chapter 28

Printers

"Faster! Faster! Faster would be better!"

—Capt. Malcolm Reynolds, *Serenity*

In this chapter, you will learn how to

- **Describe current printer technologies**
- **Explain the laser printing process**
- **Install a printer on a Windows PC**
- **Recognize and fix basic printer problems**

Despite all of the talk about the "paperless office," printers continue to be a vital part of the typical office. In many cases, PCs are used exclusively for the purpose of producing paper documents. Many people simply prefer dealing with a hard copy. Programmers cater to this preference by using metaphors such as *page*, *workbook*, and *binder* in their applications. The CompTIA A+ certification strongly stresses the area of printing and expects a high degree of technical knowledge of the function, components, maintenance, and repair of all types of printers.

Printer Technologies

No other piece of your computer system is available in a wider range of styles, configurations, and feature sets than a printer, or at such a wide price variation. What a printer can and can't do is largely determined by the type of printer technology it uses—that is, how it gets the image onto the paper. Modern printers can be categorized into several broad types: impact, inkjet, dye-sublimation, thermal, laser, and solid ink.

Impact Printers

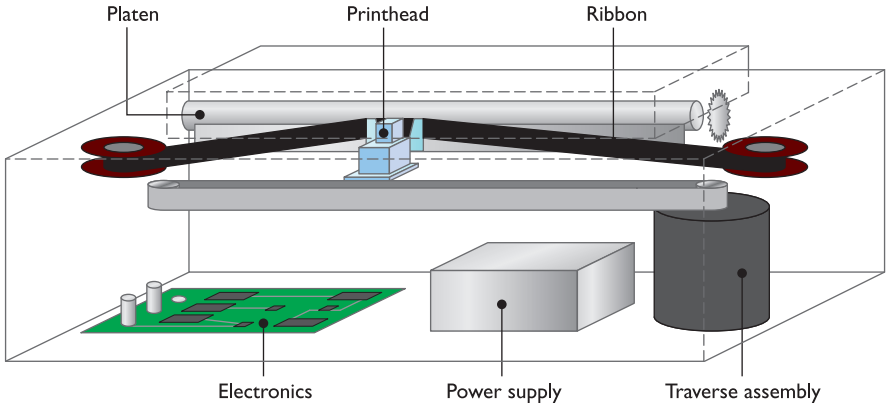
Printers that create an image on paper by physically striking an ink ribbon against the paper's surface are known as **impact printers**. Although *daisy-wheel* printers (essentially an electric typewriter attached to the PC instead of directly to a keyboard) have largely disappeared, their cousins, **dot-matrix printers**, still soldier on in many offices. Although dot-matrix printers don't deliver what most home users want—high quality and flexibility at a low cost—they're still widely found in businesses for two reasons: dot-matrix printers have a large installed base in businesses, and they can be used for multipart forms because they actually strike the paper. Impact printers tend to be relatively slow and noisy, but when speed, flexibility, and print quality are not critical, they provide acceptable results. PCs that print multipart forms, such as *point of sale* (*POS*) machines, use special *impact paper* that can print receipts in duplicate, triplicate, or more. These POS machines represent the major market for new impact printers, although many older dot-matrix printers remain in use.

Dot-matrix printers use a grid, or matrix, of tiny pins, also known as **printwires**, to strike an inked printer ribbon and produce images on paper (see Figure 28.1). The case that holds the printwires is called a **printhead**. Using either 9 or 24 pins, dot-matrix printers treat each page as a picture broken up into a dot-based raster image. The 9-pin dot-matrix printers are generically called *draft quality*, while the 24-pin printers are known as *letter quality* or **near-letter quality (NLQ)**. The BIOS for the printer (either built into the printer or a printer driver) interprets the raster image in the same way a monitor does, "painting" the image as individual dots. Naturally, the more pins, the higher the resolution. Figure 28.2 illustrates the components common to dot-matrix printers. Many dot-matrix printers use continuous-feed paper with holes on its sides that are engaged by metal sprockets to pull the paper through—this is known as *tractor-feed paper* because the sprockets are reminiscent of the wheels on a tractor.

Figure 28.1 An Epson FX-880+ dot-matrix printer (photo courtesy of Epson America, Inc.)

Inkjet Printers

Inkjet printers (also called *ink-dispersion printers*) like the one in Figure 28.3 are relatively simple devices. An inkjet printer uses a *printhead* connected to a *carriage* that contains the ink. A belt and motor move the carriage back



• **Figure 28.2** Inside a dot-matrix printer

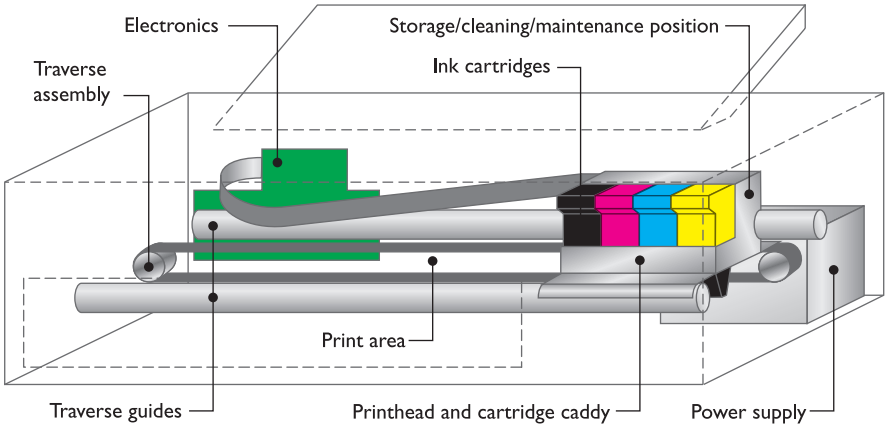
Printers can also use *duplex assemblies*, which enable the printer to print automatically on both sides of the paper. Some printers include this feature built-in, while others require a piece of additional hardware that flips the paper for the printer.

• **Figure 28.3** Typical inkjet printer

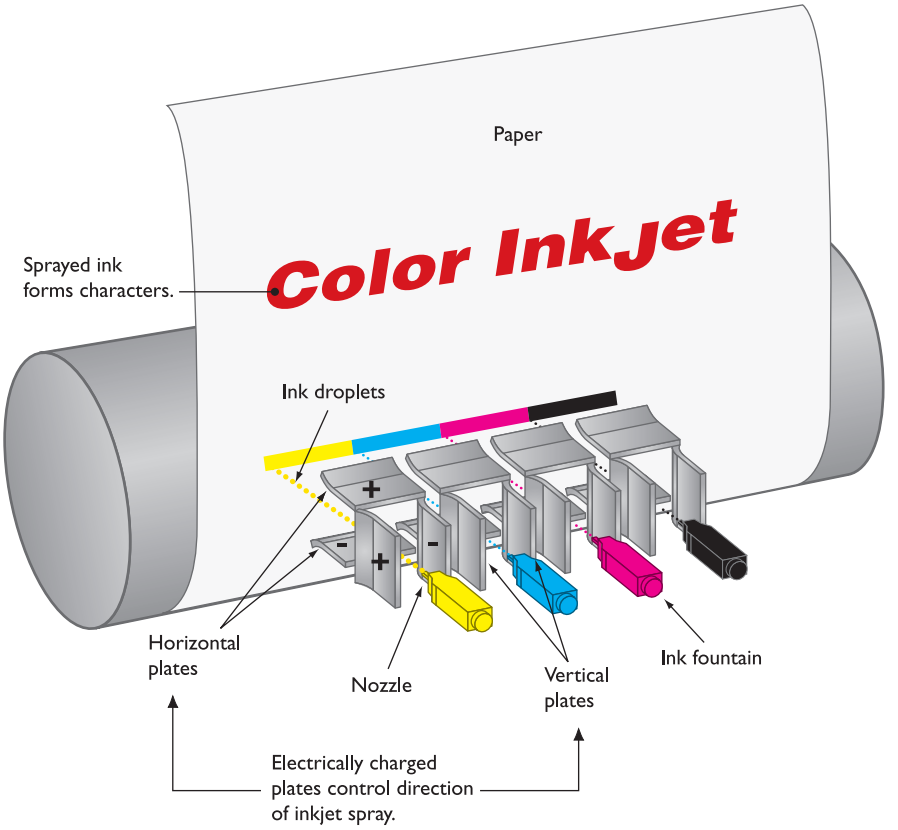
and forth so the ink can cover the whole page. A *roller* grabs paper from a paper tray (usually under or inside the printer) or feeder (usually on the back of the printer) and advances it through the printer (see Figure 28.4).

The ink is ejected through tiny tubes. Most inkjet printers use heat to move the ink, while a few use a mechanical method. The heat-method printers use tiny resistors or electroconductive plates at the end of each tube that literally boil the ink; this creates a tiny air bubble that ejects a droplet of ink onto the paper, thus creating a portion of the image (see Figure 28.5).

The ink is stored in special small containers called **ink cartridges**. Older inkjet printers had two cartridges: one for black ink and another for colored ink. The color cartridge had separate compartments for cyan (blue), magenta (red), and yellow ink, to print colors by using a method known as CMYK (you'll read more about CMYK later in this chapter). If your color cartridge ran out of one of the colors, you had



• **Figure 28.4** Inside an inkjet printer



• **Figure 28.5** Detail of the inkjet printhead

to purchase a whole new color cartridge or deal with a messy refill kit.

Printer manufacturers began to separate the ink colors into three separate cartridges so that printers came with four cartridges: one for each color and a fourth for black (see Figure 28.6). This not only was more cost-effective for the user, but it also resulted in higher quality printouts. Today you can find color inkjet printers with six, eight, or more color cartridges. In addition to the basic CMYK inks, the other cartridges provide for green, blue, gray, light cyan, dark cyan, and more. Typically, the more ink cartridges a printer uses, the higher the quality of the printed image—and the higher the cost of the printer.

• **Figure 28.6** Inkjet ink cartridges

The two key features of an inkjet printer are the **print resolution**—that is, the density of ink, which affects print quality—and the print speed. Resolution is measured in **dots per inch (dpi)**; higher numbers mean that the ink dots on the page are closer together, so your printed documents will look better. Resolution is most important when you're printing complex images such as full-color photos, or when you're printing for duplication and you care that your printouts

Print resolution is measured in dots per inch (dpi) and print speed is measured in pages per minute (ppm).

look good. Print speed is measured in **pages per minute (ppm)**, and this specification is normally indicated right on the printer's box. Most printers have one (faster) speed for monochrome printing—that is, using only black ink—and another for full-color printing.

Another feature of inkjet printers is that they can support a staggering array of print media. Using an inkjet printer, you can print on a variety of matte or glossy photo papers, iron-on transfers, and other specialty media; some printers can print directly onto specially coated optical discs, or even fabric. Imagine running a T-shirt through your printer with your own custom slogan (how about "I'm CompTIA A+ Certified!"). The inks have improved over the years, too, now delivering better quality and longevity than ever. Where older inks would smudge if the paper got wet or start to fade after a short time, modern inks are smudge proof and of archival quality—for example, some inks by Epson are projected to last up to 200 years.

Try This!

Pages per Minute Versus Price

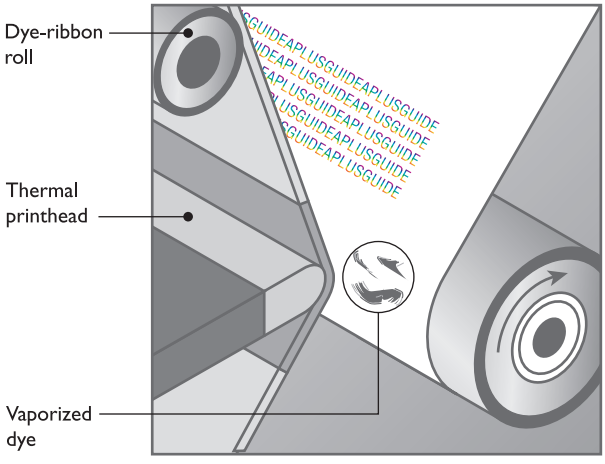
Printer speed is a key determinant of a printer's price, and this is an easy assertion to prove, so Try This!

1. Fire up your browser and head over to the Web site for Hewlett-Packard (www.hp.com), Canon (www.usa.canon.com), Epson (www.epson.com), or Lexmark (www.lexmark.com). These four companies make most of the printers on the market today.
2. Pick a particular printer technology and check the price, from the cheapest to the most expensive. Then look for printers that have the same resolution but different ppm rates.
3. Check the prices and see how the ppm rate affects the price of two otherwise identical printers.

Dye-Sublimation Printers

The term *sublimation* means to cause something to change from a solid form into a vapor and then back into a solid. This is exactly the process behind *dye-sublimation printing*, sometimes called *thermal dye transfer* printing. **Dye-sublimation printers** are used mainly for photo printing, high-end desktop publishing, medical and scientific imaging, and other applications for which fine detail and rich color are more important than cost and speed. Smaller, specialized printers called *snapshot* printers use dye-sublimation specifically for printing photos at a reduced cost compared to their full-sized counterparts.

The dye-sublimation printing technique is an example of the so-called CMYK (**c**yan, **m**agenta, **y**ellow, blac**k**) method of color printing. It uses a roll of heat-sensitive plastic film embedded with page-sized sections of cyan (blue), magenta (red), and yellow dye; many also have a section of black dye. A printhead containing thousands of heating elements, capable of precise temperature control, moves across the film, vaporizing the dyes and causing them to soak into specially coated paper underneath before cooling and reverting to a solid form. This process requires one pass per page for each color. Some printers also use a final finishing pass that applies a protective laminate coating to the page. Figure 28.7 shows how a dye-sublimation printer works.



• **Figure 28.7** The dye-sublimation printing process

Documents printed through the dye-sublimation process display *continuous-tone* images, meaning that the printed image is not constructed of pixel dots but a continuous blend of overlaid differing dye colors. This is in contrast to other print technologies' *dithered* images, which use closely packed, single-color dots to simulate blended colors. Dye-sublimation printers produce high-quality color output that rivals professional photo-lab processing.

Thermal Printers

Thermal printers use a heated printhead to create a high-quality image on special or plain paper. You'll see two kinds of thermal printers in use. The first is the *direct thermal* printer, and the other is the *thermal wax transfer* printer. Direct thermal printers use a heating element to burn dots into the surface of special heat-sensitive paper. If you remember the first generation of fax machines, you're already familiar with this type of printer. Many retail businesses still use it as a receipt printer, using large rolls of thermal paper housed in a feed assembly that automatically draws the paper past the heating element; some can even cut the paper off the roll for you.

Thermal wax printers work similarly to dye-sublimation printers, except that instead of using rolls of dye-embedded film, the film is coated with colored wax. The thermal printhead passes over the ribbon and melts the wax onto the paper. Thermal wax printers don't require special papers like dye-sublimation printers, so they're more flexible and somewhat cheaper to use, but their output isn't quite as good because they use color dithering.

Tech Tip

Hidden Costs

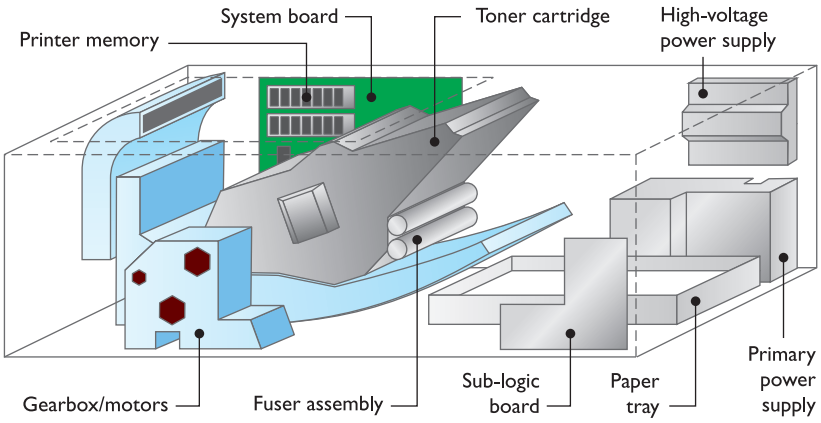
Some printers use consumables—such as ink—at a much faster rate than others, prompting the industry to rank printers in terms of their cost per page. Using an inexpensive printer (laser or inkjet) costs around 4 cents per page, while an expensive printer can cost more than 20 cents per page—a huge difference if you do any volume of printing. This hidden cost is particularly pernicious in the sub-$100 inkjet printers on the market. Their low prices often entice buyers, who then discover that the cost of consumables is outrageous—these days, a single *set of color and black inkjet cartridges can cost as much as the printer itself, if not more!*

Laser Printers

Using a process called *electro-photographic imaging*, **laser printers** produce high-quality and high-speed output of both text and graphics. Figure 28.8 shows a typical laser printer. Laser printers rely on the photoconductive properties of certain organic compounds. *Photoconductive* means that particles of these compounds, when exposed to light (that's the "photo" part), will *conduct* electricity. Laser printers usually use lasers as a light source because of their precision. Some lower-cost printers use LED arrays instead.

