats or "ticks" of the system clock, known as the **clock cycle**, set the pace by which the computer moves from process to process. The pace, known as **clock speed**, is measured in hertz (Hz), a unit of measure that describes how many times something happens per second. Today's system clocks are measured in gigahertz (GHz), each of which represents one billion clock ticks per second. Therefore, in a 3 GHz system, there are three billion clock ticks each second. Computers with older processors would sometimes need one or more cycles to process one instruction. Today, however, CPUs are designed to handle more instructions more efficiently, and are, therefore, capable of executing more than one instruction per cycle.

THE CONTROL UNIT

The CPU, like any part of the computer system, is designed from a collection of switches. How can simple on/off switches

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

"remember" the fetch-decode-execute-store sequence of the CPU machine cycle? How can they perform the work required in each of these stages?

The **control unit** of the CPU manages the switches inside the CPU. It is programmed by CPU designers to remember the sequence of processing stages for that CPU and how each switch in the CPU should be set (i.e., on or off) for each stage. With each beat of the system clock, the control unit moves each switch to the correct on or off setting and then performs the work of that stage.

Let's now look at each of the stages in the machine cycle in a bit more depth.

STAGE 1: THE FETCH STAGE

The data and program instructions the CPU needs are stored in different areas in the computer system. Data and program instructions move between these areas as they are needed by the CPU for processing. Programs (such as Microsoft Word) are permanently stored on the hard drive because it offers nonvolatile storage, meaning the programs remain stored there even when you turn the power off. However, when you launch a program (that is, when you double-click an icon to execute the program), the program, or sometimes only the essential parts of a program, is transferred from the hard drive into RAM.

The program moves to RAM because the CPU can access the data and program instructions stored in RAM more than one million times faster than if they are left on the hard drive. In part, this is because RAM is much closer to the CPU than the hard drive is. Another reason for the delay in transmission of data and program instructions from the hard drive to the CPU is that the hard drive is a mechanical device. The hard drive has read/write heads that have to sweep over the spinning platters, which takes time. RAM is faster because it's electronic, not mechanical.

As specific instructions from the program are needed, they are moved from RAM into registers (the special storage areas located on the CPU itself), where they wait to be executed.

The CPU's storage area is not big enough to hold everything it needs to process at the same time. If enough memory were located on the CPU chip itself, an entire program could be copied to the CPU from RAM before it was executed. This certainly would add to the computer's speed and efficiency, because there would be no delay while the CPU stopped processing operations to fetch instructions from RAM to the CPU. However, including so much memory on a CPU chip would make these chips extremely expensive. In addition, CPU design is so complex that only a limited amount of storage space is available on the CPU itself.

SOUND BYTE Computer Architecture Interactive

In this Sound Byte, you'll take animated tours that illustrate many of the hardware concepts introduced in this chapter. Along the way, you'll learn about the machine cycle of the CPU, the movement of data between RAM and the CPU, and the hierarchy of the different types of memory in computer systems.

Cache Memory

The CPU doesn't actually need to fetch every instruction from RAM each time it goes through a cycle. There is another layer of storage, called **cache memory**, that has even faster access than RAM. The word *cache* is derived from the French word *cacher*, which means "to hide." Cache memory consists of small blocks of memory located directly on and next to the CPU chip. These memory blocks are holding places for recently or frequently used instructions or data that the CPU needs the most. When these instructions or data are stored in cache memory, the CPU can retrieve them more quickly than would be the case if it had to access the instructions or data in RAM.

Taking data you think you'll be using soon and storing it nearby is a simple idea but a powerful one. This is a strategy that shows up in other places in your computer system. For example, when you are browsing Web pages, it takes longer to download images than text. Your browser software automatically stores images on your hard drive so that you don't have to wait to download them again if you want to go back and view a page you've already visited. Although this cache of files is not related to the cache

