High-Tech Talk
Triangulation: Can You Find Me Now?

Have you wondered how a Nintendo Wii game console is able to determine the precise location of a Wii Remote while a player interacts with a game? How does the Wii console know where the player is pointing the Wii Remote, swinging it like a golf club, or motioning as if you are throwing a bowling ball? The answer is triangulation.

Triangulation is the process by which you can use trigonometry to determine the location of an object by measuring the angles from two or more fixed points. Surveyors often use triangulation to measure distance. Starting at a known location and elevation, surveyors measure a predetermined length to create a base line and then use an instrument called a theodolite to measure the angle to the unknown point from each side of the base line. The length of the base line along with the two known angles allows a computer or individual to determine the exact location of the third point (Figure 1-44). Electronic theodolites calculate angles automatically and then send the calculated angles to a computer for analysis.

In Figure 1-44, the distance between points A and B is known. The theodolite calculates angle CAB (α) and also calculates angle ABC (ß). A human or computer can calculate the location of point C by determining the distance between points A and C and between points B and C. The formula used to determine the location of an object will vary depending upon the number of fixed points used in the measurement. With two fixed points, a relatively simple formula calculates the location of the third point. As the number of fixed points increases, the calculation becomes more complex.

Similarly, the Nintendo Wii game console uses triangulation to determine the location of a Wii Remote. When you set up a Wii game system, you place a sensor bar, which contains two infrared transmitters, near or on top of a television set. While you are using a Wii Remote, the Wii console determines the remote's location by calculating the distance and angles between the Wii Remote and the two transmitters on the sensor bar. Determining the location of a Wii Remote is relatively simple because the sensor bar only contains two fixed points: the transmitters.

A more complex application of triangulation occurs in global positioning systems. A global positioning system (GPS) is a navigation system that consists of one or more earth-based receivers that accept and analyze signals sent by satellites in order to determine the receiver's geographic location. GPS receivers are found in handheld navigation devices and many vehicles. GPS receivers use triangulation to determine their location relative to at least three geostationary satellites. Geostationary satellites, the fixed points in the triangulation formula, remain in the same location above the earth. Because 24 geostationary GPS satellites orbit the earth, a GPS receiver can increase its accuracy by using more than three satellites to determine its location by measuring the distance from each of the satellites, which always are a fixed distance apart, that are in range. In addition to determining position, GPS receivers also are able to calculate the speed of a moving object by recording its change in location from each satellite during a period of time. For instance, if a GPS receiver determines that you travel twohundredths of a mile in one second, it automatically would be able to calculate that you are traveling at a rate of 72 miles per hour.

Another form of triangulation also can be used to determine the exact location of certain cell phones, usually after a caller dials for emergency assistance. Although some cell phones are not equipped with a GPS receiver, computers still can determine the phone's distance from other known locations, which might include cell towers. Because the location of two or more cell towers within range are known, computers easily can calculate the location of the cell phone. If you are unsure of whether the position of your cell phone can be determined automatically, always be prepared to give your location to an emergency dispatcher.

The next time you are passing a surveyor, playing a Nintendo Wii, following a prescribed route on a vehicle's navigation system, or observing emergency personnel respond to an accident, keep in mind that none of it might have been possible without the concept of triangulation.

For more information, visit scsite.com/dc2011/ ch1/tech and then click Triangulation.

High-Tech Talk
A Computer's Internet Protocol (IP) Address

Every computer on the Internet has a unique address, called an IP address, that distinguishes it from other computers on the Internet. Currently, two versions of IP addresses exist: IPv4 (Internet Protocol Version 4) and IPv6 (Internet Protocol Version 6). An IPv4 address has two parts that identify a specific computer: one part to identify the network where that computer resides and a second part to pinpoint the specific computer or host within that network. An IPv6 address has three parts: a global prefix to identify the network, a subnet to identify the location within the network, and the interface ID to identify the specific computer or host (Figure 2-34). Today, IPv4 addresses are more commonly used. For this reason, the terms IP address and IPv4 address are used interchangeably.

A typical IPv4 address — such as 72.14.207.99 — has four groups of numbers that range from 0 through 255. This form of the IP address sometimes is called a dotted decimal number or dotted quad. The four groups of numbers in the dotted quad are called octets, because they each have 8 bits when viewed in binary form for a total of 32 bits in the IP address. For instance, the binary form of 72.14.207.99 is 01001000.00001110.11001111.01100011. For more information about how the binary system works, see Appendix C.

Because each of the 8 bits can be 1 or 0, the total possible combinations per octet are 28, or 256. Combining the four octets of an IP address provides a possible 232 or 4,294,967,296 unique values. The actual number of available addresses is about 3 billion, because some values are reserved for special use and are, therefore, off limits.

IP addresses, which are assigned by InterNIC (The Internet's Network Information Center), belong to one of three network classes: A, B, or C. In a Class A network, the first octet of the IPv4 address is assigned a number between 1 and 127. Large enterprises typically are assigned a Class A network, which can contain more than 16 million hosts; this allows network administrators to assign a value of their choice to the remaining three octets. Class B networks contain a number between 128 and 191 in the first octet. The second octet also is fixed, but the organization can assign values of its choice to the third and fourth octets. Class B networks have more than 65,000 hosts. Class C networks begin with a value between 192 and 223 and allow only the fourth octet to be customized. Class C networks can have only 254 hosts. Class D and E networks also exist, although they rarely are used.

To request data such as a Web page from a computer on the Internet, you need only an IP address. For instance, if you type the IPv4 address 72.14.207.99 in your Web browser's Address bar, the browser will display the home page on the machine hosting the Google Web site. Remembering an IP address is difficult at best — so you probably would just type the domain name, www.google.com, in the browser. The browser then contacts a domain name server (DNS) to resolve the human-readable domain name into a machine-readable IP address. Each domain name server houses a simple database that maps domain names to IP addresses. The DNS would resolve the human-readable domain name, www.google.com, into a machinereadable IP address, 72.14.207.99.