The first laser printers created only monochrome images. Today, you can also buy a color laser printer, although most laser printers produced today are monochrome. Although a color laser printer can produce complex full-color images such as photographs, they really shine for printing what's known as *spot color*—for example, eye-catching headings, lines, charts, or other graphical elements that dress up an otherwise plain printed presentation.

• **Figure 28.8** Typical laser printer



• **Figure 28.9** Components inside a laser printer

Critical Components of the Laser Printer

The CompTIA A+ certification exams take a keen interest in the particulars of the laser printing process, so it pays to know your way around a laser printer (see Figure 28.9). Let's take a look at the many components of laser printers and their functions.

Toner Cartridge The **toner cartridge** in a laser printer is so named because of its most obvious activity: supplying the toner that creates the image on the page (see Figure 28.10). To reduce maintenance costs, however, many other laser printer parts, especially those that suffer the most wear and tear, have been incorporated into the toner cartridge. Although this makes replacement of individual parts nearly impossible, it greatly reduces the need for replacement; those parts that are most likely to break are replaced every time you replace the toner cartridge.

Color laser printers have four toner cartridges: black, cyan, magenta, and yellow.

Photosensitive Drum The **photosensitive drum** (also called the *imaging drum*) is an aluminum cylinder coated with particles of photosensitive compounds. The drum itself is grounded to the power supply, but the coating is not. When light hits these particles, whatever electrical charge they may have "drains" out through the grounded cylinder.

Erase Lamp The **erase lamp** exposes the entire surface of the photosensitive drum to light, making the photosensitive coating conductive. Any electrical charge present in the particles bleeds away into the grounded drum, leaving the surface particles electrically neutral.

Primary Corona/Charge Roller The **primary corona** wire (or **primary charge roller**, in newer laser printers), located close to the photosensitive drum, never touches the drum. When the primary corona or primary charge roller is charged with an extremely high voltage, an electric field (or corona) forms, enabling voltage to pass to the drum and charge the photosensitive particles on its surface. The *primary grid* regulates the transfer of voltage, ensuring that the surface of the drum receives a uniform negative voltage of between ~600 and ~1000 volts.

• **Figure 28.10** Laser printer's toner cartridge

Laser The **laser** acts as the writing mechanism of the printer. Any particle on the drum struck by the laser becomes conductive and its charge is drained away into the grounded core of the drum. The entire surface of the drum has a uniform negative charge of between ~600 and ~1000 volts following its charging by the primary corona wire or charge roller.

When particles are struck by the laser, they are discharged and left with a ~100-volt negative charge. Using the laser, we can "write" an image onto the drum. Note that the laser writes a positive image to the drum.

Toner The **toner** in a laser printer is a fine powder made up of plastic particles bonded to iron particles. The *toner cylinder* charges the toner with a negative charge of between ~200 and ~500 volts. Because that charge falls between the original uniform negative charge of the photosensitive drum (~600 to ~1000 volts) and the charge of the particles on the drum's surface hit by the laser (~100 volts), particles of toner are attracted to the areas of the photosensitive drum that have been hit by the laser (that is, areas that have a *relatively* positive charge with reference to the toner particles).

The toner used in laser printers is typically carbon particles mixed with a polyester resin.

Transfer Corona/Transfer Roller To transfer the image from the photosensitive drum to the paper, the paper must be given a charge that will attract the toner particles off of the drum and onto the paper. In older printers, the **transfer corona**, a thin wire, applied a positive charge to the paper, drawing the negatively charged toner particles to the paper. Newer printers accomplish the same feat using a **transfer roller** that draws the toner onto the paper. The paper, with its positive charge, is also attracted to the negatively charged drum. To prevent the paper from wrapping around the drum, a **static charge eliminator** removes the charge from the paper.

In most laser printers, the transfer corona/roller is outside the toner cartridge, especially in large, commercial-grade machines. The transfer corona/roller is prone to a build-up of dirt, toner, and debris through electrostatic attraction, and it must be cleaned. It is also quite fragile—usually finer than a human hair. Most printers with an exposed transfer corona/roller provide a special tool to clean it, but you can also—very delicately—use a cotton swab soaked in 90 percent denatured alcohol (don't use rubbing alcohol because it contains emollients). As always, never service any printer without first turning it off and unplugging it from its power source.

Fuser Assembly The **fuser assembly** is almost always separate from the toner cartridge. It is usually quite easy to locate, as it is close to the bottom of the toner cartridge and usually has two rollers to fuse the toner. Sometimes the fuser is somewhat enclosed and difficult to recognize because the rollers are hidden from view. To help you determine the location of the fuser, think about the data path of the paper and the fact that fusing is the final step of printing.

The toner is merely resting on top of the paper after the static charge eliminator has removed the paper's static charge. The toner must be permanently attached to the paper to make the image permanent. Two rollers, a pressure roller and a heated roller, are used to fuse the toner to the paper. The pressure roller presses against the bottom of the page, and the heated roller presses down on the top of the page, melting the toner into the paper. The heated roller has a nonstick coating such as Teflon to prevent the toner from sticking to the heated roller.

Power Supplies All laser printers have at least two separate power supplies. The first power supply is called the primary power supply or sometimes just the power supply. This power supply, which may actually be more than one power supply, provides power to the motors that move

Cross Check

High Voltage—Keep Away!

The power supply inside a laser printer is not the only dangerous high-voltage toy in the world of PC equipment. You've learned about two other potentially hazardous electrical components that you should approach with caution.

1. What are they?
2. Which of these three items is potentially the most deadly?

To refresh your memory, check out Chapter 10 and Chapter 21.

the paper, the system electronics, the laser, and the transfer corona/roller. The high-voltage power supply usually provides power only to the primary corona/charge roller. The extremely high voltage of the high-voltage power supply makes it one of the most dangerous devices in the world of PCs! Before opening a printer to insert a new toner cartridge, it is imperative that you *always turn off* a laser printer!

Turning Gears A laser printer has many mechanical functions. First, the paper must be picked up. Next, the photosensitive roller must be turned and the laser, or a mirror, must be moved from left to right. The toner must be evenly distributed, and the fuser assembly must squish the toner into the paper. Finally, the paper must be kicked out of the printer and the assembly must be cleaned to prepare for the next page.

All of these functions are served by complex gear systems. In most laser printers, these gear systems are packed together in discrete units generically called *gear packs* or *gearboxes*. Most laser printers have two or three gearboxes that you can remove relatively easily in the rare case when one of them fails. Most gearboxes also have their own motor or solenoid to move the gears.

System Board Every laser printer contains at least one electronic board. On this board is the main processor, the printer's ROM, and the RAM used to store the image before it is printed. Many printers divide these functions among two or three boards dispersed around the printer (also known as sub-logic boards, as seen in Figure 28.9). An older printer may also have an extra ROM chip and/or a special slot where you can install an extra ROM chip, usually for special functions such as PostScript.

On some printer models, you can upgrade the contents of these ROM chips (the *firmware*) by performing a process called *flashing* the ROM. Flashing is a lot like upgrading the system BIOS, which you learned about in Chapter 8. Upgrading the firmware can help fix bugs, add new features, or update the fonts in the printer.

Of particular importance is the printer's RAM. When the printer doesn't have enough RAM to store the image before it prints, you get a memory overflow problem. Also, some printers store other information in the RAM, including fonts or special commands. Adding RAM is usually a simple job—just snapping in a SIMM or DIMM stick or two—but getting the *right* RAM is important. Call or check the printer manufacturer's Web site to see what type of RAM you need. Although most printer companies will happily sell you their expensive RAM, most printers can use generic DRAM like the kind you use in a PC.

Ozone Filter The coronas inside laser printers generate ozone (O_3). Although not harmful to humans in small amounts, even tiny concentrations of ozone will cause damage to printer components. To counter this

problem, most laser printers have a special ozone filter that needs to be vacuumed or replaced periodically.

Sensors and Switches Every laser printer has a large number of sensors and switches spread throughout the machine. The sensors are used to detect a broad range of conditions such as paper jams, empty paper trays, or low toner levels. Many of these sensors are really tiny switches that detect open doors and so on. Most of the time these sensors/switches work reliably, yet occasionally they become dirty or broken, sending a false signal to the printer. Simple inspection is usually sufficient to determine if a problem is real or just the result of a faulty sensor/switch.

Solid Ink

Solid ink printers use just what you'd expect—solid inks. The technology was originally developed by Tektronix, whose printer division was acquired by Xerox. Solid ink printers use solid sticks of nontoxic "ink" that produce more vibrant color than other print methods. The solid ink is melted and absorbed into the paper fibers; it then solidifies, producing a continuous-tone output. Unlike dye-sublimation printers, all colors are applied to the media in a single pass, reducing the chances of misalignment. Solid ink sticks do not rely on containers like ink for inkjet printers and can be "topped off" midway through a print job by inserting additional color sticks without taking the printer offline.

These printers are fast, too! A full-color print job outputs the first page in about six seconds. Of course, all that speed and quality comes at a price. Xerox's base model starts at about twice the cost of a laser printer, with the expensive model selling for about six times the cost! Solid ink printers become a bit more affordable when you factor in the cost of consumables. A single stick of ink costs about as much as an inkjet cartridge, for example, but with a print capacity of 1000 pages, that completely beats the cost of inkjet cartridges over time.

Printer Languages

Now that you've learned about the different types of print devices and techniques, it's time to take a look at how they communicate with the PC. How do you tell a printer to make a letter *A* or to print a picture of your pet iguana? Printers are designed to accept predefined printer languages that handle both characters and graphics. Your software must use the proper language when communicating with your printer, so that your printer can output your documents onto a piece of paper. Following are the more common printer languages.

ASCII

You might think of the **American Standard Code for Information Interchange (ASCII)** language as nothing more than a standard set of characters, the basic alphabet in upper- and lowercase with a few strange symbols thrown in. ASCII actually contains a variety of control codes for transferring data, some of which can be used to control printers. For example, ASCII code 10 (or 0A in hex) means "Line Feed," and ASCII code 12 (0C) means "Form

Feed." These commands have been standard since before the creation of IBM PCs, and all printers respond to them. Being highly standardized has advantages, but the control codes are extremely limited. Printing high-end graphics and a wide variety of fonts requires more advanced languages.

PostScript

Adobe Systems developed the **PostScript** page description language in the early 1980s as a device-independent printer language capable of high-resolution graphics and scalable fonts. PostScript interpreters are embedded in the printing device. Because PostScript is understood by printers at a hardware level, the majority of the image processing is done by the printer and not the PC's CPU, so PostScript printers print faster. PostScript defines the page as a single raster image; this makes PostScript files extremely portable—they can be created on one machine or platform and reliably printed out on another machine or platform (including, for example, high-end typesetters).

Hewlett-Packard Printer Control Language (PCL)

Hewlett-Packard developed its **printer control language (PCL)** as a more advanced printer language to supersede simple ASCII codes. PCL features a set of printer commands greatly expanded from ASCII. Hewlett-Packard designed PCL with text-based output in mind; it does not support advanced graphical functions. The most recent version of PCL, PCL6, features scalable fonts and additional line drawing commands. Unlike PostScript, however, PCL is not a true page description language; it uses a series of commands to define the characters on the page. Those commands must be supported by each individual printer model, making PCL files less portable than PostScript files.

Windows GDI and XPS

Windows XP uses the **graphical device interface (GDI)** component of the operating system to handle print functions. Although you *can* use an external printer language such as PostScript, most users simply install printer drivers and let Windows do all the work. The GDI uses the CPU rather than the printer to process a print job and then sends the completed job to the printer. When you print a letter with a TrueType font in Windows, for example, the GDI processes the print job and then sends bitmapped images of each page to the printer. The printer sees a page of TrueType text, therefore, as a picture, not as text. As long as the printer has a capable enough raster image processor (explained later in this chapter) and plenty of RAM, you don't need to worry about the printer language in most situations. We'll revisit printing in Windows in more detail later in this chapter.

Windows Vista and Windows 7 support GDI printing, but they also include a printing subsystem called the **XML Paper Specification (XPS) print path**. XPS provides several improvements over GDI, including enhanced color management (which works with Windows Color System) and better print layout fidelity. The XPS print path requires a driver that supports XPS. Additionally, some printers natively support XPS, eliminating the

requirement that the output be converted to a device-specific printer control language before printing.

Printer Connectivity

Most printers connect to one of two ports on the PC: a DB-25 parallel port or a USB port. The parallel connection is the classic way to plug in a printer, but most printers today use USB. You'll need to know how to support the more obscure parallel ports, cables, and connections as well as the plug-and-play USB connections.

Parallel Communication and Ports

The **parallel port** was included in the original IBM PC as a faster alternative to serial communication. The IBM engineers considered serial communication, limited to 1 bit at a time, to be too slow for the "high-speed" devices of the day (for example, dot-matrix printers). The standard parallel port has been kept around for backward compatibility despite several obvious weaknesses.

Parallel ports may be far faster than serial ports, but they are slow by modern standards. The maximum data transfer rate of a standard parallel port is still only approximately 150 kilobytes per second (KBps). Standard parallel communication on the PC also relies heavily on software, eating up a considerable amount of CPU time that could be used better.

Parallel ports are hindered by their lack of true bidirectional capability. Although one-way communication was acceptable for simple line printers and dot-matrix printers, parallel communication also became popular for a wide range of external devices that required two-way communication. Although it is possible to get two-way communication out of a standard parallel port, the performance is not impressive.

Many techs confuse the concept of duplex printing—a process that requires special printers capable of printing on both sides of a sheet of paper—with bidirectional printing. They are two different things!

IEEE 1284 Standard

In 1991, a group of printer manufacturers proposed to the *Institute of Electrical and Electronics Engineers* (*IEEE*) that a committee be formed to propose a standard for a backward-compatible, high-speed, bidirectional parallel port for the PC. The committee was the IEEE 1284 committee (hence the name of the standard).

The **IEEE 1284 standard** requires the following:

- Support for five distinct modes of operation: *compatibility mode*, *nibble mode*, *byte mode*, *EPP*, and *ECP*
- A standard method of negotiation for determining which modes are supported both by the host PC and by the peripheral device
- A standard physical interface (that is, the cables and connectors)
- A standard electrical interface (that is, termination, impedance, and so on)

Because only one set of data wires exists, all data transfer modes included in the IEEE 1284 standard are half-duplex: data is transferred in only one direction at a time.

Tech Tip

IEEE 1284 Transfer Modes

The five modes of operation for parallel printing specified in the IEEE 1284 standard (compatibility, nibble, byte, EPP, ECP) are inching closer to obsolescence as USB printers take over the market. If you find yourself needing to optimize the performance of a legacy parallel printer, you can look up these modes by name, using various Web search tools.

• **Figure 28.11** Standard parallel cable with 36-pin Centronics connector on one end and DB-25 connector on the other

Parallel Connections, Cabling, and Electricity

Although no true standard exists, *standard parallel cable* usually refers to a printer cable with the previously mentioned male **DB-25 connector** on one end and a 36-pin **Centronics connector** on the other (see Figure 28.11). The shielding (or lack thereof) of the internal wiring and other electrical characteristics of a standard parallel printer cable are largely undefined except by custom. In practice, these standard cables are acceptable for transferring data at 150 KBps, and for distances of less than 6 feet, but they would be dangerously unreliable for some transfer modes.

For more reliability at distances up to 32 feet (10 meters), use proper IEEE 1284–compliant cabling. The transfer speed drops with the longer cables, but it does work, and sometimes the trade-off between speed and distance is worth it.

Installing a parallel cable is a snap. Just insert the DB-25 connector into the parallel port on the back of the PC and insert the Centronics connector into the printer's Centronics port and you're ready to go to press! If your PC didn't include a parallel port, you can always add one with a PCI or PCIe expansion card.

Some printers come with both USB and parallel connections, but this, like the parallel port in general, has become very rare. If you need a parallel printer for a system, be sure to confirm that the particular model you want will work with your system!