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

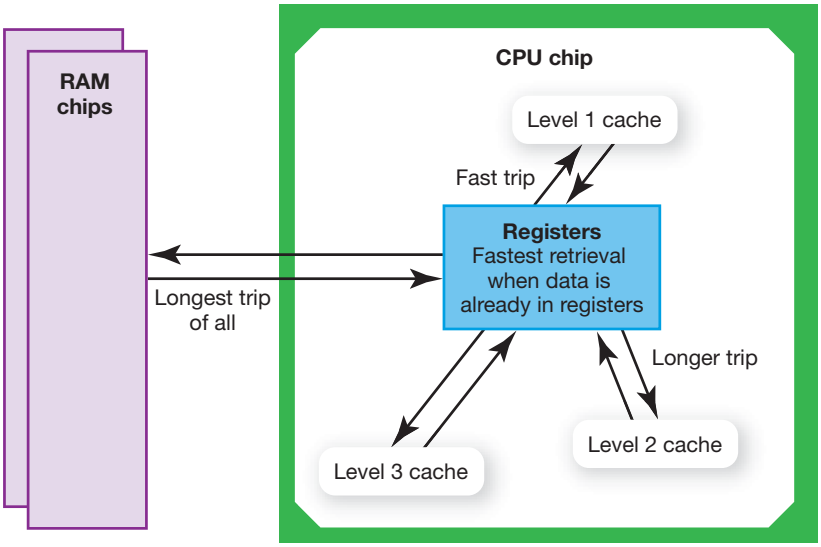


FIGURE 10
Modern CPUs have two or more levels of cache memory, which leads to faster CPU processing.

storage space designed into the CPU chip, the idea is the same.

Modern CPU designs include several types of cache memory. If the next instruction to be fetched is not already located in a CPU register, instead of looking directly to RAM to find it, the CPU first searches Level 1 cache. **Level 1 cache** is a block of memory that is built onto the CPU chip to store data or commands that have just been used.

If the command is not located in Level 1 cache, the CPU searches Level 2 cache. Depending on the design of the CPU, **Level 2 cache** is either located on the CPU chip but is slightly farther away from the CPU, or is on a separate chip next to the CPU and therefore takes somewhat longer to access. Level 2 cache contains more storage area than does Level 1 cache. For the Intel Core i7, for example, the Level 1 cache is 64 kilobytes (KB) and the Level 2 cache is 1 megabytes (MB).

Only if the CPU doesn't find the next instruction to be fetched in either Level 1 or Level 2 cache will it make the long journey to RAM to access it.

The current direction of processor design is toward increasingly large multilevel CPU cache structures. Therefore, some newer CPUs, such as Intel's Core i7 processors, have an additional third level of cache memory storage called **Level 3 cache**. On computers with Level 3 cache, the CPU checks this area for instructions and data after it looks in Level 1 and Level 2 cache, but before it makes the longer trip to RAM (see Figure 10). The Level 3 cache holds between 2 and 12 MB of data. With 12 MB of Level 3 cache, there is storage for some entire programs to be transferred to the CPU for execution.

As an end user of computer programs, you do nothing special to use cache memory. In fact, you are not even able to see that caching is being used—nothing special lights up on your system unit or keyboard. The advantage of having more cache memory is that you'll experience better performance because the CPU won't have to make the longer trip to RAM to get data and instructions as often. Unfortunately, because it is built into the CPU chip or motherboard, you can't upgrade cache; it is part of the original design of the CPU. Therefore, as with RAM, it's important when buying a computer to consider buying the one, everything else being equal, with the most cache memory.

STAGE 2: THE DECODE STAGE

The main goal of the decode stage is for the CPU's control unit to translate (or **decode**) the program's instructions into commands the CPU can understand. A CPU can understand only a tiny set of commands. The collection of commands a specific CPU can execute is called the **instruction set** for that system. Each CPU has its own unique instruction set. For example, the AMD Phenom II X6 six core processor in a Gamer Mage system from iBuyPower has a different instruction set than does the Intel Core i5 used in a Dell Inspiron notebook. The control unit interprets the code's bits according to the instruction set the CPU designers laid out for that particular CPU. Based on this process of translation, the control unit then knows how to set up all the switches on the CPU so that the proper operation will occur.

Because humans are the ones who write the initial instructions, all of the commands in an instruction set are written in a language called **assembly language**, which is easier for humans to work with than binary. Many CPUs have similar assembly commands in

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

their instruction sets, including the commands listed here:

ADD	Add
SUB	Subtract
MUL	Multiply
DIV	Divide
MOVE	Move data to RAM
STORE	Move data to a CPU register
EQU	Check if equal

CPUs differ in the choice of additional assembly language commands selected for the instruction set. Each CPU design team works to develop an instruction set that is both powerful and speedy.