Domain names are helpful because they are easier for people to remember than IP addresses. You can learn more about a domain using the whois form at the Network Solutions Web site (www.netsol.com and then click the WHOIS link). If you type a domain name, such as google.com, the form displays the registration information for that domain, including its IP address.

Like all other computers, your computer must have an IP address to connect to the Internet or another computer that has an IP address. Servers generally have static IP addresses, because they usually are connected to the Internet and their IP addresses do not change often. When you connect to the Internet using your home computer, you most likely are using a temporary or dynamic IP address. Your access provider uses the Dynamic Host Configuration Protocol (DHCP) to assign your computer a temporary dynamic IP address from a pool of IP addresses. The dynamic IP address is unique only for that session. Once you disconnect, the DHCP server releases that IP address back in the IP address pool so that it can assign it to the next requesting computer. Even if you immediately reconnect, the DHCP server might not assign you the same IP address. Using DHCP and dynamic IP addresses means an Internet access provider needs only one IP address for each modem it supports, rather than one for each of its millions of customers.

Billions of IP addresses sounds like a lot. But, because so many computers and other devices connected to the Internet need unique IP addresses, a growing shortage of IP addresses exists. The newer IP addressing scheme is IPv6, also called IPng (IP Next Generation, which) will lengthen IP addresses from 32 bits to 128 bits and increase the number of available IP addresses to a whopping 3.4 x 1038, or 340,000,000,000,000, 000,000,000,000,000,000,000,000. Software is available that will install IPv6 on most current computers, although many networks and Internet service providers do not yet require its use. In fact, it could be many years before IPv6 completely replaces IPv4.
Do you want to know the IP address currently assigned to your computer? Click the Start button on the Windows taskbar and then click Control Panel. Click Network and Internet and then click View Network Status and Tasks. Finally, click View status and then click Details.

For more information, visit scsite.com/ dc2011/ch2/tech and then click IP Addresses.

High-Tech Talk
Computer Viruses: Delivery, Infection, and Avoidance

Klez. Melissa. Mydoom. Nimda. Like the common cold, virtually countless variations of computer viruses exist. Unlike the biological viruses that cause the common cold, people create computer viruses. To create a virus, an unscrupulous programmer must code and then test the virus code to ensure the virus can replicate itself, conceal itself, monitor for certain events, and then deliver its payload — the destructive event or prank the virus was created to deliver. Despite the many variations of viruses, most have two phases to their execution: infection and delivery.

To start the infection phase, the virus must be activated. Today, the most common way viruses spread is by people running infected programs disguised as e-mail attachments. During the infection phase, viruses typically perform three actions:

1. First, a virus replicates by attaching itself to program files. A macro virus hides in the macro language of a program, such as Word. A boot sector virus targets the master boot record and executes when the computer starts. A file virus attaches itself to program files. The file virus, Win32.Hatred, for example, replicates by first infecting Windows executable files for the Calculator, Notepad, Help, and other programs on the hard disk. The virus then scans the computer to locate .exe files on other drives and stores this information in the system registry. The next time an infected file is run, the virus reads the registry and continues infecting another drive.
2. Viruses also conceal themselves to avoid detection. A stealth virus disguises itself by hiding in fake code sections, which it inserts within working code in a file. A polymorphic virus actually changes its code as it infects computers. The Win32.Hatred virus uses both concealment techniques. The virus writes itself to the last file section, while modifying the file header to hide the increased file size. It also scrambles and encrypts the virus code as it infects files.
3. Finally, viruses watch for a certain condition or event and activate when that condition or event occurs. The event might be starting the computer or reaching a date on the system clock. A logic bomb activates when it detects a specific condition (say, a name deleted from the employee list). A time bomb is a logic bomb that activates on a particular date or time. Win32.Hatred, for instance, unleashes its destruction when the computer clock hits the seventh day of any month. If the triggering condition does not exist, the virus simply replicates.

During the delivery phase, the virus unleashes its payload, which might be a harmless prank that displays a meaningless message — or it might be destructive, corrupting or deleting data and files. When the Win32.Hatred virus triggers, it displays the author's message and then covers the screen with black dots. The virus also deletes several antivirus files as it infects the system. The most dangerous viruses do not have an obvious payload; instead they quietly modify files. A virus, for example, could change numbers randomly in an inventory program or introduce delays to slow a computer. One way antivirus software detects computer viruses is by monitoring files for unknown changes, particularly in file size. Because many computer viruses alter system and data files — files that should not change in size — changes in file sizes often are a key indication of an infection.

Other kinds of electronic annoyances exist in addition to viruses. While often called viruses, worms, Trojan horse programs, and rootkits actually are part of a broader category called malicious-logic programs or malware.

• A worm, such as the CodeRed or Sircam worm, resides in active memory and replicates itself over a network to infect machines, using up the system resources and possibly shutting the system down.
• A Trojan horse is a destructive program disguised as a real program, such as a screen saver. When a user runs a seemingly innocent program, a Trojan horse hiding inside can capture information, such as user names and passwords, from your system or open up a backdoor that allows a hacker remotely to control your computer. Unlike viruses, Trojan horses do not replicate themselves.
• A rootkit is a program that easily can hide and allow someone to take full control of your computer from a remote location, often for nefarious purposes. For example, a rootkit can hide in a folder on your computer, and the folder will appear empty. This is because the rootkit has instructed your computer not to display the contents of the folder. Rootkits can be very dangerous and often require special software to detect and remove. Rootkits are becoming more common. In fact, a recent study

has shown that more than 20 percent of computers in the United States are infected with a rootkit. It is extremely important that you use caution when installing software from unknown sources.
Every computer user is susceptible to a computer virus. Studies show that an unprotected computer can be infected by a virus within minutes after being connected to the Internet. Due to the increasing threat of viruses attacking your computer, it is more important than ever to protect your computer from viruses. Figure 3-47 lists steps you can follow to protect your computer from a virus infection.

For more information, visit scsite.com/ dc2011/ch3/tech and then click Computer Viruses.