USB Printers

New printers now use USB connections that you can plug into any USB port on your computer. USB printers don't usually come with a USB cable, so you need to purchase one when you purchase a printer. (It's quite a disappointment to come home with your new printer only to find you can't connect it because it didn't come with a USB cable.) Most printers use the standard USB type A connector on one end and the smaller USB type B connector on the other end, although some use two type A connectors. Whichever configuration your USB printer has, just plug in the USB cable—it's that easy!

In almost all cases, you must install drivers before you plug a USB printer into your computer. You'll learn about installing printer drivers later in this chapter.

Network Printers

Connecting a printer to a network isn't just for offices anymore. More and more homes and home offices are enjoying the benefits of network printing. It used to be that to share a printer on a network—that is, to make it available to all network users—you would physically connect the printer to a single computer and then share the printer on the network. The downside to this was that the computer to which the printer was connected had to be left on for others to use the printer.

Today, the typical **network printer** comes with its own onboard network adapter that uses a standard RJ-45 Ethernet cable to connect the printer directly to the network by way of a router. Other printers include a built-in Wi-Fi adapter to enable wireless printing over the network. The printer

can typically be assigned a static IP address, or it can acquire one dynamically from a DHCP server. (Don't know what a router, IP address, or DHCP server is? Take a look back at Chapters 5 and 22.) Once connected to the network, the printer acts independently of any single PC. Some of the more costly network printers come with a built-in Wi-Fi adapter to connect to the network wirelessly. Alternatively, some printers offer Bluetooth or infrared (IR) interfaces for networking.

Even if a printer does not come with built-in Ethernet, Wi-Fi, or Bluetooth, you can purchase a standalone network device known as a *print server* to connect your printer to the network. These print servers, which can be Ethernet or Wi-Fi, enable one or several printers to attach via USB cable (or even parallel port, if you still have a printer that old). So take that ancient ImageWriter dot-matrix printer and network it—I dare you!

The CompTIA A+ 220-801 exam objectives refer to a wireless print connection called "802.11x." This is not a new Wi-Fi standard. It's a generic term used to describe all Wi-Fi standards, including 802.11a, 802.11b, 802.11g, and 802.11n.

You'll find print servers outside standalone network devices. In fact, your Windows PC is capable of operating as a print server. Anytime you plug a printer into a PC and share the printer over the network, the sharing PC can be referred to as a print server. The CompTIA A+ exams, however, will most likely stick to standalone print server boxes, as opposed to Windows print servers.

Other Printers

Plenty of other connection types are available for printers. We've focused mainly on parallel, USB, and networked connections. Be aware that you may run into an old serial port printer or a SCSI printer. Although this is unlikely, know that it's a possibility.

The Laser Printing Process

The laser printing process can be broken down into seven steps, and the CompTIA A+ exams expect you to know them all. As a tech, you should be familiar with these phases, as this can help you troubleshoot printing problems. For example, if an odd line is printed down the middle of every page, you know there's a problem with the photosensitive drum or cleaning mechanism and the toner cartridge needs to be replaced.

The seven steps to the laser printing process may be performed in a different order, depending on the printer, but it usually goes like this:

1. Processing
2. Charging
3. Exposing
4. Developing
5. Transferring
6. Fusing
7. Cleaning

Processing

When you click the Print button in an application, several things happen. First, the CPU processes your request and sends a print job to an area of memory called the print spooler. The **print spooler** enables you to queue up multiple print jobs that the printer will handle sequentially. Next, Windows sends the first print job to the printer. That's your first potential bottleneck—if it's a big job, the OS has to dole out a piece at a time and you'll see the

little printer icon in the notification area at the bottom right of your screen. Once the printer icon goes away, you know the print queue is empty—all jobs have gone to the printer.

Once the printer receives some or all of a print job, the hardware of the printer takes over and processes the image. That's your second potential bottleneck and has multiple components.

Raster Images

Impact printers transfer data to the printer one character or one line at a time, whereas laser printers transfer entire pages at a time to the printer. A laser printer generates a **raster image** (a pattern of dots) of the page, representing what the final product should look like. It uses a device (the laser) to "paint" a raster image on the photosensitive drum. Because a laser printer has to paint the entire surface of the photosensitive drum before it can begin to transfer the image to paper, it processes the image one page at a time.

A laser printer uses a chip called the **raster image processor (RIP)** to translate the raster image into commands to the laser. The RIP takes the digital information about fonts and graphics and converts it to a rasterized image made up of dots that can then be printed. An inkjet printer also has a RIP, but it's part of the software driver instead of onboard hardware circuitry. The RIP needs memory (RAM) to store the data that it must process.

A laser printer must have enough memory to process an entire page. Some images that require high resolutions require more memory. Insufficient memory to process the image will usually be indicated by a memory overflow ("MEM OVERFLOW") error. If you get a memory overflow error, try reducing the resolution, printing smaller graphics, or turning off RET (see the following section for the last option). Of course, the best solution to a memory overflow error is simply to add more RAM to the laser printer.

Do not assume that every error with the word *memory* in it can be fixed simply by adding more RAM to the printer. Just as adding more RAM chips will not solve every conventional PC memory problem, adding more RAM will not solve every laser printer memory problem. The message "21 ERROR" on an HP LaserJet, for example, indicates that "the printer is unable to process very complex data fast enough for the print engine." This means that the data is simply too complex for the RIP to handle. Adding more memory would *not* solve this problem; it would only make your wallet lighter. The only answer in this case is to reduce the complexity of the page image (that is, fewer fonts, less formatting, reduced graphics resolution, and so on).

Tech Tip

Inkjet RIPs

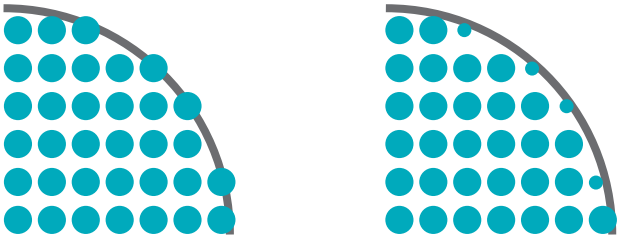
Inkjet printers use RIPs as well, but they're written into the device drivers instead of the onboard programming. You can also buy third-party RIPs that can improve the image quality of your printouts; for an example, see www.colorbytesoftware.com.

Resolution

Laser printers can print at different resolutions, just as monitors can display different resolutions. The maximum resolution that a laser printer can handle is determined by its physical characteristics. Laser printer resolution is expressed in dots per inch (dpi). Common resolutions are 600 × 600 dpi or 1200 × 1200 dpi. The first number, the horizontal resolution, is determined by how fine a focus can be achieved by the laser. The second number is determined by the smallest increment by which the drum can be turned. Higher resolutions produce higher-quality output, but keep in mind that higher resolutions also require more memory. In some instances, complex images can be printed only at lower resolutions because of their high

memory demands. Even printing at 300 dpi, laser printers produce far better quality than dot-matrix printers because of **resolution enhancement technology (RET)**.

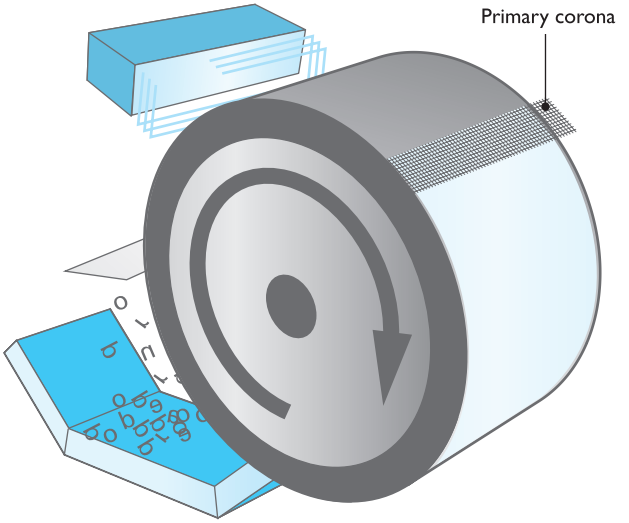
RET enables the printer to insert smaller dots among the characters, smoothing out the jagged curves that are typical of printers that do not use RET (see Figure 28.12). Using RET enables laser printers to output high-quality print jobs, but it also requires a portion of the printer's RAM. If you get a MEM OVERFLOW error, sometimes disabling RET will free up enough memory to complete the print job.



• **Figure 28.12** RET fills in gaps with smaller dots to smooth out jagged characters.

Charging

Now we turn to the physical side of the printing process. To make the drum receptive to new images, it must be charged (see Figure 28.13). Using the primary corona wire or primary charge roller, a uniform negative charge is applied to the entire surface of the drum (usually between ~600 and ~1000 volts).



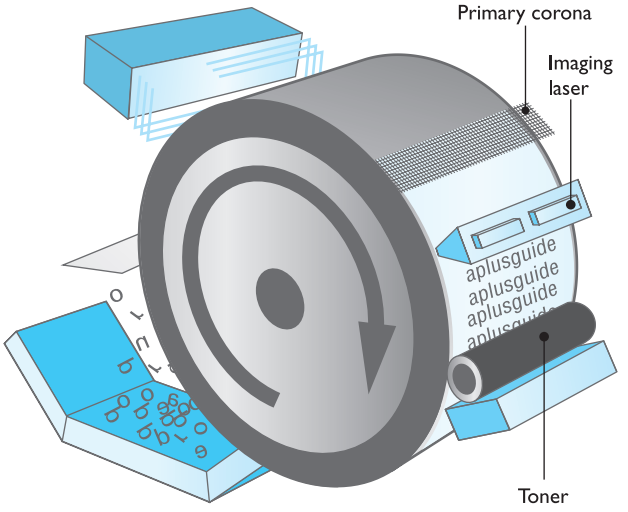
• **Figure 28.13** Charging the drum with a uniform negative charge

Exposing

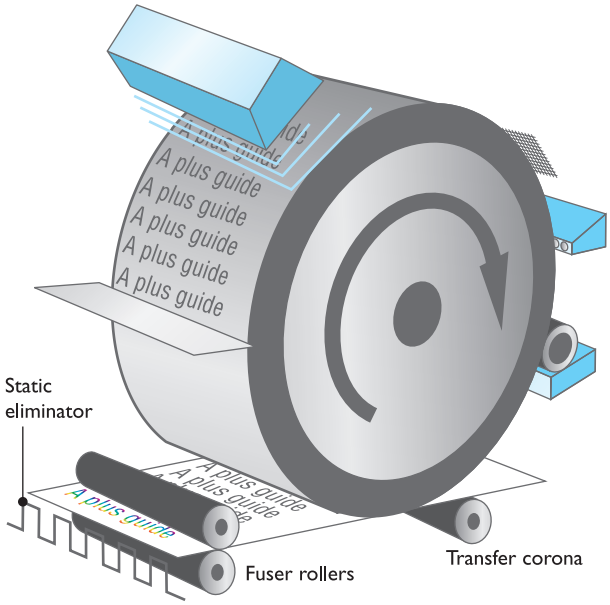
A laser is used to create a positive image on the surface of the drum. Every particle on the drum hit by the laser releases most of its negative charge into the drum.

Developing

Those particles with a lesser negative charge are positively charged relative to the toner particles and attracts them, creating a developed image (see Figure 28.14).



• **Figure 28.14** Writing the image and applying the toner



• **Figure 28.15** Transferring the image to the paper and fusing the final image

Transferring

The printer must transfer the image from the drum onto the paper. The transfer corona or transfer roller gives the paper a positive charge; then the negatively charged toner particles leap from the drum to the paper. At this point, the particles are merely resting on the paper and must still be permanently fused to the paper.

Fusing

The particles have been attracted to the paper because of the paper's positive charge, but if the process stopped here, the toner particles would fall off the page as soon as you lift it. Because the toner particles are mostly composed of plastic, they can be melted to the page. Two rollers—a heated roller coated in a nonstick material and a pressure roller—melt the toner to the paper, permanently affixing it. Finally, a static charge eliminator removes the paper's positive charge (see Figure 28.15). Once the page is complete, the printer ejects the printed copy and the process begins again with the physical and electrical cleaning of the printer.

Tech Tip

Laser Printing in Color

Color laser printers use four different colors of toner (cyan, magenta, yellow, and black) to create their printouts. Most models send each page through four different passes, adding one color at each pass to create the needed results, while others place all the colors onto a special transfer belt *and then transfer them to the page in one pass. In some cases, the printer uses four separate toner cartridges and four lasers for the four toner colors, and in others the printer simply lays down one color after the other on the same drum, cleaning after each of four passes per page.*

Cleaning

The printing process ends with the physical and electrical cleaning of the photosensitive drum (see Figure 28.16). Before printing another new page, the drum must be returned to a clean, fresh condition. All residual toner left over from printing the previous page must be removed, usually by scraping the surface of the drum with a rubber cleaning blade. If residual particles remain on the drum, they will appear as random black spots and streaks on the next page. The physical cleaning mechanism either deposits the residual toner in a debris cavity or recycles it by returning it to the toner supply in the toner cartridge. The physical cleaning must be done carefully. Damage to the drum will cause a permanent mark to be printed on every page.

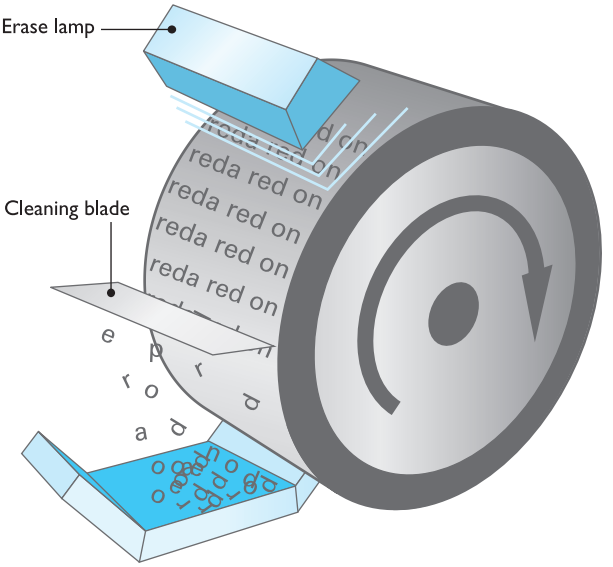
The printer must also be electrically cleaned. One or more erase lamps bombard the surface of the drum with the appropriate wavelengths of light, causing the surface particles to discharge into the grounded drum. After the cleaning process, the drum should be completely free of toner and have a neutral charge.

The heated roller produces enough heat to melt some types of plastic media, particularly overhead transparency materials. This could damage your laser printer (and void your warranty), so make sure you're printing on transparencies designed for laser printers!

Installing a Printer in Windows

You need to take a moment to understand how Windows handles printing, and then you'll see how to install, configure, and troubleshoot printers in these operating systems.

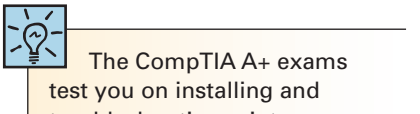
To Windows, a printer is not a physical device; it is a *program* that controls one or more physical printers. The *physical* printer is called a print device by Windows (although I continue to use the term "printer" for most



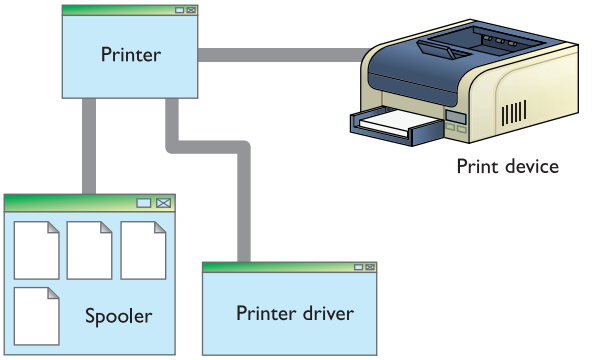
• **Figure 28.16** Cleaning and erasing the drum

purposes, just like almost every tech on the planet). Printer drivers and a spooler are still present, but in Windows, they are integrated into the printer itself (see Figure 28.17). This arrangement gives Windows amazing flexibility. For example, one printer can support multiple print devices, enabling a system to act as a print server. If one print device goes down, the printer automatically redirects the output to a working print device.

The general installation, configuration, and troubleshooting issues are basically identical in all modern versions of Windows. Here's a review of a typical Windows printer installation. I'll mention the trivial differences among Windows XP, Vista, and 7 as I go along.



The CompTIA A+ exams test you on installing and troubleshooting printers, so read these sections carefully!