However, because the CPU knows and recognizes only patterns of 0s and 1s, it cannot understand assembly language directly, so these human-readable instructions are translated into long strings of binary code. The control unit uses these long strings of binary code called **machine language** to set up the hardware in the CPU for the rest of the operations it needs to perform. Machine language is a binary code for computer instructions, much like the ASCII code is a binary code for letters and characters. Similar to each letter or character having its own unique combination of 0s and 1s assigned to it, a CPU has a table of codes consisting of combinations of 0s and 1s for each of its commands. If the CPU sees a particular pattern of bits arrive, it knows the work it must do. Figure 11 shows a few commands in both assembly language and machine language.

STAGE 3: THE EXECUTE STAGE

The **arithmetic logic unit (ALU)** is the part of the CPU designed to perform mathematical operations such as addition, subtraction, multiplication, and division and to test the comparison of values such as *greater than*, *less than*, and *equal to*. For example, in calculating an average, the ALU is where the addition and division operations would take place. The ALU also performs logical OR, AND, and NOT operations. For example, in determining whether a student can graduate, the ALU would need to ascertain whether the student had taken all required courses AND obtained a passing grade in each of them. The ALU is specially designed to execute such calculations flawlessly and with incredible speed.

The ALU is fed data from the CPU's registers. The amount of data a CPU can process at a time is based in part on the amount of data each register can hold. The number of bits a computer can work with at a time is referred to as its **word size**. Therefore, a 64-bit processor can process more information faster than a 32-bit processor.

STAGE 4: THE STORE STAGE

In the final stage, the result produced by the ALU is stored back in the registers. The instruction itself will explain which register should be used to store the answer. Once the entire instruction has been completed, the next instruction will be fetched, and the fetch-decode-execute-store sequence will begin again.

FIGURE 11 Representations of Sample CPU Commands

Human Language for Command	CPU Command in Assembly Language (Language Used by Programmers)	CPU Command in Machine Language (Language Used in the CPU's Instruction Set)
Add	ADD	1110 1010
Subtract	SUB	0001 0101
Multiply	MUL	1111 0000
Divide	DIV	0000 1111

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

Making CPUs Even Faster

Knowing how to build a CPU that can run faster than the competition can make a company rich. However, building a faster CPU is not easy. A new product launch must take into consideration the time it will take to design, manufacture, and test that processor. When the processor finally hits the market, it must be faster than the competition if the manufacturer hopes to make a profit. To create a CPU that will be released 36 months from now, it must be built to perform at least twice as fast as anything currently available.

Gordon Moore, the cofounder of processor manufacturer Intel, predicted more than 40 years ago that the number of transistors on a processor would double every 18 months. Known as **Moore's Law**, this prediction has been remarkably accurate—but only with tremendous engineering ingenuity. The first 8086 chip had only 29,000 transistors and ran at 5 MHz. Advances in the number of transistors on processors through the 1970s, 1980s, and 1990s continued to align with Moore's prediction.

However, there was a time near the turn of the 21st century when skeptics questioned how much longer Moore's Law would hold true. These skeptics were proved wrong with the microprocessor's continued growth in power. Today's Intel i7 chip has 774 million transistors—more than 18 times the transistor count of the Pentium 4 from the year 2000. Moreover, Intel's Itanium 9300 flaunts a whopping 2.3 billion transistors! How much longer can Moore's prediction hold true? Only time will tell.

Processor manufacturers can increase CPU performance in many different ways. One approach is to use a technique called *pipelining* to boost performance. Another approach is to design the CPU's instruction set so that it contains specialized, faster instructions for handling multimedia and graphics. In addition, some CPUs, such as Intel's i7 980X or the AMD Phenom II x6 processors, now have six independent processing paths inside, with one CPU chip doing the work of six separate CPU units. Some heavy computational problems are attacked by large numbers of computers actually clustered together to work at the same time.

PIPELINING

As an instruction is processed, the CPU runs sequentially through the four stages of processing: fetch, decode, execute, and store. **Pipelining** is a technique that allows the CPU to work on more than one instruction (or stage of processing) at a time, thereby boosting CPU performance.