High-Tech Talk
Random Access Memory (RAM): The Genius of Memory

Inside your computer, RAM takes the form of separate microchip modules that plug in slots on the computer's motherboard. These slots connect through a line (bus) or set of electrical paths to the computer's processor. Before you turn on a computer, its RAM is a blank slate. As you start and use your computer, the operating system files, programs, and any data currently being used by the processor are written to and stored in RAM so that the processor can access them quickly.
How is this data written to and stored in RAM? In the most common form of RAM, dynamic random access memory (DRAM), transistors (in this case, acting as switches) and a capacitor (as a data storage element) create a memory cell, which represents a single bit of data.
Memory cells are etched onto a silicon wafer in a series of columns (bitlines) and rows (wordlines), known as an array. The intersection of a column and row constitutes the address of the memory cell (Figure 4-40). Each memory cell has a unique address that can be found by counting across columns and then counting down by row. The address of a character consists of a series of memory cell addresses put together.
To write data to RAM, the processor sends the memory controller the address of a memory cell in which to store data. The memory controller organizes the request and sends the column and row address in an electrical charge along the appropriate address lines, which are very thin electrical lines etched into the RAM chip. This causes the transistors along those address lines to close.
These transistors act as a switch to control he flow of electrical current in an either closed or open circuit. While the transistors are closed, the software sends bursts of electricity along selected data lines. When the electrical charge traveling down the data line reaches an address line where a transistor is closed, the charge flows through the closed transistor and charges the capacitor.
A capacitor works as electronic storage that holds an electrical charge. Each charged capacitor along the address line represents a 1 bit. An uncharged capacitor represents a 0 bit. The combination of 1s and 0s from eight data lines forms a single byte of data.
The capacitors used in dynamic RAM, however, lose their electrical charge. The processor or memory controller continuously has to recharge all of the capacitors holding a charge (a 1 bit) before the capacitor discharges. During this refresh operation, which happens automatically thousands of times per second, the memory controller reads memory and then immediately rewrites it. This refresh operation is what gives dynamic RAM its name. Dynamic RAM has to be refreshed continually, or it loses the charges that represent bits of data. A specialized circuit called a counter tracks the refresh sequence to ensure that all of the rows are refreshed.
The process of reading data from RAM uses a similar, but reverse, series of steps. When the processor gets the next instruction it is to perform, the instruction may contain the address of a memory cell from which to read data. This address is sent to the memory controller. To locate the memory cell, the memory controller sends the column and row address in an electrical charge down the appropriate address lines.
This electrical charge causes the transistors along the address line to close. At every point along the address line where a capacitor is holding a charge, the capacitor discharges through the circuit created by the closed transistors, sending electrical charges along the data lines.
A specialized circuit called a sense amplifier determines and amplifies the level of charge in the capacitor. A capacitor charge over a certain voltage level represents the binary value 1; a capacitor charge below that level represents a 0. The sensed and amplified value is sent back down the address line to the processor.
As long as a computer is running, data continuously is being written to and read from RAM. As soon as you shut down a computer, RAM loses its data. The next time you turn on a computer, operating system files and other data are again loaded into RAM and the read/write process starts all over.

For more information, visit scsite.com/ dc2011/ch4/tech and then click Memory.

Chapter 5 Input

High-Tech Talk
Biometrics: Personalized Security

Biometric authentication is based on the measurement of an individual's unique physiological and behavioral characteristics. The most common measurements, described earlier in this chapter, such as fingerprints, hand geometry, facial features, and eye patterns are physiological biometrics. Some of the more novel measurements, such as body odor, brain wave patterns, DNA, ear shape, sweat pores, and vein patterns also fall into the category of physiological biometrics. Voice scan and signature scan are examples of behavioral biometrics.

Any biometric technology process involves two basic steps — enrollment and matching. To illustrate these steps, this High-Tech Talk uses the most common biometric technology, finger-scan technology. ENROLLMENT Enrollment is the process in which a user presents the fingerprint data to be stored in a template for future use, as shown in the top of Figure 5-46. This initial template is called the enrollment template. Creating the enrollment template involves four basic steps: (1) acquire fingerprint, (2) extract fingerprint feature, (3) create enrollment template, and (4) store enrollment template. The enrollment template usually is created only after the user has submitted several samples of the same fingerprint. Most fingerprint images will have false details, usually caused by cuts, scars, or even dirt, which must be filtered out.

The first step, acquire fingerprint, presents a major challenge to finger-scan technology. The quality of a fingerprint may vary substantially from person to person and even finger to finger. The two main methods of acquiring images are optical and silicon. With optical technology, a camera is used to register the fingerprint image against a plastic or glass platen (scanner). Silicon technology uses a silicon chip as a platen, which usually produces a higher quality fingerprint image than optical devices.

The second step, extract fingerprint feature, involves thinning the ridges of the raw image to a minuscule size and then converting the characteristics to binary format. Fingerprints are comprised of ridges and valleys that have unique patterns, such as arches, loops, and swirls. Irregularities and discontinuities in these ridges and valleys are known as minutiae. Minutiae are the distinctive characteristics upon which most finger-scan technology is based. The fingerprint-feature extraction process used is highly sophisticated, patented, and a closely-held vendor secret.

In the third step, the binary format is used to create the enrollment template. The fourth and final step involves storing the template on a storage device, such as a hard disk or smart card for future use when the same person attempts to be authenticated.

MATCHING Matching is the process of comparing a match template to an enrollment template. A match template is created when the user attempts to gain access through a fingerprint reader. Some biometric systems also include liveness detection, which verifies that a living person is creating the match template. For example, a fingerprint reader with liveness detection might monitor a pulse. Most computer and network systems are set up so that the person also must claim an identity, such as a user name, along with the fingerprint. In this case, the match template is compared directly to the enrollment template for that user name. Other systems, such as those used for criminal investigations, will search the entire enrollment template database for a match.