• **Figure 28.17** Printer driver and spooler in Windows

Setting Up Printers

Setting up a printer is so easy that it's almost scary. Most printers are plug and play, so installing a printer is reduced to simply plugging it in and loading the driver if needed. With USB printers (and infrared printers, for that matter), Windows won't even wait for you to do anything—once you connect a printer (or point the IR beam at a compatible PC), Windows immediately detects and installs the printer. If the system does not detect the printer or if the printer is not plug and play, however, click Start | Printers and Faxes in Windows XP to open the Printers applet. In Windows Vista, you need to open the Control Panel and find the Printer menu item—it is either by itself or, in the categorized view, under Hardware. With Windows 7, go to Start | Devices and Printers. As you might guess, you install a new printer by clicking the Add a Printer icon/button (somehow Microsoft has managed to leave the name of this option unchanged through all Windows versions since 9*x*). This starts the Add Printer Wizard.

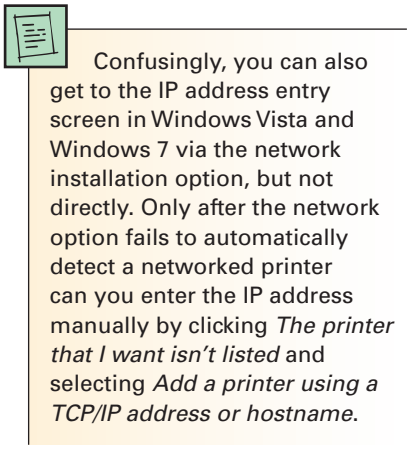
The Add Printer Wizard enables you to install a local printer or a network printer. This distinction is actually a little misleading. Windows divides printer installation into two scenarios: a printer connected directly to a PC (your local PC or another PC on a network), or a standalone printer directly connected to a switch or router. While you might think the local versus network installation options divide these scenarios nicely, they do not. Let's take a quick look at both local and network installations so you know when to use each.

Installing a Local Printer

At first glance, you might think the local printer installation option is used to install your standard USB printer, but don't forget that Windows will automatically detect and install USB printers (or any other plug-and-play printer). So what do you use it for? This option is most commonly used to install printers using a parallel connection or to install standalone network printers using an IP address. Using current versions of Windows and a modern printer, you shouldn't need to use the IP address to install a standalone network printer, but it can be a helpful alternative if Windows won't detect it any other way.

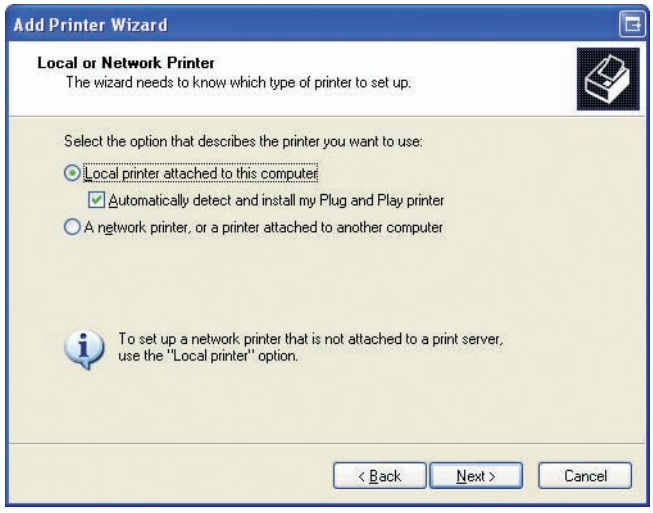
For parallel port printers, check the *Automatically detect and install my Plug and Play printer* option in Windows XP (see Figure 28.18). Windows won't automatically detect a new parallel device. When you check this box and click Next, Windows XP will run a search for any plug-and-play printers, including those connected via parallel cables. (Windows Vista and Windows 7 don't include this option; you'll need to configure parallel-connected printers manually by selecting a port and driver.)

If you need to install a standalone network printer using its IP address, uncheck the *Automatically detect and install my Plug and Play printer* option in Windows XP and click Next. In Windows Vista and Windows 7, click *Add a local printer*. In the *Create a new port* drop-down box, select Standard TCP/IP Port. Click Next. Type the IP address here.



Confusingly, you can also get to the IP address entry screen in Windows Vista and Windows 7 via the network installation option, but not directly. Only after the network option fails to automatically detect a networked printer can you enter the IP address manually by clicking *The printer that I want isn't listed* and selecting *Add a printer using a TCP/IP address or hostname*.

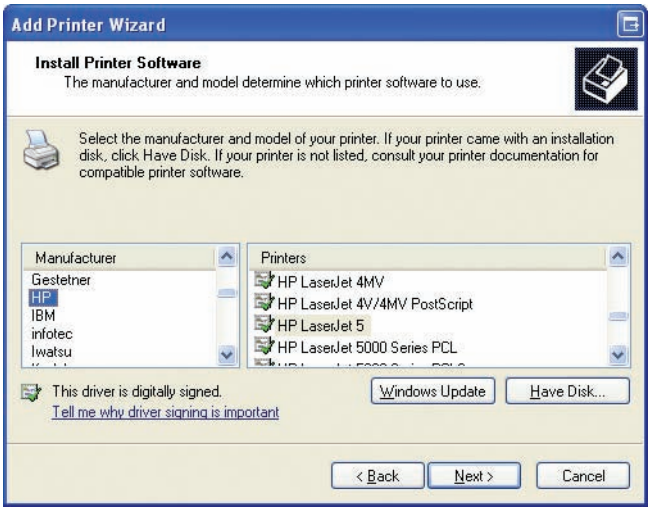
You will be unable to install a printer using the drivers that came with a disc unless you have administrative privileges.



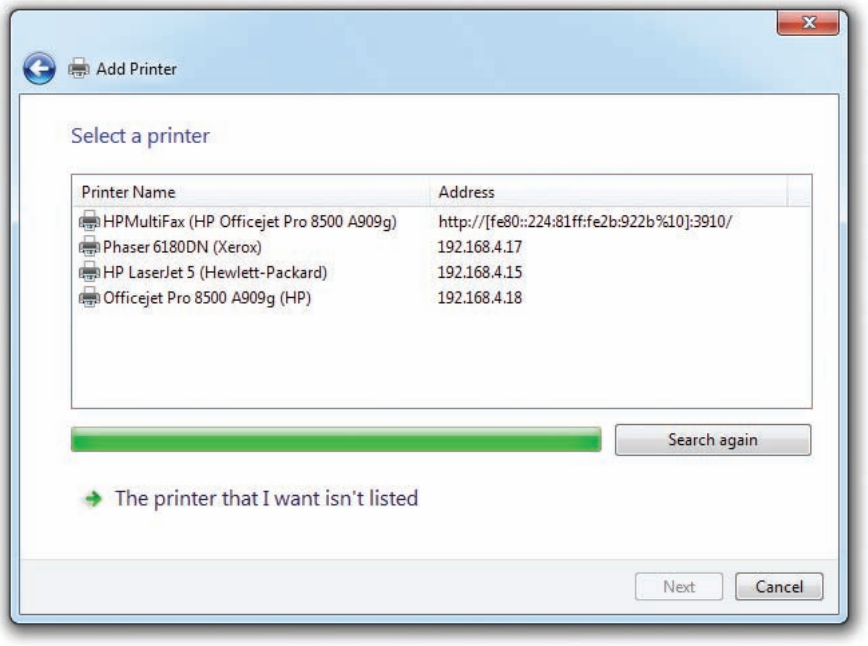
• **Figure 28.18** Automatically detecting plug-and-play printers in Windows XP

Whether you use a parallel port or a TCP/IP port, you'll need to manually select the proper driver (see Figure 28.19). Windows includes a lot of printer drivers, but you can also use the handy Have Disk option to use the disc that came with the printer. If you use the driver included on the disc, Windows will require administrator privileges to proceed; otherwise, you won't be able to finish the installation. The Windows Update button enables you to grab the latest printer drivers via the Internet.

You'll be asked if the new local printer should be the default printer and whether or not you want to share it with other PCs on the network. And before you ask, yes, you can share a standalone network printer connected to your PC via a TCP/IP port using File and Printer Sharing, though the printer would be disabled for other users any time you turned off your PC. You'll be asked to print a test page to make sure everything works. Then you're done!



• **Figure 28.19** Selecting drivers



• **Figure 28.20** List of available shared printers on a network

Installing a Network Printer

Surprisingly, setting up network printers doesn't require much more effort than setting up local printers, unless you're using Windows XP—but isn't that always the case? When you try to install a network printer in Windows Vista or Windows 7, the Add Printer Wizard will scan for any available printers on your local network. More often than not, the printer you are looking for will pop up in a list (see Figure 28.20). When you select that printer and click Next, Windows will search for drivers. If you need to, you

If you need to search for drivers online, make sure you download the driver designed for your operating system! If you have a 64-bit copy of Windows 7, the 32-bit Windows 7 drivers won't work.

Remember printer sharing from Chapter 22? Here's the other side of the operation. Keep in mind that after you install a shared printer onto your PC, you can actually share that shared printer with others. Windows considers the shared printer *your* printer, so you can do what you want with it, including sharing it.

can pick from a list of available drivers or use the disc that came with the printer. Either way, you're already done.

Windows XP doesn't include this automatic discovery feature, and if Windows Vista or Windows 7 fails to find your printer, you'll need to configure the network printer manually. Every version of Windows includes multiple methods of doing this. These methods change depending on whether you are connected to a domain or a workgroup.

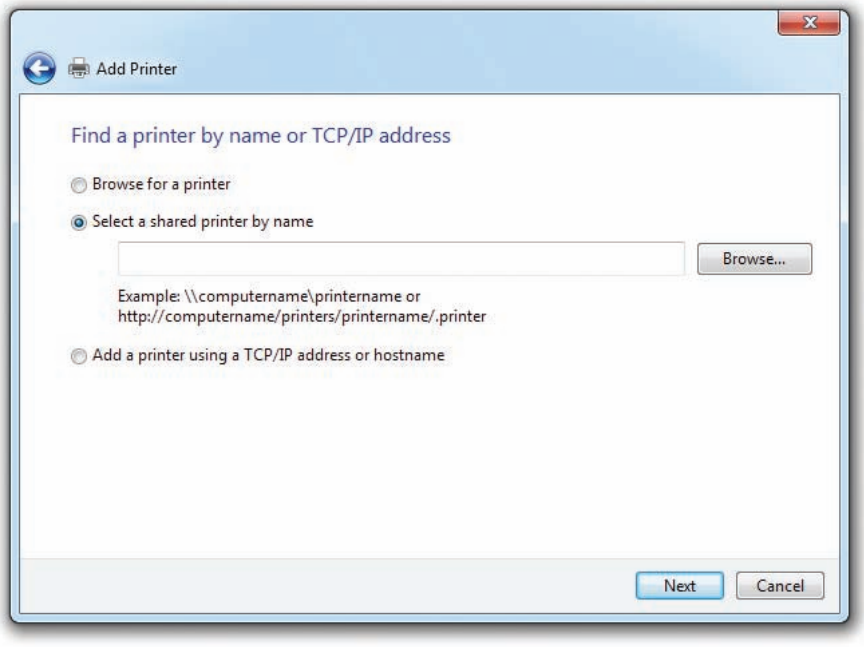
If you are on a workgroup, you can browse for a printer on your network, connect to a specific printer (using its name or URL), or use a TCP/IP address or hostname (Windows Vista/7 only), as you can see in Figure 28.21. In a domain, most of those options remain the same, except that instead of browsing the workgroup, you can search and browse the domain using several search parameters, including printer features, printer location, and more. Once you've found your printer, you might be prompted for drivers. Provide them using the usual methods described earlier and then you are finished!

Remember that Windows doesn't always see your network's printers exactly how they are physically arranged. Imagine you have a network with three PCs. Andy's computer has a printer connected via USB, whereas Beth's computer and Carol's computer have no printers. There is, however, a second printer connected directly to their router via Ethernet. Beth has configured her PC to connect directly to the network printer using an IP address. Now that she's done that, she can actually share that printer with the rest of her network, even though it's not attached to her computer—Windows doesn't care where it is. The process for sharing a local printer and a network printer is identical because Windows considers both printers to be installed on your PC and under your control. So now Andy and Beth both share printers. When Carol goes looking for shared printers to use,

If a computer is a member of a Windows 7 homegroup and printer sharing is enabled, all printers connected to the homegroup are shared with that computer automatically.

Depending upon how your network shares printers, you can end up seeing the same printer shared multiple ways. Everyone who has a shared printer installed can share the same printer again as their own printer. This can lead to some confusing printer usage, especially once people start turning off their computers and breaking the connections to the shared printer. Avoid this web of print sharing.

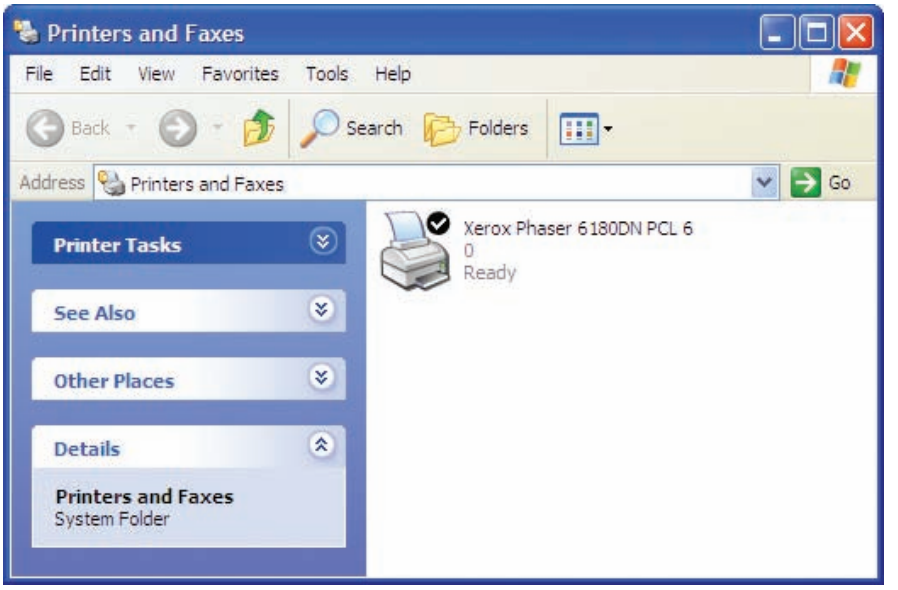
In addition to the Devices and Printers applet, Windows 7 (excluding the Home Premium edition) also includes the Print Management console. This tool enables you to view and modify all the printers and drivers on your PC or connected to your network. You can also manage any Windows print servers connected to the network. Many of Print Management's advanced features go beyond the scope of the CompTIA A+ exams, but know that it centralizes (and in a few cases, enhances) the standard printer controls in Windows 7. You can find Print Management in Control Panel | Administrative Tools | Print Management.



• **Figure 28.21** Options for finding network printers

the network printer attached to the router will look like Beth's printer, as if it were directly connected to Beth's machine.

Figure 28.22 shows a typical Windows XP Printers and Faxes screen on a system with one printer installed. Note the small checkmark in the icon's corner; this shows that the device is the default printer. If you have multiple printers, you can change the default printer by right-clicking the printer's icon and selecting *Make Default Printer* in Windows XP or *Set as default printer* in Windows Vista/7.



• **Figure 28.22** Installed default printer in the Printers and Faxes applet

In addition to the regular driver installation outlined previously, some installations use printer emulation. *Printer emulation* simply means using a substitute printer driver for a printer, as opposed to using one made exclusively for that printer. You'll run into printer emulation in two circumstances. First, some new printers do not come with their own drivers. They instead emulate a well-known printer (such as an HP LaserJet 4) and run perfectly well on that printer driver. Second, you may see emulation in the "I don't have the right driver!" scenario. I keep about three different HP LaserJet and Epson inkjet printers installed on my PC because I know that with these printer drivers, I can print to almost any printer. Some printers may require you to set them into an *emulation mode* to handle a driver other than their native one.

Optimizing Print Performance

Although a quality printer is the first step toward quality output, your output relies on factors other than the printer itself. What you see on the screen may not match what comes out of the printer, so calibration is important. Using the wrong type of paper can result in less than acceptable printed documents. Configuring the printer driver and spool settings can also affect your print jobs.

Calibration

If you've ever tweaked that digital photograph so it looks perfect on your screen, only to discover that the final printout was darker than you had hoped, consider calibrating your monitor. **Calibration** matches the print output of your printer to the visual output on your monitor and governs that through software. All three parts need to be set up properly for you to print what you see consistently.