For example, without pipelining, it may take four clock cycles to complete one instruction (one clock cycle for each of the four

DOES YOUR COMPUTER NEED MORE POWER? TEAM IT UP!

The history of computing shows us that processing power increases tremendously each year. One strategy in use now for continuing that trend is cluster computing. If one computer is powerful, then two are twice as powerful—if you can get them to work together. A *computing cluster* is a group of computers, connected by specialized clustering software, that works together to solve complex equations. Most clusters work on something called the *balancing principle*, whereby computational work is transferred from overloaded (busy) computers in the cluster to computers that have more computing resources available. Computing clusters, although not as fast as supercomputers (single computers with extremely high processing capabilities), can perform computations faster than one computer working alone and are used for complex calculations such as weather forecasting and graphics rendering. You can now rent time on computing clusters through services like PurePowua (**purepowua.com**), where you can upload and remotely control your job from your desktop as it runs on a cluster of computers.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

processing stages). However, with a four-stage pipeline, the computer can process four instructions at the same time. Like an automobile assembly line, instead of waiting for one car to go completely through each process of assembly, painting, and so on, you can have four cars going through the assembly line at the same time. When every component of the assembly line is done with its process, the cars all move on to the next stage.

Pipelined architectures allow several instructions to be processed at the same time. The ticks of the system clock (the clock cycle) indicate when all instructions move to the next process. The secret of pipelining is that the CPU is allowed to be fetching one instruction while it is simultaneously decoding another, executing a third, storing a fourth, and so on. Using pipelining, a four-stage processor can potentially run up to four times faster because some instruction is finishing every clock cycle rather than waiting four cycles for each instruction to finish. In Figure 12a, a non-pipelined instruction takes four clock cycles to be completed, whereas in Figure 12b, the four instructions have been completed in the same time using pipelining.

The number of stages in a pipeline depends entirely on design decisions. Earlier we analyzed a CPU that went through four stages in the execution of an instruction. The Intel Pentium 4 with hyperthreading featured a 31-stage pipeline, and the PowerPC G5 processor used a 10-stage pipeline. Thus, similar to an assembly line, in a 31-stage pipeline, as many as 31 different instructions can be processed at any given time, making the processing of information much faster. However, because so many aspects of the CPU design interact, you cannot predict performance based solely on the number of stages in a pipeline.

There is a cost to pipelining a CPU as well. The CPU must be designed so that each stage (fetch, decode, execute, and store) is independent. This means that each stage must be