The match template is created in the same fashion as the enrollment template described earlier. Rather than storing the match template on disk, however, it is compared to the user's stored enrollment template, as shown in the bottom of Figure 5-46. The result of the matching process is a score. The score is compared against a threshold. The threshold is a predefined number that can be adjusted depending on the desired level of security.

The scoring process leads to the decision process. The decision process will produce one of three actions: (1) the threshold has been exceeded, thereby resulting in a match; (2) the threshold has not been met, thereby resulting in a nonmatch; or (3) the data may have been insufficient, resulting in the system requesting a new sample from the user to begin a new comparison.

Finger-scan technology has grown to become the centerpiece of the biometric industry, and even is becoming more common as an authentication method on desktop and notebook computers.

For more information, visit scsite.com/dc2011/ch5/tech and then click Biometrics.

Chapter 6 Output

High-Tech Talk
3-D Graphics: Creating a Realistic Experience

Three-dimensional (3-D) graphics, which appear to have height, width, and depth, give realistic qualities to objects in computer programs, particularly computer games. Although you view computer games on a two-dimensional (2-D) computer screen, modern technology creates a 3-D experience
by adding the appearance of depth. A game programmer can give single objects or an entire virtual world a 3-D appearance.
Creating a 3-D appearance first requires that you create a wireframe. A wireframe is a series of lines, curves, and shapes arranged to resemble an object in a 3-D world (Figure 6-35a). Most 3-D wireframes, for example, consist of a series of polygons. A completed wireframe enables you to identify the shape of the object, although it appears to be hollow. To transform the appearance of the 3-D object from hollow to solid, you add a surface to the wireframe (Figure 6-35b). Some 3-D graphics are composed of more than one wireframe. When adding a surface, it is important to make the object look as realistic as possible by adding color, texture, and reflectance. Reflectance refers to the amount of light the object's surface reflects.
With the surface added to a wireframe, you next consider how the object will be lit from one or more lighting sources. Some people create 3-D graphics using a technique called ray-tracing. Ray-tracing involves drawing an imaginary path that rays of light follow as they leave their source and then land on an object. The light intensity will be greater on some portions of the object and less on other portions. In addition, the object also might cast a shadow once it is lit from a particular angle.
When creating a 3-D world, the next considerations are perspective and depth of field. Perspective refers to differences in how objects appear in relation to one another when they are close to you, versus farther away. Objects appearing close may seem to be spaced apart. As they move farther away from you, they become closer to one another. A technique for calculating which objects appear in front of or behind one another is called the Z-Buffer, named after the imaginary axis from the screen to the distant horizon. Depth of field gives the appearance that objects farther from you are less focused than closer objects.
Anti-aliasing is the final technique in creating 3-D objects that appear in a 3-D world. Anti-aliasing makes curved and diagonal lines appear straight. When computers render graphics with curved and diagonal lines, they often appear jagged. Anti-aliasing inserts additional colored pixels that give the appearance of a smooth edge. All these techniques combined create a realistic 3-D graphic (Figure 6-35c).
The complex nature of 3-D technology requires more computing power in order to render a graphic in an acceptable period of time. For example, computer gamers often buy computers designed for gaming so that a lack of performance does not slow their game. Gaming computers often have faster processors, several gigabytes of RAM, and one or more video cards containing at least 256 MB of RAM. These video cards also might support DirectX, which is a programming interface that allows game programmers direct access to enhanced hardware features. For some computer games to work properly, they require a video card that supports a specific version of DirectX. For example, if a game is programmed using the DirectX 11 standard, the video card also must support DirectX 11 for the game to work.
Although game programmers spend many hours creating 3-D graphics for programs such as computer games, the results are rewarding when a player faces an experience so realistic that it is difficult to differentiate between the game and reality.

For more information, visit scsite.com/ dc2011/ch6/tech and then click 3-D Graphics.

High-Tech Talk
DNS Servers: How Devices on the Internet Easily Locate Each Other

Domain name system (DNS) servers, also called name servers, play an important role for Internet users who visit Web sites and send e-mail messages. DNS is a service on the Internet that converts domain names into Internet protocol (IP) addresses. Recall that a domain name is the text version of an IP address; for example, www.google.com is the domain name for the IP address of 72.14.207.99. Because the DNS stores IP addresses for each domain name, it is one of the largest databases stored across servers worldwide. In fact, some view DNS databases as nothing more than large address books. The absence of DNS servers would require users to remember IP addresses for Web sites. To visit a Web site on the Internet, you begin by starting a Web browser and typing the Web address (which includes a domain name) in the Address bar. Once you press the FOUFS key, the Web browser initiates a request for the IP address associated with the Web address. If the DNS server on your network or your Internet access provider's network knows the IP address, it will answer the request. Otherwise, it will ask another DNS server for this information or return an error message indicating that the domain name does not exist. If a DNS server is able to return an IP address to the Web browser, the Web browser contacts the Web server located at that IP address and requests a Web page. In some cases, DNS servers cache IP addresses for frequently requested domain names for a specified period of time, called the Time To Live (TTL). Because IP addresses are cached for certain domain names, it can take several days or more for updates to be reflected on DNS servers worldwide. For example, if the google.com Web server (accessible at www.google.com) is replaced with a new Web server with a new IP address, it might take several days for other DNS servers to acquire the new IP address.

If a DNS server does not know the IP address for a requested domain name, it will contact a root name server. A root name server stores a list of IP addresses for all DNS servers that handle a specific top-level domain, such as com or edu. For example, if you are attempting to reach www.google.com and your DNS server does not know the IP address, the root name server forwards the request to one of the DNS servers that handle the top-level domain of com. Your request will travel from one root server to the next until one can fulfill it. At that time, it requests the IP address associated with the Web address – in this case, www.google.com – from the COM root name server. Figure 7-41 illustrates a simple example of a DNS request.

The DNS has built-in redundancy. Network administrators typically set up multiple DNS servers on their network so that if one becomes overburdened or stops functioning, the other one(s) can continue filling requests. Similarly, multiple root name servers exist for each top-level domain.