Computer monitors output in RGB—that is, they compose colors using red, green, and blue pixels, as discussed in Chapter 21—while printers mix their colors differently to arrive at their output. As mentioned earlier, the

Tech Tip

Readme Files

You've seen how to get your system to recognize a printer, but what do you do when you add a brand-new printer? Like most peripherals, the printer will include an installation disc that contains various useful files. One of the most important but least-used tools on this disc is the Readme file. This file, generally in TXT format, contains the absolute latest information on any idiosyncrasies, problems, or incompatibilities related to your printer or printer driver. Usually, you can find it in the root folder of the installation disc, although many printer drivers install the Readme file on your hard drive so you can access it from the Start menu. The rule here is read first to avoid a headache later*!*

The RGB color display model is used for displaying mixtures of red, green, and blue. The CMYK color printing model uses cyan, magenta, yellow, and black for producing colored printed images.

CMYK method composes colors from cyan (blue), magenta (red), yellow, and black.

The upshot of all this is that the printer tries to output—by using CMYK (or another technique)—what you see on the screen using RGB. Because the two color modes do not create color the same way, you see color shifts and not-so-subtle differences between the onscreen image and the printed image. By calibrating your monitor, you can adjust the setting to match the output of your printer. You can do this manually through "eyeballing" it or automatically by using calibration hardware.

To calibrate your monitor manually, obtain a test image from the Web (try sites such as www.DigitalDog.net) and print it out. If you have a good eye, you can compare this printout to what you see on the screen and make the adjustments manually through your monitor's controls or display settings.

Another option is to calibrate your printer by using an International Color Consortium (ICC) color profile, a preference file that instructs your printer to print colors a certain way—for example, to match what is on your screen. Loading a different color profile results in a different color output. Color profiles are sometimes included on the installation media with a printer, but you can create or purchase custom profiles as well. The use of ICC profiles is not limited to printers; you can also use them to control the output of monitors, scanners, or even digital cameras. Windows Vista/7 include *Windows Color System* (*WCS*) to help build color profiles for use across devices. WCS is based on a new standard Microsoft calls *color infrastructure and translation engine* (*CITE*).

802

Troubleshooting Printers

Every printer is different. Read the documentation included with your printer to learn how you can perform the tasks listed in this section.

As easy as printers are to set up, they are equally robust at running, assuming that you install the proper drivers and keep the printer well maintained. But printer errors do occasionally develop. Take a look at the most common print problems with Windows, as well as problems that crop up with specific printer types.

General Troubleshooting Issues

Don't forget to check the obvious. Many printers include tiny displays that can clue you in to what's wrong. Most brands use a series of *error codes* that indicate the problem. Use the manual or the manufacturer's Web site to translate the error code into meaningful information.

Printers of all stripes share some common problems, such as print jobs that don't go, strangely sized prints, and misalignment. Other issues include disposing of consumables, sharing multiple printers, and crashing on power-up. Let's take a look at these general troubleshooting issues, but start with a recap of the tools of the trade.

Tools of the Trade

Before you jump in and start to work on a printer that's giving you fits, you'll need some tools. You can use the standard computer tech tools in

your toolkit, plus a couple of printer-specific devices. Here are some that will come in handy:

- A multimeter for troubleshooting electrical problems such as faulty wall outlets
- Various cleaning solutions, such as denatured alcohol
- An extension magnet for grabbing loose screws in tight spaces and cleaning up iron-based toner
- An optical disc or USB thumb drive with test patterns for checking print quality
- Your trusty screwdriver—both a Phillips-head and flat-head, because if you bring just one kind, it's a sure bet that you'll need the other

Print Job Never Prints

If you click Print but nothing comes out of the printer, first check all the obvious things. Is the printer on? Is it connected? Is it online? Does it have paper?

If you can't connect to the printer, check all cables, ports, and power involved. If everything is plugged in and ready to go, check the appropriate printer applet for your version of Windows. If you don't see the printer you are looking for, you'll need to reinstall it using the Add Printer Wizard.

If you attempt to use a printer shared by another PC, but Windows pops up with an "Access Denied" error, you might not have permission to use the printer. Go to the host PC and check the Security tab of the Printer Properties dialog box. Make sure your user account is allowed to use the printer.

Assuming the printer is in good order, it's time to look at the spooler. You can see the spooler status either by double-clicking the printer's icon in the appropriate printer Control Panel applet or by double-clicking the tiny printer icon in the notification area if it's present. If you're having a problem, the printer icon will almost always be there. Figure 28.23 shows the print spooler open.

Print spoolers can easily overflow or become corrupt due to a lack of disk space, too many print jobs, or one of a thousand other factors. The status window shows all of the pending print jobs and enables you to delete, start, or pause jobs. I usually just delete the affected print job(s) and try again.

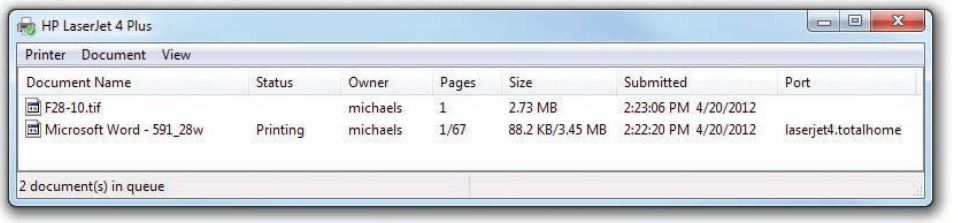
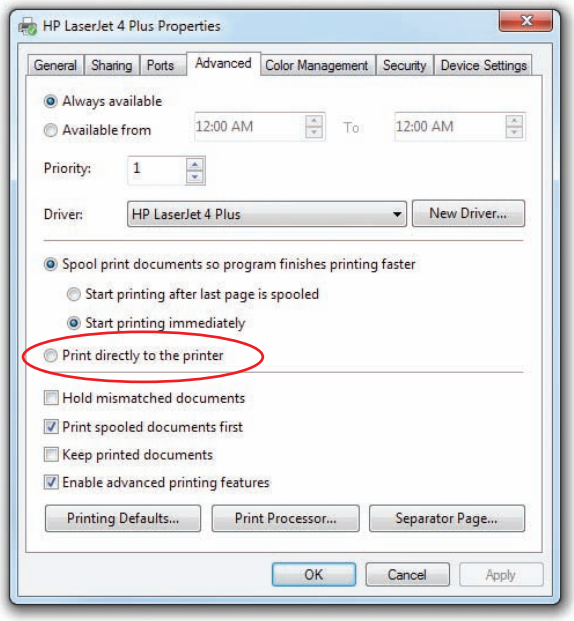


Figure 28.23 Print spooler

Print spoolers are handy. If the printer goes down, you can just leave the print jobs in the spooler until the printer comes back online. Some versions of Windows require you to select Resume Printing manually, but others automatically continue the print job(s). If you have a printer that isn't coming on anytime soon, you can simply delete the print job in the spooler window and try another printer.

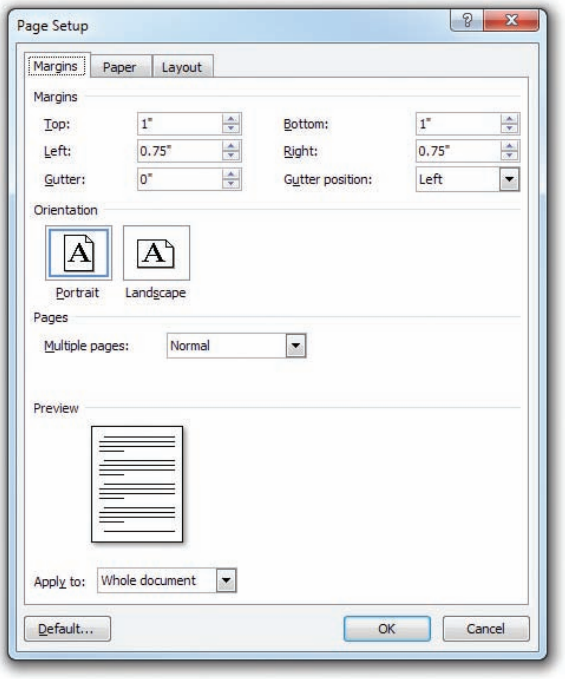


• **Figure 28.24** Print spool settings

If you have problems with the print spooler, you can get around them by changing your print spool settings. Go into the Printers and Faxes/Printers/Devices and Printers applet, right-click the icon of the printer in question, and choose Properties. In the resulting Properties dialog box (see Figure 28.24), choose the *Print directly to the printer* radio button and click OK; then try sending your print job again. Note that this window also offers you the choice of printing immediately—that is, starting to print pages as soon as the spooler has enough information to feed to the printer—or holding off on printing until the entire job is spooled.

If that isn't enough, try restarting the print spooler service. Open the Start menu and right-click on My Computer/Computer. Select Manage—you'll need administrator privileges to continue. In the column on the left, double-click on Services and Applications, and then click on Services. The Services console should appear in the center of the Computer Management window. Scroll down and find the service named Print Spooler. Right-click on the service and select Stop. After it has stopped, right-click on the service again and select Start. You should be able to print using the print spooler again.

Another possible cause for a stalled print job is that the printer is simply waiting for the correct paper! Laser printers in particular have settings that tell them what size paper is in their standard paper tray or trays. If the application sending a print job specifies a different paper size—for example, it wants to print a standard No. 10 envelope, or perhaps a legal sheet, but the standard paper tray holds only 8.5 × 11 letter paper—the printer usually pauses and holds up the queue until someone switches out the tray or manually feeds the type of paper that this print job requires. You can usually override this pause, even without having the specified paper, by pressing the OK or GO button on the printer.



• **Figure 28.25** Page Setup options for Microsoft Word

The printer's default paper tray and paper size options will differ greatly depending on the printer type and model. To find these settings, go into the printer's Properties dialog box from the Printers and Faxes/Printers/Devices and Printers applet, and then select the Device Settings tab. This list of settings includes Form To Tray Assignment, where you can specify which tray (in the case of a printer with multiple paper trays) holds which size paper.

Strange Sizes

A print job that comes out a strange size usually points to a user mistake in setting up the print job. All applications have a Print command and a Page Setup interface. The Page Setup interface enables you to define a number of print options, which vary from application to application. Figure 28.25 shows the Page Setup options for Microsoft Word. Make sure the page is set up properly before you blame the printer for a problem.

If you know the page is set up correctly, recheck the printer drivers. If necessary, uninstall and reinstall the printer drivers. If the problem persists, you may have a serious problem with the printer's print engine, but that comes up as a likely answer only when you continually get the same strangely sized printouts using a variety of applications.

Misaligned, Garbled, or Garbage Printouts

Misaligned or garbage printouts invariably point to a corrupted or incorrect driver. Make sure you're using the right driver (it's hard to mess this up, but not impossible) and then uninstall and reinstall the printer driver. If the problem persists, you may be asking the printer to do something it cannot do. For example, you may be printing to a PostScript printer with a PCL driver. Check the printer type to verify that you haven't installed the wrong type of driver for that printer!

Dealing with Consumables

All printers tend to generate a lot of trash in the form of **consumables**. Impact printers use paper and ribbons, inkjet printers use paper and ink cartridges, and laser printers use paper and toner cartridges. In today's environmentally sensitive world, many laws regulate the proper disposal of most printer components. Be sure to check with the local sanitation department or disposal services company before throwing away any component. Of course, you should never throw away toner cartridges—certain companies will *pay* for used cartridges!

Problems Sharing Multiple Printers

If you want to use multiple printers attached to the same parallel port, you have to use a switch box. Laser printers should never be used with mechanical switch boxes. Mechanical switch boxes create power surges that can damage your printer. If you must use a switch box, use a box that switches between printers electronically and has built-in surge protection.

Crashes on Power-up

Both laser printers and PCs require more power during their initial power-up (the POST on a PC and the warm-up on a laser printer) than once they are running. Hewlett-Packard recommends a *reverse power-up*. Turn on the laser printer first and allow it to finish its warm-up before turning on the PC. This avoids having two devices drawing their peak loads simultaneously.

Troubleshooting Impact Printers

Impact printers require regular maintenance but will run forever as long as you're diligent. Keep the platen (the roller or plate on which the pins impact) clean and the printhead clean with denatured alcohol. Be sure to lubricate gears and pulleys according to the manufacturer's specifications. Never lubricate the printhead, however, because the lubricant will smear and stain the paper. Don't forget to replace the ink ribbon every so often.

Tech Tip

Check the MSDS

When in doubt about what to do with a component, check with the manufacturer for a **material safety data sheet (MSDS)**. *These standardized forms provide detailed information about not only the potential environmental hazards associated with different components but also proper disposal methods. For example, surf to www.hp.com/hpinfo/globalcitizenship/environment/productdata/index.html to find the latest MSDS for all Hewlett-Packard products. This isn't just a printer issue—you can find an MSDS for most PC components. When in doubt about how to get rid of any PC component, check with the manufacturer for an MSDS.*

MSDSs contain important information regarding hazardous materials such as safe use procedures and emergency response instructions. An MSDS is typically posted anywhere a hazardous chemical is used.

Bad-looking Text

White bars going through the text point to a dirty or damaged printhead. Try cleaning the printhead with a little denatured alcohol. If the problem persists, replace the printhead. Printheads for most printers are readily available from the manufacturer or from companies that rebuild them. If the characters look chopped off at the top or bottom, the printhead probably needs to be adjusted. Refer to the manufacturer's instructions for proper adjustment.

Bad-looking Page

If the page is covered with dots and small smudges—the "pepper look"—the platen is dirty. Clean the platen with denatured alcohol. If the image is faded, and you know the ribbon is good, try adjusting the printhead closer to the platen. If the image is okay on one side of the paper but fades as you move to the other, the platen is out of adjustment. Platens are generally difficult to adjust, so your best plan is to take it to the manufacturer's local warranty/repair center.

Troubleshooting Thermal Printers

Compared to other printer styles, thermal printers are simple to troubleshoot and maintain. With direct thermal printers, you only need to worry about three things: the heating element, the rollers, and the paper. With thermal wax printers, you also need to care for the wax ribbon.

To clean the heating element, turn off the thermal printer and open it according to the manufacturer's instructions. Use denatured alcohol and a lint-free cloth to wipe off the heating element. You might need to use a little pressure to get it completely clean. Clean the rollers with a cloth or compressed air. You want to keep them free of debris so they can properly grip the paper. Replacing the paper is as easy as sliding off the old roll and replacing it with a new one. Remember to feed the paper through the heating element, because otherwise you won't print anything. Replacing the ribbon is similar to replacing the roll of paper; make sure to feed it past the heating element, or the printer won't work properly. Your printer's manufacturer should include any special instructions for installing a new ribbon.

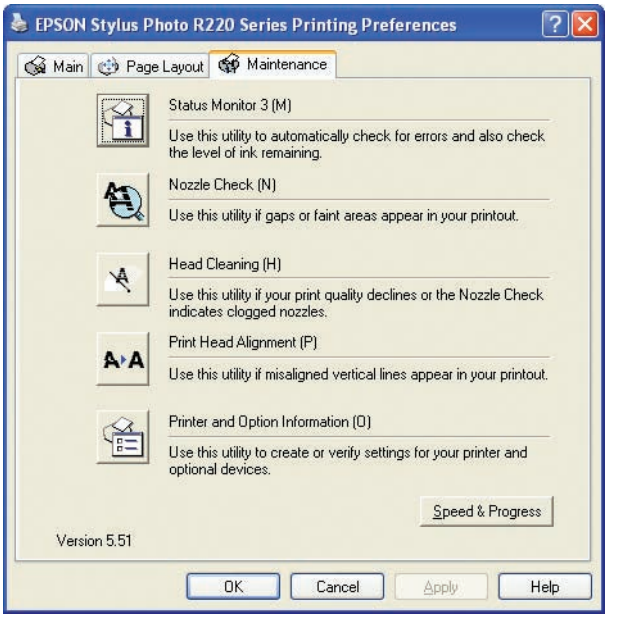
Troubleshooting Inkjet Printers

Inkjet printers are reliable devices that require little maintenance as long as they are used within their design parameters (high-use machines will require more intensive maintenance). Because of the low price of these printers, manufacturers know that people don't want to spend a lot of money keeping them running. If you perform even the most basic maintenance tasks, they will soldier on for years without a whimper. Inkjets generally have built-in maintenance programs that you should run from time to time to keep your inkjet in good operating order.