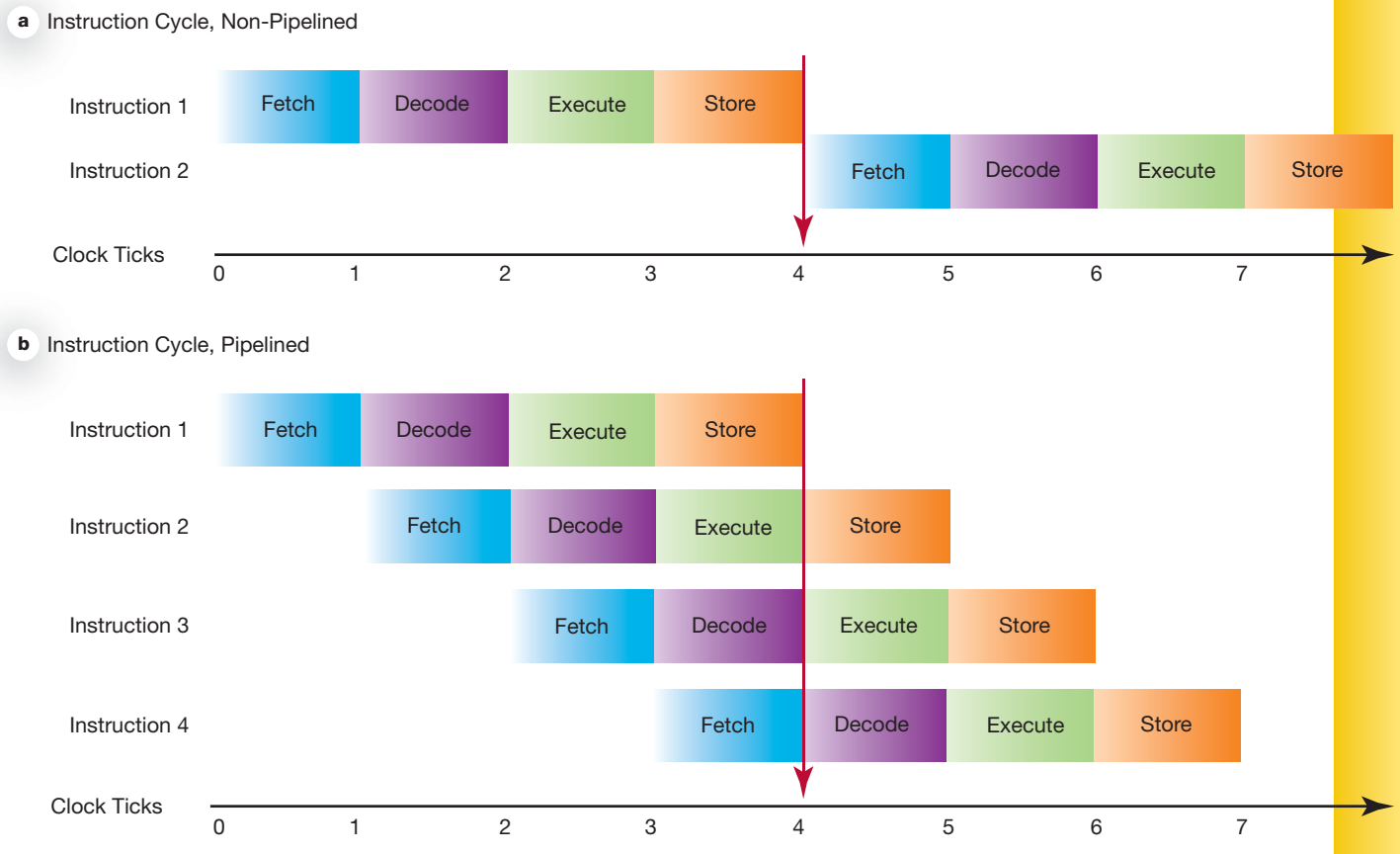


FIGURE 12

Instead of (a) waiting for each instruction to complete, (b) pipelining allows the system to work on more than one set of instructions at one time.

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

able to run at the same time that the other three stages are running. This requires more transistors and a more complicated hardware design.

SPECIALIZED MULTIMEDIA INSTRUCTIONS

Each design team that develops a new CPU tries to imagine what users' greatest needs will be in four or five years. Currently, several processors on the market reflect this consideration by incorporating specialized multimedia instructions into the basic instruction set.

Hardware engineers have redesigned the chip so that the instruction set contains new commands that are specially designed to speed up the work needed for video and audio processing. For example, Intel has integrated the Streaming Single Instruction Multiple Data (SIMD) Extensions 3 set of commands into its processor designs, adding a special group of 157 commands to the basic instruction set. These multimedia-specific instructions work to accelerate video, speech, and image processing in the CPU.

MULTIPLE PROCESSING EFFORTS

Many high-end server systems employ a **quad processor design** that has four completely separate CPU chips on one motherboard. Often, these server systems can later be scaled so that they can accommodate four, six, or even twelve processors. The Cray Jaguar supercomputer has a total of 37,376 independent processors!

Meanwhile, Intel is promoting a technology called *multi-core processing* in its Core processor line of chips. Chips with dual-core processing capabilities have two separate parallel processing paths inside them, so they are almost as fast as two separate CPUs. Dual-core processing is especially helpful because antivirus software and other security programs often run in the background as you use your system. A dual-core processor enables these multiple applications to execute much more quickly than with traditional CPUs. Six-core processors, like the Intel i7 Extreme Edition, are appearing in high-performance home-based systems now as well, executing six separate processing paths.

Multiprocessor systems are often used when intensive computational problems need to be solved in such areas as computer simulations, video production, and graphics processing. Having two processors allows the work to be done almost twice as quickly, but not quite. It is not quite twice as fast because the system must do some extra work to decide which processor will work on which part of the problem and to recombine the results each CPU produces.