Domain name servers also play an important role in e-mail communications. If you send an e-mail message to kbarnhill@scsite .com, the DNS servers will locate the mail exchange (MX) record for the scsite.com domain. The MX record identifies the location, or IP address, of the SMTP server accepting e-mail messages.

DNS servers often process billions of requests each day; each time you send an e-mail message or view a Web site, you are creating a request for a DNS server. While the average user might generate around 20 requests each day, those who primarily work with computers may generate hundreds of requests per day. Consequently, the millions of users connected to the Internet at any given time are generating billions of DNS requests each day.

For more information, visit scsite.com/ dc2011/ch7/tech and then click DNS Servers.

High-Tech Talk
Touch Screen Technology: How the Screen Is So Smart

Touch screen technology is becoming a larger part of everyday life for many individuals. As presented in Chapter 5, a touch screen is a touch-sensitive display device that users can interact with by touching areas of the screen. People have been using touch screens for more than 30 years, and this technology now is being used in more places, such as in smart phones, point-of-sale terminals, automated teller machines, remote controls, GPS receivers, home security systems, and Tablet PCs.
Touch screen technology has evolved since its creation in the late 1960s. The first touch screens developed allowed users to press only one area at a time with the tip of their finger, and they were much less accurate than today's touch screens. As the technology is advancing, users are able to perform additional tasks, such as dragging their finger across the screen and touching more than one area of the screen at a time. For example, the iPhone and iPod touch allow you to zoom in pictures or other objects on the screen by placing two fingers close together on the screen, and then slowly moving them apart. Three types of touch screens most in use today are capacitive, resistive, and surface wave touch screens.
A capacitive touch screen has a layer of material that stores electrical charges coating the surface. When a finger touches the screen, it conducts a small amount of the electrical charge, reducing the charge on the capacitive layer. Circuits located at each corner of the capacitive touch screen measure the change in electrical charge. The circuits then send this data to the touch screen controller, or software that is running on the computer. The controller then uses the data to calculate the location where the finger is touching the screen. Capacitive touch screens typically are high-quality and unaffected by items that do not conduct electrical charges. An example of the components of a capacitive touch screen is shown in Figure 8-41.
The second type of touch screen is a resistive touch screen. A metallic conductive and resistive layer held apart by spacers cover a resistive touch screen. When a user touches a resistive touch screen, the conductive and resistive layers connect in the location of the touch. An electronic current runs between the two layers, and the interruption in the current enables the touch screen controller to calculate the exact location of the touch. Although resistive touch screens usually are more affordable than capacitive touch screens, they are not as clear and can be damaged more easily.
The third type of touch screen uses surface wave technology. Surface wave technology passes ultrasonic waves over the touch screen. Touching the screen absorbs portions of the waves, which then allows the touch screen controller to calculate the position at which the object touched the screen. Because ultrasonic waves pass over the touch screen, it is easy for outside elements to damage the device. Touch screens using surface wave technology are the most advanced and often the most expensive of the three types.
Additional types of touch screen technologies exist, but they are not used as widely as the capacitive, resistive, and surface wave touch screens. Optical touch screens use cameras mounted at two corners of the screen to detect objects close to the surface. Infrared touch screens use light emitting diodes and light detectors at the edges of the touch screen to detect objects that break the beams of light traveling across the screen.
As touch screen prices continue to decrease, they most likely will be incorporated in an increasing number of computers and devices. Touch screens have increased productivity by allowing people to interact with devices more quickly than they can with a mouse or keyboard.

For more information, visit scsite.com/ dc2011/ch8/tech and then click Touch Screen Technology.

High-Tech Talk
OSI Reference Model: The Driving Force behind Network Communications

Every message sent over a network — even the simplest e-mail message — must be divided into discrete packages of data and routed via transmission media such as telephone lines. While traveling from the sending computer to the receiving computer, each data package can take a different path over the network. How do these messages get to their destination, intact and accurate?

The Open Systems Interconnection (OSI) reference model, a communications standard developed by the International Organization for Standardization (ISO), offers an answer. The OSI reference model describes the flow of data in a network through seven layers, from the user's application to the physical transmission media.

A simple way to understand the OSI reference model is to think of it as an elevator (Figure 9-43). On the sending end, data enters at the top floor (the application layer) and travels to the bottom floor (the physical layer). Each layer communicates with the layers immediately above and below it. When a layer receives data, it performs specific functions, adds control information to the data, and passes it to the next layer. The control information contains error-checking, routing, and other information needed to ensure proper transmission along the network.

The top layer, the application layer, serves as the interface between the user and the network. Using application software, such as an e-mail program, a user can type a message and specify a recipient. The application then prepares the message for delivery by converting the message data into bits and attaching a header identifying the sending and receiving computers.

The presentation layer translates the converted message data into a language the receiving computer can process (from ASCII to EBCDIC, for example) and also may compress or encrypt the data. Finally, the layer attaches another header specifying the language, compression, and encryption schemes.

The next layer, called the session layer, establishes and maintains communications sessions. A session is the period between establishment of a connection, transmission of the data, and termination of the connection.

The transport layer, also called the end-toend layer, ensures that data arrives correctly and in proper sequence. The transport layer divides the data into segments and creates a checksum, a mathematical sum based on the data, and puts this information in the transport header. The checksum later is used to determine if the data was scrambled during transmission.

The network layer routes the message from sender to receiver. This layer splits the data segments from the transport layer into smaller groups of bits called packets. Next, it adds a header containing the packet sequence, the receiving computer address, and routing information. The network layer also manages network problems by rerouting packets to avoid network congestion.

The data link layer supervises the transmission of the message to the next network node by specifying the network technology (such as Ethernet or token ring) and grouping data accordingly. The data link layer also calculates the checksum and keeps a copy of each packet until it receives confirmation that the packet arrived undamaged at the next node.

Finally, the physical layer encodes the packets into a signal recognized by the medium that will carry them — such as an analog signal to be sent over a telephone line — and sends the packets along that medium to the receiving computer.