Inkjet Printer Maintenance

Inkjet printers don't get nearly as dirty as laser printers, and most manufacturers do not recommend periodic cleaning. Unless your manufacturer explicitly tells you to do so, don't vacuum an inkjet. Inkjets generally do not have maintenance kits, but most inkjet printers come with extensive maintenance software (see Figure 28.26). Usually, the hardest part of using this software is finding it in the first place. Look for an option in Printing Preferences, a selection on the Start menu, or an icon on your desktop. Don't worry—it's there!

When you first set up an inkjet printer, it normally instructs you to perform a routine (sometimes confusingly referred to as *calibration*) to align the printheads properly, wherein you print out a page and select from sets of numbered lines. If this isn't done, the print quality will show it, but the good news is that you can perform this procedure at any time. If a printer is moved or dropped or it's just been working away untended for a while, it's often worth running the alignment routine.



• **Figure 28.26** Inkjet printer maintenance screen

Inkjet Problems

Did I say that you never should clean an inkjet? Well, that may be true for the printer itself, but there is one part of your printer that will benefit from an occasional cleaning: the inkjet's printer head nozzles. The nozzles are the tiny pipes that squirt the ink onto the paper. A common problem with inkjet printers is the tendency for the ink inside the nozzles to dry out when not used even for a relatively short time, blocking any ink from exiting. If your printer is telling Windows that it's printing and feeding paper through, but either nothing is coming out (usually the case if you're just printing black text) or only certain colors are printing, the culprit is almost certainly dried ink clogging the nozzles.

Every inkjet printer has a different procedure for cleaning the printhead nozzles. On older inkjets, you usually have to press buttons on the printer to start a maintenance program. On more modern inkjets, you can access the head-cleaning maintenance program from Windows.

Another problem that sometimes arises is the dreaded multi-sheet paper grab. This is often not actually your printer's fault—humidity can cause sheets of paper to cling to each other—but sometimes the culprit is an overheated printer, so if you've been cranking out a lot of documents without stopping, try giving the printer a bit of a coffee break. Also, fan the sheets of the paper stack before inserting it into the paper tray.

Finally, check to see if excess ink overflow is a problem. In the area where the printheads park, look for a small tank or tray that catches excess ink from the cleaning process. If the printer has one, check to see how full it is. If this tray overflows onto the main board or even the power supply, it will kill your printer. If you discover that the tray is about to overflow, you can remove excess ink by inserting a twisted paper towel into the tank to soak up some of the ink. It is advisable to wear latex or vinyl gloves while doing this. Clean up any spilled ink with a paper towel dampened with distilled water.

All inkjet inks are water-based, and water works better than alcohol to clean them up.

Cleaning the heads on an inkjet printer is sometimes necessary, but I don't recommend that you do it on a regular basis as preventive maintenance. The head-cleaning process uses up a lot of that very expensive inkjet ink—so do this only when a printing problem seems to indicate clogged or dirty printheads!

Before you service a laser printer, always, *always* turn it off and unplug it! Don't expose yourself to the very dangerous high voltages found inside these machines.

The CompTIA A+ 220-802 exam refers to a "toner vacuum," which is the same as a low-static vacuum.

The photosensitive drum, usually contained in the toner cartridge, can be wiped clean if it becomes dirty, but be very careful if you do so! If the drum becomes scratched, the scratch will appear on every page printed from that point on. The only repair in the event of a scratch is to replace the toner cartridge.

Troubleshooting Laser Printers

Quite a few problems can arise with laser printers, but before getting into those details, you need to review some recommended procedures for *avoiding* those problems.

Laser Printer Maintenance

Unlike PC maintenance, laser printer maintenance follows a fairly well established procedure. Of course, you'll need to replace the toner cartridge every so often, but keeping your laser printer healthy requires following these maintenance steps.

Keep It Clean Laser printers are quite robust as a rule. A good cleaning every time you replace the toner cartridge will help that printer last for many years. I know of many examples of original HP LaserJet I printers continuing to run perfectly after a dozen or more years of operation. The secret is that they were kept immaculately clean.

Your laser printer gets dirty in two ways: Excess toner, over time, will slowly coat the entire printer. Paper dust, sometimes called *paper dander*, tends to build up where the paper is bent around rollers or where pickup rollers grab paper. Unlike (black) toner, paper dust is easy to see and is usually a good indicator that a printer needs to be cleaned. Usually, a thorough cleaning using a can of compressed air to blow out the printer is the best cleaning you can do. It's best to do this outdoors, or you may end up looking like one of those chimney sweeps from *Mary Poppins*! If you must clean a printer indoors, use a special low-static vacuum designed especially for electronic components (see Figure 28.27).

• Figure 28.27 Low-static vacuum

Every laser printer has its own unique cleaning method, but the cleaning instructions tend to skip one little area. Every laser printer has a number of rubber guide rollers through which the paper is run during the print process. These little rollers tend to pick up dirt and paper dust over time, making them slip and jam paper. They are easily cleaned with a small amount of 90 percent or better alcohol on a fibrous cleaning towel. The alcohol will remove the debris and any dead rubber. If the paper won't feed, you can give the rollers and separator pads a textured surface that will restore their feeding properties by rubbing them with a little alcohol on a nonmetallic scouring pad.

If you're ready to get specific, get the printer's service manual. They are a key source for information on how to keep a printer clean and running. Sadly, not all printer manufacturers provide these, but most do. While you're at it, see if the manufacturer has a Quick Reference Guide; these can be very handy for most printer problems!

Periodic Maintenance Although keeping the printer clean is critical to its health and well being, every laser printer has certain components that you need to replace periodically. Your ultimate source for determining the parts that need to be replaced (and when to replace them) is the printer manufacturer. Following the manufacturer's maintenance guidelines will help to ensure years of trouble-free, dependable printing from your laser printer.

Many manufacturers provide kits that contain components that you should replace on a regular schedule. These **maintenance kits** include sets

of replacement parts, such as a fuser, as well as one or more rollers or pads. Typically, you need to reset the page counter after installing a maintenance kit so the printer can remind you to perform maintenance again after a certain number of pages have been printed.

Some ozone filters can be cleaned with a vacuum and some can only be replaced—follow the manufacturer's recommendation. You can clean the fuser assembly with 90 percent or better denatured alcohol. Check the heat roller (the Teflon-coated one with the light bulb inside) for pits and scratches. If you see surface damage on the rollers, replace the fuser unit.

Most printers will give you an error code when the fuser is damaged or overheating and needs to be replaced; others will produce the error code at a preset copy count as a preventive maintenance measure. Again, follow the manufacturer's recommendations.

The transfer corona can be cleaned with a 90 percent denatured alcohol solution on a cotton swab. If the wire is broken, you can replace it; many just snap in or are held in by a couple of screws. Paper guides can also be cleaned with alcohol on a fibrous towel.

Failure of the thermal fuse (used to keep the fuser from overheating) can necessitate replacing the fuser assembly. Some machines contain more than one thermal fuse. As always, follow the manufacturer's recommendations. Many manufacturers have kits that alert you with an alarm code to replace the fuser unit and key rollers and guides at predetermined page counts.

The fuser assembly operates at 200 to 300 degrees Fahrenheit, so always allow time for this component to cool down before you attempt to clean it.

Laser Printer Problems

Laser printers usually manifest problems by creating poor output. One of the most important tests you can do on any printer, not just a laser printer, is called a *diagnostic print page* or an *engine test page*. You do this by either holding down the On Line button as the printer is started or using the printer's maintenance software.

Blank Paper Blank sheets of paper usually mean the printer is out of toner. If the printer does have toner and nothing prints, print a diagnostic print page. If that is also blank, remove the toner cartridge and look at the imaging drum inside. If the image is still there, you know the transfer corona or the high-voltage power supply has failed. Check the printer's maintenance guide to see how to focus on the bad part and replace it.

Dirty or Smudged Printouts If the fusing mechanism in a laser printer gets dirty, it will leave a light dusting of toner all over the paper, particularly on the back of the page. When you see toner speckles on your printouts, you should get the printer cleaned.

If the printout looks smudged, the fuser isn't properly fusing the toner to the paper. Depending on the paper used, the fuser needs to reach a certain temperature to fuse the toner. If the toner won't fuse to the paper, try using a lighter-weight paper. You might also need to replace the fuser.

Ghosting Ghost images sometimes appear at regular intervals on the printed page. This happens when the imaging drum has not fully discharged and is picking up toner from a previous image or when a previous image has used up so much toner that either the supply of charged toner is insufficient or the toner has not been adequately charged. Sometimes it can also be caused by a worn-out cleaning blade that isn't removing the toner from the drum.

Light Ghosting versus Dark Ghosting A variety of problems can cause both light and dark ghosting, but the most common source of light ghosting is "developer starvation." If you ask a laser printer to print an extremely

dark or complex image, it can use up so much toner that the toner cartridge will not be able to charge enough toner to print the next image. The proper solution is to use less toner. You can fix ghosting problems in the following ways:

- Lower the resolution of the page (print at 300 dpi instead of 600 dpi).
- Use a different pattern.
- Avoid 50 percent grayscale and "dot-on/dot-off patterns."
- Change the layout so that grayscale patterns do not follow black areas.
- Make dark patterns lighter and light patterns darker.
- Print in landscape orientation.
- Adjust print density and RET settings.
- Print a completely blank page immediately prior to the page with the ghosting image, as part of the same print job.

In addition to these possibilities, low temperature and low humidity can aggravate ghosting problems. Check your user's manual for environmental recommendations. Dark ghosting can sometimes be caused by a damaged drum. It may be fixed by replacing the toner cartridge. Light ghosting would *not* be solved in this way. Switching other components will not usually affect ghosting problems because they are a side effect of the entire printing process.

Vertical White Lines Vertical white lines usually happen when the toner is clogged, preventing the proper dispersion of toner on the drum. Try shaking the toner cartridge to dislodge the clog. If that doesn't work, replace the toner cartridge.

Blotchy Print Blotches are commonly a result of uneven dispersion of toner, especially if the toner is low. Shake the toner from side to side and then try to print. Also be sure that the printer is sitting level. Finally, make sure the paper is not wet in spots. If the blotches are in a regular order, check the fusing rollers and the photosensitive drum for any foreign objects.

Spotty Print If the spots appear at regular intervals, the drum may be damaged or some toner may be stuck to the fuser rollers. Try wiping off the fuser rollers. Check the drum for damage. If the drum is damaged, get a new toner cartridge.

Embossed Effect If your prints are getting an embossed effect (like putting a penny under a piece of paper and rubbing it with a lead pencil), there is almost certainly a foreign object on a roller. Use 90 percent denatured alcohol or regular water with a soft cloth to try to remove it. If the foreign object is on the photosensitive drum, you're going to have to use a new toner cartridge. An embossed effect can also be caused by the contrast control being set too high. The contrast control is actually a knob on the inside of the unit (sometimes accessible from the outside, on older models). Check your manual for the specific location.

Incomplete Characters You can sometimes correct incompletely printed characters on laser-printed transparencies by adjusting the print density. Be extremely careful to use only materials approved for use in laser printers.

Creased Pages Laser printers have up to four rollers. In addition to the heat and pressure rollers of the fuser assembly, other rollers move the paper from the source tray to the output tray. These rollers crease the paper to avoid curling that would cause paper jams in the printer. If the creases are noticeable, try using a different paper type. Cotton bond paper is usually more susceptible to noticeable creasing than other bonds. You might also try sending the output to the face-up tray, which avoids one roller. There is no hardware solution to this problem; it is simply a side effect of the process.

Paper Jams Every printer jams now and then. If you get a jam, always refer first to the manufacturer's jam removal procedure. It is simply too easy to damage a printer by pulling on the jammed paper! If the printer reports a jam but there's no paper inside, you've almost certainly got a problem with one of the many jam sensors or paper feed sensors inside the printer, and you'll need to take it to a repair center.

Pulling Multiple Sheets If the printer grabs multiple sheets at a time, first try opening a new ream of paper and loading that in the printer. If that works, you have a humidity problem. If the new paper angle doesn't work, check the separation pad on the printer. The separation pad is a small piece of cork or rubber that separates the sheets as they are pulled from the paper feed tray. A worn separation pad looks shiny and, well, *worn*! Most separation pads are easy to replace. Check out www.printerworks.com to see if you can replace yours.

Warped, Overprinted, or Poorly Formed Characters Poorly formed characters can indicate either a problem with the paper (or other media) or a problem with the hardware.

Incorrect media cause a number of these types of problems. Avoid paper that is too rough or too smooth. Paper that is too rough interferes with the fusing of characters and their initial definition. If the paper is too smooth (like some coated papers, for example), it may feed improperly, causing distorted or overwritten characters. Even though you can purchase laser printer–specific paper, all laser printers print acceptably on standard photocopy paper. Try to keep the paper from becoming too wet. Don't open a ream of paper until it is time to load it into the printer. Always fan the paper before loading it into the printer, especially if the paper has been left out of the package for more than just a few days.

The durability of a well-maintained laser printer makes hardware a much rarer source of character printing problems, but you should be aware of the possibility. Fortunately, it is fairly easy to check the hardware. Most laser printers have a self-test function—often combined with a diagnostic printout but sometimes as a separate process. This self-test shows whether the laser printer can properly develop an image without actually having to send print commands from the PC. The self-test is quite handy to verify the question "Is it the printer or is it the computer?" Run the self-test to check for connectivity and configuration problems.

Possible solutions include replacing the toner cartridge, especially if you hear popping noises; checking the cabling; and replacing the data cable, especially if it has bends or crimps or if objects are resting on the cable. If you have a front menu panel, turn off advanced functions and high-speed settings to determine whether the advanced functions are either not working properly or not supported by your current software configuration (check your manuals for configuration information). If these solutions do not work, the problem may not be user serviceable. Contact an authorized service center.

Beyond A+

Multifunction Peripherals

It's a common theme in computing: why have two devices that do one thing each when you can have one device that does two things? In that spirit, manufacturers started gluing various peripherals together to create *multifunction peripherals*, or *MFPs* (see Figure 28.28). These devices can include printers, scanners, fax machines, photocopiers, and more. All of your standard connection options are available, including USB, parallel, Ethernet, Wi-Fi, and more.

One of the best parts of a multifunction device is that all of these functions are available using a single connection. On the other hand, because a multifunction device is much more complicated than a single-function device, you'll probably need to follow very specific instructions and use the

• **Figure 28.28** All-in-one printer/scanner/fax machine/copier/coffee maker/iPod dock

manufacturer-supplied installation disc to get it all working. Many multifunction devices also include functions that don't require a PC at all, such as photocopying and faxing. You can even print files from a digital camera's memory card without plugging the MFP into a PC.

Chapter 28 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following aspects of printers.

Describe current printer technologies

- Impact printers create an image on paper by physically striking an ink ribbon against the paper's surface. The most commonly used impact printer technology is dot matrix. Dot-matrix printers have a large installed base in businesses, and they can be used for multipart forms because they actually strike the paper. Dot-matrix printers use a grid, or matrix, of tiny pins, also known as printwires, to strike an inked printer ribbon and produce images on paper. The case that holds the printwires is called a printhead. Dot-matrix printers come in two varieties: 9-pin (draft quality) and 24-pin (letter quality).
- Inkjet printers include a printhead mechanism, support electronics, a transfer mechanism to move the printhead back and forth, and a paper feed component to drag, move, and eject paper. They eject ink through tiny tubes. The heat or pressure used to move the ink is created by tiny resistors or electroconductive plates at the end of each tube.
- Ink is stored in ink cartridges. Older color printers used two cartridges: one for black and one for cyan, magenta, and yellow. Newer printers come with four, six, eight, or more cartridges.
- The quality of a print image is called the print resolution. The resolution is measured in dots per inch (dpi), which has two values: horizontal and vertical. An example of a resolution is 600 × 600 dpi. Printing speed is measured in pages per minute (ppm). Modern inkjet printers can print on a variety of media, including glossy photo paper, optical discs, or fabric.
- Dye-sublimation printers are used to achieve excellent print quality, especially in color, but they're expensive. Documents printed through the dye-sublimation process display continuous-tone images, meaning that each pixel dot is a blend of the dye colors. This is in contrast to other print technologies' dithered images, which use closely packed, single-color dots to simulate blended colors.
- Two kinds of thermal printers create either quick one-color printouts such as faxes or store receipts (direct thermal) or higher-quality color prints (thermal wax transfer).
- Using a process called electro-photographic imaging, laser printers produce high-quality and high-speed output. Laser printers usually use lasers as a light source because of their precision, but some lower-cost printers may use LED arrays instead. The toner cartridge in a laser printer supplies the toner that creates the image on the page; many other laser printer parts, especially those that suffer the most wear and tear, have been incorporated into the toner cartridge. Although the majority of laser printers are monochrome, you can find color laser printers capable of printing photographs.
- Be aware of the cost of consumables when purchasing a printer. Some less expensive printers may seem like a good deal, but ink or toner cartridge replacements can cost as much as the entire printer.
- The photosensitive drum (or imaging drum) in a laser printer is an aluminum cylinder coated with particles of photosensitive compounds. The erase lamp exposes the entire surface of the photosensitive drum to light, making the photosensitive coating conductive and leaving the surface particles electrically neutral. When the primary corona or charge roller is charged with an extremely high voltage, an electric field (or corona) forms, enabling voltage to pass to the drum and charge the photosensitive particles on its surface; the surface of the drum receives a uniform negative voltage of between ~600 and ~1000 volts.
- The laser acts as the writing mechanism of the printer. When particles are struck by the laser, they are discharged and left with a ~100 volt negative charge. The toner in a laser printer is a fine powder made up of plastic particles bonded to iron particles. The toner cylinder charges the toner with a negative charge of between ~200 and ~500 volts. Because that charge falls between the original

uniform negative charge of the photosensitive drum (~600 to ~1000 volts) and the charge of the particles on the drum's surface hit by the laser (~100 volts), particles of toner are attracted to the areas of the photosensitive drum that have been hit by the laser. The transfer corona or transfer roller applies a positive charge to the paper, drawing the negatively charged toner particles on the drum to the paper. The toner is merely resting on top of the paper after the static charge eliminator has removed the paper's static charge. Two rollers, a pressure roller and a heated roller, are used to fuse the toner to the paper.