Certain types of problems are well suited to a parallel-processing environment. In **parallel processing**, there is a large network of computers, with each computer working on a portion of the same problem simultaneously. To be a good candidate for parallel processing, a problem must be one that can

TODAY'S SUPER-COMPUTERS: THE FASTEST OF THE FAST

Supercomputers are the biggest and most powerful type of computer. Scientists and engineers use these computers to solve complex problems or to perform massive computations. Some supercomputers are single computers with multiple processors, whereas others consist of multiple computers that work together.

The top spot on the June 2010 Top 500 List was won by the Cray Jaguar. It operates at a peak of more than 2,300 teraflops (or 2,300 trillion operations per second). That's almost 23,000 times faster than the fastest personal computer! Second position was the entry from China, the Nebulae.

Check out the current crop of the world's fastest supercomputers at the Top 500 site (**top500.org**).

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.

be divided into a set of tasks that can be run simultaneously. So, for example, a problem where millions of faces are being compared with a target image for recognition is easily adapted to a parallel setting. The target face can be compared at the same time to many hundreds of faces. But if the next step of an algorithm can be started only after the results of the previous step have been computed, parallel processing will present no advantages.

A simple analogy of parallel processing is a laundromat. Instead of taking all day to do five loads of laundry with one machine, you can bring all your laundry to a laundromat, load it into five separate machines, and finish it all in approximately the same time it would have taken you to do just one load on a single machine. In real life, parallel processing is used in complex weather forecasting to run calculations over many different regions around the globe; in the airline industry to analyze customer information in an effort to forecast demand; and by the government in census data compilation.

Thus, what you can continue to expect from CPUs in the future is that they will continue to get smaller and faster and consume less power. This fits with the current demands of consumers for more powerful portable computing devices.

At the most basic level of binary 1s and 0s, computers are systems of switches that can accomplish impressive tasks. By understanding the hardware components that make up your computer system, you can use your system more effectively and make better buying decisions.

Multiple Choice

Instructions: Answer the multiple-choice questions below for more practice with key terms and concepts from this Technology in Focus feature.

1. Which is *not* a typical use of parallel processing systems?
   a. Computer simulations
   b. Word processing
   c. Weather modeling
   d. Graphics processing

2. What is another name for the base 10 number system?
   a. Decimal notation
   b. Binary number system
   c. Hexadecimal notation
   d. Integer system

3. Which encoding scheme can represent the alphabets of all modern and historic languages?
   a. Base 2 number system
   b. Unicode
   c. ASCII
   d. Scientific

4. Moore's Law is best described as
   a. an observation of the rate of increasing transistor density.
   b. a physical principle.
   c. a legal construct limiting performance.
   d. an advertising campaign by Intel.

5. To regulate the internal timing of a computer system, the motherboard uses
   a. a system clock.
   b. software simulation.
   c. RAM.
   d. a register.

6. Special areas of memory storage built into the CPU are known as
   a. switches.
   b. semiconductors.
   c. registers.
   d. integrated circuits.

7. Which is the correct set of steps in the machine cycle?
   a. Execute, store, fetch, decode
   b. Store, fetch, execute, decode
   c. Decode, execute, fetch, store
   d. Fetch, decode, execute, store

8. All data inside the computer is stored as
   a. bytes.
   b. bits.
   c. switches.
   d. cache memory.

9. Which statement about pipelining is *false?*
   a. Pipelining boosts CPU performance.
   b. Pipeline design is used in many modern CPUs.
   c. Pipelining requires a less complicated hardware design.
   d. The process allows the computer to process multiple instructions simultaneously.

10. From fastest to slowest, which is the fastest sequence of accessing memory?
    a. RAM, Level 1 cache, Level 2 cache, Level 3 cache
    b. Registers, Level 1 cache, Level 2 cache, RAM
    c. Level 1 cache, Level 2 cache, RAM, registers
    d. Level 2 cache, Level 1 cache, registers, RAM

ISBN: 978-1-256-30685-6

Technology in Action: Complete, Eighth Edition, by Alan Evans, Kendall Martin, and Mary Anne Poatsy. Published by Prentice Hall. Copyright © 2012 by Pearson Education, Inc.