At the receiving computer, the process is reversed and the data moves back through the seven layers from the physical layer to the application layer, which identifies the recipient, converts the bits into readable data, removes some of the error-checking and control information from the data, and directs it to the appropriate application. A modified 5-layer model is used for data sent using the Transmission Control Protocol (TCP) and/or the Internet Protocol (IP). This model includes the physical, data link, network, transport, and application layers. The next time you send an e-mail message to a friend, consider the network communications processes described by the OSI reference model, which ensure that your message travels safely over many networks to your friend's computer.

For more information, visit scsite.com/ dc2011/ch9/tech and then click OSI Reference Model.

High-Tech Talk
Normalization: Ensuring Data Consistency

Normalization organizes a database into one of several normal forms to remove ambiguous relationships between data and minimize data redundancy. In zero normal form (0NF), the database is completely nonnormalized, and all of the data fields are included in one relation or table. Repeating groups are listed within parentheses (Figure 10-26a). The table has large rows due to the repeating groups and wastes disk space when an order has only one item.

To normalize the data from 0NF to 1NF (first normal form), you remove the repeating groups (fields 3 through 7 and 8 through 12) and place them in a second table (Figure 10-26b). You then assign a primary key to the second table (Line Item), by combining the primary key of the nonrepeating group (Order #) with the primary key of the repeating group (Product #), called a composite key. Primary keys are underlined to distinguish them from other fields.

To further normalize the database from 1NF to 2NF (second normal form), you remove partial dependencies. A partial dependency exists when fields in the table depend on only part of the primary key. In the Line Item table (Figure 10-26b), Product Name is dependent on Product #, which is only part of the primary key. Second normal form requires you to place the product information in a separate Product table to remove the partial dependency (Figure 10-26c).

To move from 2NF to 3NF (third normal form), you remove transitive dependencies. A transitive dependency exists when a nonprimary key field depends on another nonprimary key field. As shown in Figure 10-26c, Vendor Name is dependent on Vendor #, both of which are nonprimary key fields. If Vendor Name is left in the Line Item table, the database will store redundant data each time a product is ordered from the same vendor.

Third normal form requires Vendor Name to be placed in a separate Vendor table, with Vendor # as the primary key. The field that is the primary key in the new table — in this case, Vendor # — also remains in the original table as a foreign key and is identified by a dotted underline (Figure 10-26d). In 3NF, the database now is logically orga nized in four separate tables and is easier to maintain. For instance, to add, delete, or modify a Vendor or Product Name, you make the change in just one table.

For more information, visit scsite.com/ dc2011/ch10/tech and then click Normalization.

High-Tech Talk
Encryption Algorithms: The Brains behind Encryption

As mentioned in this chapter, encryption is a process of converting readable data into unreadable characters to prevent unauthorized access. Various encryption algorithms are used to encrypt data, with some more secure than others. The chapter showed a few simple encryption algorithms. Individuals and organizations often desire more secure encryption, which requires a complex encryption algorithm. Thousands of encryption algorithms exist, and it even is possible to write your own. Commonly used secure encryption algorithms include Blowfish, DES, 3DES, and IDEA.

The Blowfish encryption algorithm was introduced in 1993 as a free alternative to other encryption algorithms that were available at that time. Blowfish, which has been thoroughly tested since its development and has proven to be a strong algorithm, uses a key length varying between 32 and 448 bits and is applied to a block of data as opposed to single bits of data.

The DES (Data Encryption Standard) encryption algorithm in the late 1970s was developed by the United States government and IBM. This standard uses a 56-bit key to encrypt 64-bit blocks of data at a time. The encryption process requires that each block of the message go through 16 different stages, adding to the strength of the algorithm. Advancements in technology, however, made it easier and faster for computers with increased processing capabilities to decrypt these 56-bit keys, which were only 7 characters long. As a result, the Triple-DES (3DES) encryption algorithm was developed. This algorithm uses the original Data Encryption Standard to encrypt the data with the first 56-bit key and then decrypts the data with another 56-bit key. Finally, a third 56-bit key encrypts the data once again. This process creates a total key length of 168 bits, which is significantly more difficult to compromise.

IDEA (International Data Encryption Algorithm) was developed in the early 1990s to replace the DES encryption algorithm. This algorithm uses the same key for encryption and decryption on blocks of data that are 64 bits long. Unlike the DES algorithm, IDEA uses a 128-bit key, greatly increasing the complexity and security of the encrypted data.

The U.S. government uses the Advanced Encryption Standard (AES), mostly for unclassified data. In addition, various other organizations use AES. Windows 7 Ultimate edition includes BitLocker Drive Encryption (Figure 11-38), a security feature using the Encrypting File System (EFS) to encrypt data. EFS uses the Advanced Encryption Standard to protect files and data from almost any method of unauthorized access. When a user encrypts a file, EFS generates a random number for the file that EFS calls the file's FEK (file encryption key) to encrypt the data. EFS then uses FEK to encrypt the file's contents with the encryption algorithm. The user's public key then encrypts the FEK using the RSA public-key-based encryption algorithm, and the encrypted FEK then is stored with the file. The entire encryption process happens behind the scenes for the user, who simply completes a few mouse clicks to encrypt a folder or file. That is part of the elegance of EFS: while it is simple for a user, it is very difficult for any unauthorized user without the correct keys to crack the encryption. In the end, that is the key to keeping your data safe and sound.

For more information, visit scsite.com/ dc2011/ch11/tech and then click Encryption Algorithms.

High-Tech Talk
Benchmarking: Testing Performance through Calculations

A benchmark is a surveyor's reference mark — a point of reference from which other measurements can be made. Benchmarking is used to evaluate various aspects of enterprises and is widely used in computer technology. Additional types of benchmarking exist, such as process benchmarking and performance benchmarking. In computer technology, a benchmark is a set of conditions used to measure the performance of hardware or software. Benchmark testing involves running a set of standard tests to compare the performance of two or more systems. Web sites and programs are available that can perform simple benchmark tests against parameters such as the speed of your computer's processor or the speed of your Internet connection. The computer industry, however, uses far more complex benchmark tests.