- All laser printers have at least two separate power supplies. The primary power supply, which may actually be more than one power supply, provides power to the motors that move the paper, the system electronics, the laser, and the transfer corona. The high-voltage power supply usually only provides power to the primary corona/charge roller; it is one of the most dangerous devices in the world of PCs. Always turn off a laser printer before opening it up.
- A laser printer's mechanical functions are served by complex gear systems packed together in discrete units generically called gear packs or gearboxes. Most laser printers have two or three. Every laser printer has sensors that detect a broad range of conditions, such as paper jams, empty paper trays, or low toner levels.
- Every laser printer contains at least one electronic system board (many have two or three) that contains the main processor, the printer's ROM, and the RAM used to store the image before it is printed. When the printer doesn't have enough RAM to store the image before it prints, you get a memory overflow problem. Most printers can use generic DRAM like the kind you use in your PC, but check with the manufacturer to be sure.
- Because even tiny concentrations of ozone (O_3) will cause damage to printer components, most laser printers have a special ozone filter that needs to be vacuumed or replaced periodically.
- Solid ink printers use sticks of solid ink to produce extremely vibrant color. The inks are melted, absorbed into the paper fibers, and then solidify, producing continuous-tone output in a single pass. The solid ink sticks may be inserted midway through a print job if a certain color needs to be topped off.
- ASCII contains a variety of control codes for transferring data, some of which can be used to control printers; ASCII code 10 (or 0A in hex) means "Line Feed," and ASCII code 12 (0C) means "Form Feed." These commands have been standard since before the creation of IBM PCs, and all printers respond to them; however, the control codes are extremely limited. Utilizing high-end graphics and a wide variety of fonts requires more advanced languages.
- Adobe Systems' PostScript page description language is a device-independent printer language capable of high-resolution graphics and scalable fonts. Because PostScript is understood by printers at a hardware level, the majority of the image processing is done by the printer and not the PC's CPU, so PostScript printers print faster. PostScript defines the page as a single raster image; this makes PostScript files extremely portable.
- Hewlett-Packard's printer control language (PCL) features a set of printer commands greatly expanded from ASCII, but it does not support advanced graphical functions. PCL6 features scalable fonts and additional line drawing commands. PCL uses a series of commands to define the characters on the page, rather than defining the page as a single raster image like PostScript.
- Windows XP use the graphical device interface (GDI) component of the operating system to handle print functions. The GDI uses the CPU rather than the printer to process a print job and then sends the completed job to the printer. As long as the printer has a capable-enough raster image processor (RIP) and plenty of RAM, you don't need to worry about the printer language at all in most situations. Windows Vista/7 include support for the XML Paper Specification (XPS) print path, which requires an XPS-compatible driver. Some devices support XPS natively.
- Most printers connect to one of two ports on the PC: a DB-25 parallel port or a USB port. The parallel connection is the classic way to plug in a printer, but new printers use USB. The parallel port was included in the original IBM PC as a faster alternative to serial communication and has been kept around for backward compatibility. Parallel ports are slow by modern standards, with a maximum data transfer rate of 150 KBps. Parallel ports lack true bidirectional capability. A standard

parallel connection normally manifests as a female DB-25 connector on the PC and a corresponding male connector on the printer cable. The parallel connector on the printer side is called a Centronics connector.

- IEEE 1284 was developed as a standard for a backward-compatible, high-speed, bidirectional parallel port for the PC. It requires support for compatibility, nibble mode, byte mode, EPP, and ECP; a standard method of negotiating compatible modes between printer and PC; standard cables and connectors; and a standard electrical interface.
- USB is the most popular type of printer connection today. USB printers rarely come with the necessary USB cable, so you may need to purchase one at the same time you purchase the printer.
- Network printers come with their own network card and connect directly to a network. This can be an RJ-45 port for an actual cable, or it can be a wireless network card. Some printers offer Bluetooth or infrared adapters for networking.

Explain the laser printing process

- Laser printing is a seven-step process: processing, charging, exposing, developing, transferring, fusing, and cleaning.
- Laser printers generate a pattern of dots, called a raster image, representing what each page should look like. Laser printers use the laser to "paint" the raster image on the photosensitive drum. Laser printers use a chip called the RIP to translate the raster image sent to the printer into commands to the laser.
- Laser printer resolution is expressed in dots per inch (dpi). Common resolutions are 600 dpi × 600 dpi or 1200 dpi × 1200 dpi. The first number, the horizontal resolution, is determined by how fine a focus can be achieved by the laser. The second number is determined by the smallest increment by which the drum can be turned. Higher resolutions produce higher-quality output but also require more memory. Even printing at 300 dpi, laser printers produce far better quality than dot-matrix printers, because RET enables the printer to insert smaller dots among the characters, smoothing out the jagged curves that are typical of printers that do not use RET.
- Using the primary corona wire or primary charge roller, a uniform negative charge is applied to the entire surface of the drum (usually between ~600 and ~1000 volts) to make the drum receptive to new images.
- A laser is used to write a positive image relative to the toner particles on the surface of the drum, attracting them and creating a developed image.
- The transfer corona or transfer roller gives the paper a positive charge, making the negatively charged toner particles leap from the drum to the paper.
- The toner particles are mostly composed of plastic, so they can be melted to the page. Two rollers, a heated roller coated in a nonstick material and a pressure roller, melt the toner to the paper, permanently affixing it.
- The printing process ends with the physical and electrical cleaning of the photosensitive drum. All residual toner left over from printing the previous page must be removed, usually by scraping the surface of the drum with a rubber cleaning blade. One or more erase lamps bombard the surface of the drum with the appropriate wavelengths of light, causing the surface particles to discharge completely into the grounded drum.

Install a printer on a Windows PC

- In Windows, a printer is not a physical device; it is a program that controls one or more physical printers. The physical printer is called a print device. Print drivers and a spooler are still present, but they are integrated into the printer itself.
- To install a printer not automatically detected by Windows, select Start | Printers and Faxes in Windows XP to open the Printers and Faxes applet. In Windows Vista, select the Printers applet from the Control Panel. In Windows 7, go to Start | Devices and Printers. You install a new printer by clicking the Add a Printer icon to start the Add Printer Wizard. You must choose to install a local or a network printer; and you must select a port for a local printer. Windows automatically detects and installs USB printers. You must specify the printer type from the wizard's list, or use the Have Disk option. The wizard also features a Windows Update button you can use to get the latest printer driver via the Internet.
- One printer will always be the default printer. If you have more than one printer installed, you can make any printer the default printer. The icon

for the default printer has a small checkmark in the corner. If you have multiple printers, you can change the default printer by right-clicking the printer's icon in the appropriate printer applet and selecting Make Default Printer (XP) or Set as default printer (Vista/7).

- Printer emulation means to use a substitute printer driver for a printer, as opposed to one made exclusively for that printer. Some printers are designed to emulate other, more widely supported models. If you don't have the specific driver for a printer, you can often use the driver from a similar model.
- Your monitor creates colors by using RGB, while a printer outputs in CMYK. This difference can lead to a printed page differing greatly in color and tone from what you see on the monitor. Calibrating your monitor to your printer is an important step in printing the colors you see on your screen. Manually calibrate your monitor by eyeballing it, by using ICC color profiles to instruct the printer to output colors a certain way, or by using calibration hardware and software to automate the process. Windows Vista/7 include Windows Color System to help build color profiles for use across devices.

Recognize and fix basic printer problems

- When troubleshooting a printer, first check all the obvious things. Is the printer on? Is it connected? Is it online? Does it have paper? Does the printer display an error code on an LCD display? Then check the spooler status either by double-clicking the printer's icon in the Printers applet or by double-clicking the tiny printer icon in the notification area, if it's present. You may be able to bypass spooler problems by changing the printer's Properties dialog box setting to *Print directly to the printer*.
- If you see an "Access Denied" error when trying to print using a shared printer, make sure you have permission to use that printer.
- A print job that comes out a strange size usually points to a user mistake in setting up the print job. Use the program's Page Setup feature to fix these problems. If you know the page is set up correctly, recheck the printer drivers. Misaligned or garbage printouts invariably point to a corrupted or incorrect driver.
- Printer manufacturers will supply an MSDS for each of their products; they provide detailed information about the potential environmental hazards associated with different components and proper disposal methods. This isn't just a printer issue—you can find an MSDS for most PC components.
- Turn on the laser printer first and allow it to finish its warm-up before turning on the PC (a reverse power-up). This avoids having two devices drawing their peak loads simultaneously.
- With regular maintenance, impact printers run forever. White bars going through the text point to a dirty or damaged printhead. Try cleaning the printhead with a little 90 percent or better denatured alcohol. If the characters look chopped off at the top or bottom, you probably need to adjust the printhead.
- Thermal printers are easy to maintain. Keep the rollers and heating element clean and replace the ribbon and paper as needed.
- Inkjet printers generally have built-in maintenance programs that you should run from time to time to keep your inkjet in good operating order. A common problem with inkjet printers is the tendency for the ink inside the nozzles to dry out when not used even for a relatively short time, blocking any ink from exiting. To clean the nozzles on older inkjets, you usually have to press buttons on the printer to start a maintenance program. On more modern inkjets, you can access the head-cleaning maintenance program from Windows.
- Remember to clean your laser printer every time you replace the toner. Many manufacturers provide kits that contain components that you should replace on a regular schedule. These maintenance kits include sets of replacement parts, such as a fuser, as well as one or more rollers or pads.
- One of the most important tests you can do on any printer, not just a laser printer, is called a diagnostic print page or an engine test page. There are two types of printer test: the Windows test in which you print a test page, and the printer self-test that runs from the printer itself.
- Over time, excess toner will slowly coat a laser printer. Paper dander will build up where the paper is bent around rollers or where pickup rollers grab paper. Use a small amount of 90

percent or better alcohol on a fibrous cleaning towel to remove the debris and any dead rubber.

- Blank sheets of paper usually mean a laser printer is out of toner. If the printer has toner and nothing prints, print a diagnostic print page. If that is also blank, remove the toner cartridge and look at the imaging drum inside. If the image is still there, you know the transfer corona or the high-voltage power supply has failed. Blotchy print is most commonly due to uneven dispersion of toner, especially if the toner is low; also check that the printer is level and the paper is completely dry.
- Ghost images can be caused either because a laser printer's imaging drum has not fully discharged (and is picking up toner from a previous image) or because a previous image has used up so much toner that either the supply of charged toner is insufficient or the toner has not been adequately charged. Dark ghosting can sometimes be caused by a damaged drum. It may be fixed by replacing the toner cartridge. Light ghosting would *not* be solved in this way.
- The rollers that move the paper from the source tray to the output tray crease the paper to avoid curling that would cause paper jams in the printer. If the creases are noticeable, try using a different paper type. If the printer reports a jam but there's no paper inside, you almost certainly have a problem with one of the many jam sensors or paper feed sensors. If the printer grabs multiple sheets at a time, it may be humidity, or a worn separation pad. Hardware problems are a much rarer source of character printing problems. Most laser printers have a self-test function that shows whether the laser printer can properly develop an image without having to send print commands from the PC. Run the self-test to check for connectivity and configuration problems.

Key Terms

American Standard Code for Information Interchange (ASCII) *(1067)*
calibration *(1079)*
Centronics connector *(1070)*
consumables *(1083)*
DB-25 connector *(1070)*
dot-matrix printer *(1059)*
dots per inch (dpi) *(1061)*
dye-sublimation printer *(1062)*
erase lamp *(1064)*
fuser assembly *(1065)*
graphical device interface (GDI) *(1068)*
IEEE 1284 standard *(1069)*
impact printer *(1059)*
ink cartridge *(1060)*
Inkjet printer *(1059)*
laser *(1064)*
laser printer *(1063)*
maintenance kit *(1086)*
material safety data sheet (MSDS) *(1083)*
near-letter quality (NLQ) *(1059)*
network printer *(1070)*
pages per minute (ppm) *(1062)*
parallel port *(1069)*
photosensitive drum *(1064)*
PostScript *(1068)*
primary charge roller *(1064)*
primary corona *(1064)*
printer control language (PCL) *(1068)*
printhead *(1059)*
print resolution *(1061)*
print spooler *(1071)*
printwire *(1059)*
raster image *(1072)*
raster image processor (RIP) *(1072)*
resolution enhancement technology (RET) *(1073)*
solid ink printer *(1067)*
static charge eliminator *(1065)*
thermal printer *(1063)*
toner *(1065)*
toner cartridge *(1064)*
transfer corona *(1065)*
transfer roller *(1065)*
XML Paper Specification (XPS) print path *(1068)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. The _____ requires support for compatibility mode, nibble mode, byte mode, EPP, and ECP.
2. A standard parallel printer cable normally has a male _____ on one end and a 36-pin _____ on the other.
3. A printer that creates an image on paper by physically striking an ink ribbon against the paper's surface is known as a(n) _____.
4. Laser printers use lasers to create the print image on a(n) _____.
5. The _____ on a standard laser printer contains a pressure roller and a heated roller.
6. Adobe Systems' _____ is a device-independent printer language capable of high-resolution graphics and scalable fonts.
7. Windows XP uses the _____ component of the operating system to handle print functions.
8. The resolution of a printer is measured in _____.
9. A printer's speed is rated in _____.
10. The _____ is responsible for cleaning the photosensitive drum of electrical charge.

Multiple-Choice Quiz

1. Which part of a laser printer applies a positive charge to the paper that attracts the toner particles to it?
   - **A.** Erase lamp
   - **B.** Transfer corona
   - **C.** Laser
   - **D.** Primary corona
2. What is the approximate maximum data transfer rate of a standard parallel port?
   - **A.** 50 KBps
   - **B.** 150 KBps
   - **C.** 500 KBps
   - **D.** 2 MBps
3. Janet just bought a new computer. She wants to install her three-year-old inkjet printer on the new system but has lost the driver disc. She can't get on the Internet to download the latest drivers. What should she do for drivers?
   - **A.** Install a driver for a similar printer.
   - **B.** She's stuck until she can get on the Internet.
   - **C.** She can use the Mac drivers.
   - **D.** She can install the printer without drivers.
4. John just installed a second printer on his system. When he prints in Microsoft Word, the job goes to the wrong printer. What does he need to do to get print jobs always to go to one printer or the other?
   - **A.** He needs to set the primary printer.
   - **B.** He needs to set the main printer.
   - **C.** He needs to set the default printer.
   - **D.** He needs to set the system printer.
5. Frank's color inkjet printer no longer prints the color yellow, though it prints all the other colors just fine. The printer worked fine last month, the last time he printed in color. Which of the following is the most likely problem?
   - **A.** He turned off the yellow nozzle.
   - **B.** He has run out of yellow ink.
   - **C.** He has a corrupt printer driver.
   - **D.** His printer is set to monochrome mode.
6. Beth's laser printer is printing tiny specks on the paper. What should she do first?
   - **A.** Wipe the paper with bleach.
   - **B.** Run the printer maintenance program.
   - **C.** Clean the nozzles.
   - **D.** Vacuum the printer.