Suppose you are a network administrator and need to buy new servers to support your organization's e-commerce Web site. To start, you can access published benchmark results from organizations such as SPEC and TPC. Both SPEC (Standard Performance Evaluation Corporation) and TPC (Transaction Processing Performance Counsel) are nonprofit groups that define and maintain benchmarks for the computer industry. TPC, for example, tests using its TPC Benchmark W (TPC-W), which measures how servers perform while supporting an e-commerce Web site. Reading published benchmark test results from these groups can help you determine how one vendor's system might perform relative to another.

To understand benchmark results fully, you should understand the design and measurements (or metrics) used for the test. The TPC-W benchmark, for example, uses two primary metrics: WIPS and $/WIPS. WIPS is the number of Web Interactions Per Second that can be sustained by the system under test, or SUT (in this case, multiple servers). The $/WIPS is the system cost per WIPS, which is the total cost of the SUT divided by WIPS.

To calculate WIPS, TPC-W uses several algorithms, or formulas (Figure 12-23). One calculation is Web Interaction Response Time (WIRT), which is the time it takes to complete a Web interaction. A Web interaction might start when a user clicks a link to request a Web page and ends when the browser receives all of the data from the requested page. WIRT is calculated using the algorithm shown in Figure 12-23. Using this algorithm, if a Web interaction starts at 1:00:00 and the last byte of data is sent at 1:00:07, the WIRT is 7 seconds.

WIRT is used to calculate the number of Web interactions successfully completed during the length of the benchmark test, or measurement interval. During the measurement interval, the browser repeatedly cycles through requesting and then receiving a requested page, measuring the time to receive it (WIRT), and then requesting the next page. To be considered a successful Web interaction, each type of Web interaction must have a WIRT less than the TPC-specified constraint. For example, a home page Web interaction must have a WIRT of less than three seconds or it is not used when calculating WIPS.

The total number of successful Web interactions completed in a measurement interval is used to calculate WIPS. WIPS is calculated using the algorithm shown in Figure 12-23. Using this algorithm, if 14,009,400 Web interactions are completed successfully during a 30-minute test period, the WIPS rating for the system is 14,009,400/1,800 or 7,783 WIPs. The higher the WIPs rating, the more requests the Web server can handle per second.

The $/WIPS rating is determined by dividing the price of the SUT by the WIPS value (Figure 12-23). Using this algorithm, if a system rated as 7,783 WIPS costs $190,036, the $/WIPS rating is $190,036/7,783 or 24.42.

The TPC-W benchmark also measures the total number of connections a Web server can handle. Using the algorithm shown in Figure 12-23, if a Web site supports 35,000 browsers using 10 Web servers, each Web server is supporting 2 * (35,000/10), or 7,000 connections.

Data points such as WIPS, $/WIPS, and number of connections are the result of a benchmarking process. These data points provide the detailed information required to make informed purchasing decisions. For example, the WIPS and $/WIPS ratings in a benchmark report can help you better understand how the servers will perform in the real-world environment of your e-commerce Web site.

The TPC-W benchmark is just one of numerous industry benchmarks used to test different aspects of systems' performance.

For more information, visit scsite.com/ dc2011/ch12/tech and then click Benchmarking.

High-Tech Talk
Acid3 Browser Test: Verifying Standards Support

Each day, people work to develop new technologies intended to enhance a user's Web browsing experience by creating more dynamic and interactive Web pages. Simultaneously, companies such as Microsoft, Mozilla, and Google work to create new Web browser versions that include features designed to help people search and browse the Web more efficiently. In addition to providing new and exciting features with each release, new Web browsers also should support new technologies that Web developers are including in Web pages and Web applications. As presented earlier in the book, each Web browser might display a Web page with slight differences. For example, the top margin on a Web page might be twice as thick in Internet Explorer as it is in Firefox. While this might not seem significant, positioning Web page elements accurately often is necessary to display information properly, in the manner that the Web developer intends. For this reason, The Web Standards Project has created a series of test pages designed to inform users whether their browser supports certain Web technologies. In 1998, The Web Standards Project developed Acid1, the first in the series of three tests designed to test a Web browser's interpretation of the first version of basic HTML and cascading style sheets (CSS1). In 2005, The Web Standards Project introduced the Acid2 test, which tested Web standards such as CSS positioning, CSS table formatting, and hovering effects. Throughout the past several years, new Web technologies have led companies to develop new versions of their Web browsers more frequently. The Web Standards Project released the Acid3 Browser Test in early 2008. During an Acid3 Browser Test, the Web browser displays a percentage counter that gradually increases. When the counter reaches 100 and displays a page similar to the one in Figure 13-40, it is an indication that the browser has passed the test.

The Acid3 Browser Test uses JavaScript to perform approximately 100 subtests. These subtests evaluate how the Web browser interprets newer Web technologies such as DOM2, ECMAScript, Media Queries, Selectors, XHTML, CSS2, CSS2.1, CSS3, and Standard Vector Graphics (SVG). To perform an Acid3 Browser Test using a Web browser, you first should ensure that the Web browser is configured with the default settings. If you have changed settings such as the default font, view, or zoom, you should return them to their original settings before performing the test. Failure to do so might result in incorrect test results. Once the browser is configured with the default settings, type http://acid3.acidtests.org in the Address bar and then press the ENTER key. A Web page then will display with a counter beginning at zero. The counter slowly increments as the tests are performed. The counter's value increasing is indicative of the Web browser passing additional subtests. If the counter stops for more than a few seconds, does not increment smoothly, or the graphic on the screen is not arranged similarly to Figure 13-40, the Web browser has not passed the Acid3 Browser Test. If the browser does not pass the test, you first should make sure that you are using the most recent version of the Web browser and that you have downloaded and installed all updates and security patches. You also should ensure that the Web browser is performing the test with its default settings.

The Acid3 Browser Test is one of the only tests that comprehensively measures compliance with many current Web standards. If ever you must decide which Web browser to use, consider the one that passes, or comes closest to passing, the Acid3 Browser Test.

For more information, visit scsite.com/ dc2011/ch13/tech and then click Acid3 Browser Test.

High-Tech Talk
Neural Networks: Learning from Experience

A neural network is a type of artificial intelligence system that attempts to emulate the way the human brain works. Neural networks are named after neurons, which are the billons of cells in the human brain that perform intelligent operations. Each neuron is like a small computer with basic capabilities. When billions of neurons are connected together, however, these cells are the intellectual capacity in the human brain, the most intelligent system known.

Neural networks are modeled on the human brain. A neural network uses an interconnected system of hundreds or thousands of specially designed circuits, also called artificial neurons. Like the brain's neurons, these circuits are connected together. Neural networks also are called artificial neural networks (ANNs) to differentiate the network of artificial neurons from the network of biological neurons in the human brain.

A neural network uses these circuits to create connections between inputs and outputs. The most common neural network model is the multilayer perceptron (MLP), which consists of at least three layers of circuits: a layer of input circuits, which is connected to one or more layers of hidden circuits, which are connected to a layer of output circuits (Figure 14-35). The knowledge of a neural network is housed in the hidden layers, which store the information that defines relationships between inputs and outputs.

Just as people do, neural networks learn from experience. Some neural networks are trained using a process called backpropagation, as shown in Figure 14-35. During backpropagation, the input data, which is the information used to make a decision, repeatedly is presented to the neural network via the input layer. The neural network then generates an output, which is the resulting decision, prediction, or response, based on the weighted connections between the inputs and outputs, as stored in the hidden layers.

The output of the neural network then is compared with the desired output, and the error is calculated based on historical or known data. This error then is fed back, or backpropagated, to the hidden layer to adjust the weights of the connection. During each repetition, the neural network learns to associate the weight of the relationship between certain inputs and outputs. It then adjusts the weights of the connections between the inputs and outputs accordingly. The hidden layers thus store a neural network's knowledge as weighted connections between inputs and outputs, which are known as synaptic weights. As training continues, the extent of the error decreases with each iteration, until the neural network reaches a fully trained state where it reliably produces the desired output. The neural network then is ready to produce outputs when the desired output is unknown.

Unlike humans, once trained fully, a neural network recognizes and classifies patterns in huge quantities of complex data, at high speeds that humans cannot duplicate. Uses of neural networks include a wide range of applications, such as sorting mail at the U.S. Postal Service, determining the number of jurors to call at county courthouses, and identifying police officers with a potential for misconduct. Scientists use neural networks to predict rainfall and forecast air quality. Manufacturers benefit from neural networks that allow them to test the quality of plastics and welding and determine which type of concrete to use on a highway. In health care, neural networks help predict heart attacks and cancer risk, while helping to improve treatment.

For more information visit scsite.com/ dc2011/ch14/tech and then click Neural Networks.

Chapter 15 Computer Careers and Certification

High-Tech Talk
Bioinformatics: Technology Collides with Biology

Informatics, also referred to as information science, refers to the gathering, processing, storing, retrieving, and organizing of information. Informatics typically combines information technology or computer science with another area of study. As we use computers to collect massive amounts of data, we also must rely on them to process the data into meaningful information. Computers continually become more powerful, requiring only seconds to process data that otherwise might require several human years to process. In fact, the informatics field is exploding in popularity.
As mentioned previously, several specializations of informatics exist, each combining computer science with another field of study. These specializations include the combination of information technology with other fields such as molecular biology (bioinformatics), biomedical sciences (biomedical informatics), chemistry (chemoinformatics), ecology (ecoinformatics), geosciences (geoinformatics), health (health informatics), neuroscience (neuroinformatics), sociology (social informatics), and veterinary medicine (veterinary informatics).
Many colleges and universities now are offering an increasing number of courses in bioinformatics. Bioinformatics refers to computer applications in biological sciences where biologists use computers to analyze, store, or retrieve biological information. Bioinformatics research requires extensive collaboration between biologists and computer scientists. Essentially, biologists help the computer scientists understand the research study they would like to perform, and the computer scientists design programs to collect the data, process the data, and determine the results. Throughout this entire process, the biologists work closely with the computer scientists to ensure the accuracy of the data, its processing, and the output. Computer technology has assisted in analyzing the DNA sequence, advancing the study of molecular genetics.
One of the greatest accomplishments of bioinformatics might be the Human Genome Project. Scientists have used computers to map the complete set of the human genome in an effort to understand more fully specific aspects of human life (Figure 15-30). At one time, scientists were unable to determine scientifically why children resembled their parents. Currently, scientists can use the genes from two individuals and predict, with great accuracy, how their children will look. While 99.9 percent of DNA is identical in all humans, computers play a critical role in determining which DNA is different and how the DNA determines human characteristics such as height and hair color. Because diseases have a genetic component, bioinformatics also will use the information from the Human Genome Project to better understand diseases plaguing humans, as well as discover ways to prevent and/ or cure these diseases. Humans acquire diseases either through heredity or as a body's response to various environmental conditions. Understanding the human genome in greater detail can assist scientists in determining exactly which genes contribute to inherited diseases and possibly provide a way to prevent these genes from passing to future generations.
In addition to assisting with disease treatment and prevention, bioinformatics and knowledge of the human genome can help advance clinical medicine. An individual's genetic makeup determines both his or her physical characteristics and how his or her body might respond to certain medications and treatments. Many medications are developed that affect only a small percentage of people; thus, they never make it to pharmacy shelves. For a medication to be approved for the market, it must be effective on a wide range of individuals. Scientists can use knowledge of the similarities in the genetic characteristics of all humans to aid in developing medications that will be widely effective.
Bioinformatics, although a relatively new field, has helped us to learn much more about human life. Improvements in technology and the rate at which this field is gaining popularity might help scientists soon explain phenomenon that have mystified humans for hundreds of years.

For more information, visit scsite.com/ dc2011/ch15/tech and then click Bioinformatics.