7. Ursula's laser printer has stopped working and is displaying this error message: "Error 81 – Service." What should she do first?
   - **A.** Update the printer's firmware.
   - **B.** Reinstall the printer driver.
   - **C.** Try to find the error in the user's guide or maintenance program or online.
   - **D.** Turn off the printer and call the manufacturer's help line.
8. Kevin's inkjet printer isn't printing blue (cyan). He checks the ink levels and sees that there's plenty of ink. What should he consider next?
   - **A.** A printhead is jammed.
   - **B.** A laser is blocked.
   - **C.** A nozzle is clogged.
   - **D.** An ink cartridge is missing.
9. The output from Diane's laser printer is fading evenly. What should she suspect first?
   - **A.** A laser is blocked.
   - **B.** The printer is out of toner.
   - **C.** A nozzle is clogged.
   - **D.** Her printer is dirty.
10. The dye-sublimation printing technique is an example of what method of color printing?
    - **A.** CMYK
    - **B.** Thermal wax transfer
    - **C.** RGB
    - **D.** Direct thermal
11. The output from your inkjet printer appears much darker than what you see on your screen. What is the problem?
    - **A.** You are using a paperweight that is not supported in the MSDS.
    - **B.** The printer and monitor need to be calibrated.
    - **C.** The color ink cartridges are almost empty.
    - **D.** The black ink cartridge is almost empty.
12. What is the best way to make a printer available to everyone on your network and maintain the highest level of availability?
    - **A.** Use a FireWire printer connected to a user's PC and share that printer on the network.
    - **B.** Use a USB printer connected to a user's PC and share that printer on the network.
    - **C.** Use a network printer connected directly to the network.
    - **D.** Use a mechanical switch box with the printer.
13. Sheila in accounting needs to print receipts in duplicate. The white copy stays with accounting and the pink copy goes to the customer. What type of printer should you install?
    - **A.** Inkjet
    - **B.** Impact
    - **C.** Laser jet
    - **D.** Thermal wax transfer
14. Your laser printer fails to print your print jobs and instead displays a MEM OVERFLOW error. What can you do to rectify the problem? (Select two.)
    - **A.** Install more printer RAM.
    - **B.** Install more PC RAM.
    - **C.** Upgrade the RIP.
    - **D.** Disable RET.
15. What is the proper order of the laser printing process?
    - **A.** Process, clean, charge, expose, develop, transfer, and fuse
    - **B.** Process, charge, expose, develop, transfer, fuse, and clean
    - **C.** Clean, expose, develop, transfer, fuse, process, and charge
    - **D.** Clean, charge, expose, develop, process, fuse, and transfer

Essay Quiz

1. Your department needs a number of color inkjet printers. At your organization, though, all purchases are handled through professional buyers. Sadly, they know nothing about color inkjet printers. You need to submit a Criteria for Purchase form to your buyers. This is the standard form that your organization gives to buyers so they know what to look for in the products they buy. What are the top three purchasing criteria that you think they need to consider? Write the criteria as simply and clearly as possible.
2. Interview a person who uses a computer for work. Ask what the person does and then write a short description of the type of printer that would most suit that person's needs. Explain why this printer would be the best choice.
3. You have been tasked to make a recommendation for a printer purchase for a busy office of ten people. Make a case for purchasing either an inkjet or laser printer, providing enough information to compare the two technologies. You can choose the type of business, so recommend the appropriate printer, such as a laser printer to an office that primarily produces text documents. Make your recommendation opposite to the one you made for essay question #2.
4. Write a short essay comparing and contrasting inkjet printers with the three less-common print technologies: dye-sublimation, thermal, and solid ink.
5. Your boss is fascinated by the laser printing process. Write a short memo that outlines how it works, in the proper order.

Lab Projects

• Lab Project 28.1

Laser printers often have rather complex maintenance procedures and schedules. Select a laser printer—preferably one that you actually have on hand—and answer the following questions.

1. Using the user's guide or online sources, determine the exact cleaning procedures for your laser printer. How often should it be vacuumed? Do any parts need to be removed for cleaning? Does the manufacturer recommend any specialized cleaning steps? Does your printer come with any specialized cleaning tools? Does the manufacturer have any recommended cleaning tools you should purchase?
2. Based on the information you gathered, create a cleaning toolkit for your laser printer. Be sure to include a vacuum. Locate sources for these products and determine the cost of the toolkit.
3. Determine the model number of the toner cartridge. Locate an online company that sells name-brand (such as Hewlett-Packard) toner cartridges. Locate an equivalent third-party toner cartridge. Assuming that the printer uses a toner cartridge every three months, what is your per system annual cost savings using third-party toner cartridges?
4. All toner cartridges have a material safety data sheet (MSDS). Locate the MSDS for your model of toner cartridge and read it. Note any potential hazards of the toner cartridges.
5. Print out the description of the cleaning kit you created as well as the manufacturer's cleaning instructions.

• Lab Project 28.2

Using the same laser printer you used in the first project, locate and compile, on paper, all of the following information about your printer:

- User's guide
- List of error codes
- Troubleshooting guides
- Location of the latest drivers for Windows

chapter 29

Securing Computers

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat."

—Sun Tzu, *The Art of War*

In this chapter, you will learn how to

- **Explain the threats to your computers and data**
- **Describe key security concepts and technologies**
- **Explain how to protect computers from network threats**

Your PC is under siege. Through your PC, a malicious person can gain valuable information about you and your habits. He can steal your files. He can run programs that log your keystrokes and thus gain account names and passwords, credit card information, and more. He can run software that takes over much of your computer processing time and use it to send spam or steal from others. The threat is real and right now. Worse, he's doing one or more of these things to your clients as I write these words. You need to secure your computer and your users' computers from these attacks.

But what does *computer security* mean? Is it an antivirus program? Is it big, complex passwords? Sure, it's both of these things, but what about the fact that your laptop can be stolen easily or that improper ventilation can cause hard drives and other components to die?

To secure computers, you need both a sound strategy and proper tactics. From a strategic sense, you need to understand the threat from unauthorized access to local machines as well as the big threats posed when computers go onto networks. Part of the big picture means to know what policies, software, and hardware to put in place to stop those threats. From a tactical in-the-trenches sense, you need to master the details, to know how to implement and maintain the proper tools. Not only do you need to install antivirus programs in your users' computers, for example, but you also need to update those programs regularly to keep up with the constant barrage of new viruses.

The majority of topics in this chapter apply exclusively to the 802 exam, but several 801 exam objectives fit well here too. I'll point out the 801 topics when they appear in the chapter.

801/802

Analyzing Threats

Threats to your data and PC come from two directions: accidents and malicious people. All sorts of things can go wrong with your computer, from users getting access to folders they shouldn't see to a virus striking and deleting folders. Files can be deleted, renamed, or simply lost. Hard drives can die, and optical discs get scratched and rendered unreadable. Accidents happen and even well-meaning people can make mistakes.

Unfortunately, a lot of people out there intend to do you harm. Add that intent together with a talent for computers, and you have a deadly combination. Let's look at the following issues:

- Unauthorized access
- Data destruction, accidental or deliberate
- Administrative access
- Catastrophic hardware failures
- Malware
- Environmental threats

Unauthorized Access

Unauthorized access occurs when a person accesses resources without permission. Resources in this case mean data, applications, and hardware. A user can alter or delete data; access sensitive information, such as financial data, personnel files, or e-mail messages; or use a computer for purposes the owner did not intend.

Not all unauthorized access is malicious—often this problem arises when users who are randomly poking around in a computer discover that they can access resources in a fashion the primary user did not intend. Unauthorized access becomes malicious when outsiders knowingly and intentionally take advantage of weaknesses in your security to gain information, use resources, or destroy data!

One of the ways to gain unauthorized access is through intrusion. You might imagine someone kicking in a door and hacking into a computer, but more often than not it's someone sitting at a home computer, trying various passwords over the Internet. Not quite as glamorous, but still….

Dumpster diving is the generic term for anytime a hacker goes through your refuse, looking for information. This is also a form of intrusion. The amount of sensitive information that makes it into any organization's trash bin boggles the mind! Years ago, I worked with an IT security guru who gave me and a few other IT people a tour of our office's trash. In one 20-minute tour of the personal wastebaskets of one office area, we had enough information to access the network easily, as well as to embarrass seriously more than a few people. When it comes to getting information, the trash is the place to look!

Shoulder surfing is another technique for gaining unauthorized access. Shoulder surfing is simply observing someone's screen or keyboard to get information, often passwords. As the name implies, it usually requires the bad guy looking over your shoulder to see what you are doing.

Social Engineering

Although you're more likely to lose data through accident, the acts of malicious users get the vast majority of headlines. Most of these attacks come under the heading of **social engineering**—the process of using or manipulating people inside the networking environment to gain access to that network from the outside—which covers the many ways humans can use other humans to gain unauthorized information. This unauthorized information may be a network login, a credit card number, company customer data—almost anything you might imagine that one person or organization may not want a person outside of that organization to access.

It's common for social engineering attacks to be used together, so if you discover one of them being used against your organization, it's a good idea to look for others.

Social engineering attacks aren't hacking—at least in the classic sense of the word—although the goals are the same. Social engineering means people attacking an organization through the people in the organization or physically accessing the organization to get the information they need. Following are a few of the more classic types of social engineering attacks.

Infiltration

Hackers can physically enter your building under the guise of someone who might have a legitimate reason for being there, such as cleaning personnel, repair technicians, or messengers. They then snoop around desks, looking for whatever they can find. They might talk with people inside the organization, gathering names, office numbers, department names—little things in and of themselves but powerful tools when combined later with other social engineering attacks.

Dressing the part of a legitimate user—with fake badge and everything—enables malicious people to gain access to locations and thus potentially your data. Following someone through the door, for example, as if you belong, is called **tailgating**. Tailgating is a common form of infiltration.

Telephone Scams

Telephone scams are probably the most common social engineering attack. In this case, the attacker makes a phone call to someone in the organization to gain information. The attacker attempts to come across as someone inside the organization and uses this to get the desired information. Probably the most famous of these scams is the "I forgot my user name and password" scam. In this gambit, the attacker first learns the account name of a legitimate person in the organization, usually using the infiltration method. The attacker then calls someone in the organization, usually the help desk, in an attempt to gather information, in this case a password.

> **Hacker:** "Hi, this is John Anderson in accounting. I forgot my password. Can you reset it, please?"
>
> **Help Desk:** "Sure, what's your user name?"
>
> **Hacker:** "j_w_Anderson"
>
> **Help Desk:** "OK, I reset it to e34rd3."

Certainly telephone scams aren't limited to attempts to get network access. There are documented telephone scams against organizations aimed at getting cash, blackmail material, or other valuables.

Phishing

Phishing is the act of trying to get people to give their user names, passwords, or other security information by pretending to be someone else electronically. A classic example is when a bad guy sends you an e-mail that's supposed to be from your local credit card company asking you to send them your user name and password. Phishing is by far the most common form of social engineering done today.

Data Destruction

Often an extension of unauthorized access, data destruction means more than just intentionally or accidentally erasing or corrupting data. It's easy to imagine some evil hacker accessing your network and deleting all your important files, but authorized users may also access certain data and then use that data beyond what they are authorized to do. A good example is the person who legitimately accesses a Microsoft Access product database to modify the product descriptions, only to discover that she can change the prices of the products, too.

This type of threat is particularly dangerous when users are not clearly informed about the extent to which they are authorized to make changes. A fellow tech once told me about a user who managed to mangle an important database when someone gave him incorrect access. When confronted, the user said: "If I wasn't allowed to change it, the system wouldn't let me do it!" Many users believe that systems are configured in a paternalistic way that wouldn't allow them to do anything inappropriate. As a result, users often assume they're authorized to make any changes they believe are necessary when working on a piece of data they know they're authorized to access.

Administrative Access

Every operating system enables you to create user accounts and grant those accounts a certain level of access to files and folders in that computer. As an administrator, supervisor, or root user, you have full control over just about every aspect of the computer. Windows XP, in particular, makes it entirely too easy to give users administrative access to the computer, especially Windows XP Home, which has only two kinds of users: administrators and limited users. Because you can't do much as a limited user, most home and small office systems simply use multiple administrator accounts. If you need to control access, you need to use non-Home versions of Windows.

System Crash/Hardware Failure

As with any technology, computers can and will fail—usually when you can least afford for it to happen. Hard drives crash, the power fails—it's all part of the joy of working in the computing business. You need to create redundancy in areas prone to failure (such as installing backup power in case of electrical failure) and perform those all-important data backups. Chapter 17 goes into detail about using backups and other issues involved in creating a stable and reliable system.

Physical Theft

A fellow network geek once challenged me to try to bring down his newly installed network. He had just installed a powerful and expensive firewall router and was convinced that I couldn't get to a test server he added to his network just for me to try to access. After a few attempts to hack in over the Internet, I saw that I wasn't going to get anywhere that way.

So I jumped in my car and drove to his office, having first outfitted myself in a techy-looking jumpsuit and an ancient ID badge I just happened to have in my sock drawer. I smiled sweetly at the receptionist and walked right by my friend's office (I noticed he was smugly monitoring incoming IP traffic by using some neato packet-sniffing program) to his new server.

I quickly pulled the wires out of the back of his precious server, picked it up, and walked out the door. The receptionist was too busy trying to figure out why her e-mail wasn't working to notice me as I whisked by her carrying the 65-pound server box. I stopped in the hall and called him from my cell phone.

Me (cheerily): "Dude, I got all your data!"

Him (not cheerily): "You rebooted my server! How did you do it?"

Me (smiling): "I didn't reboot it—go over and look at it!"

Him (really mad now): "YOU <EXPLETIVE> THIEF! YOU STOLE MY SERVER!"

Me (cordially): "Why, yes. Yes, I did. Give me two days to hack your password in the comfort of my home, and I'll see everything! Bye!"

I immediately walked back in and handed him the test server. It was fun. The moral here is simple: Never forget that the best network software

security measures can be rendered useless if you fail to protect your systems physically!

Malware

Networks are without a doubt the fastest and most efficient vehicles for transferring computer viruses among systems. News reports focus attention on the many malicious software attacks from the Internet, but a huge number of such attacks still come from users who bring in programs on optical discs and USB drives. The "Network Security" section of this chapter describes the various methods of virus infection and other malware and what you need to do to prevent such attacks from damaging your networked systems.

Environmental Threats

Your computer is surrounded by a host of dangers all just waiting to wreak havoc: bad electricity from the power company, a host of chemicals that just by the nature of your business may or may not be near your computer, dust, heat, cold, wet…it's a jungle out there!

Expect questions on environmental threats on the 220-801 exam.

Power

We've covered power issues extensively back in Chapter 10. Don't ever fail to appreciate the importance of surge suppressors and uninterruptible power supplies (UPSs) to protect your electronics from surges, brownouts, and blackouts. Also remember that network devices need power protection as well. Figure 29.1 shows a typical UPS protecting a network rack.

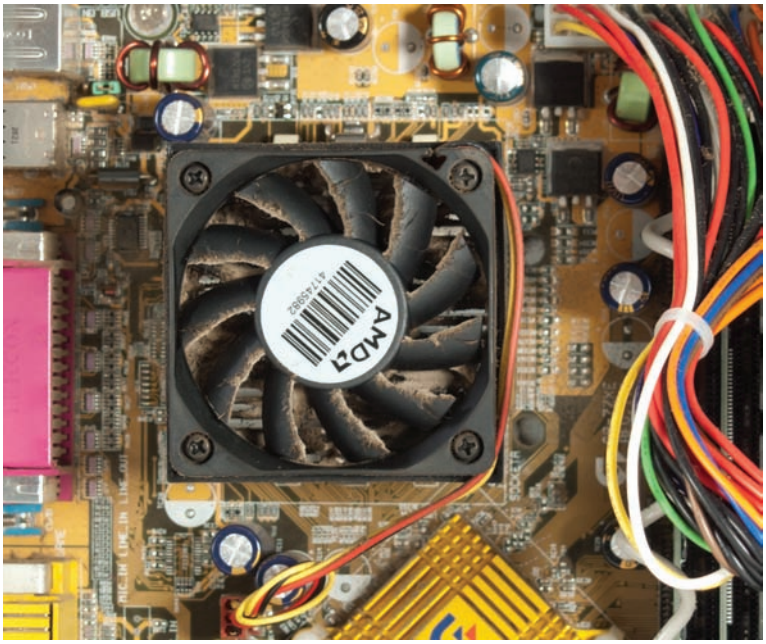
• **Figure 29.1** UPS on rack

How's the Air in There?

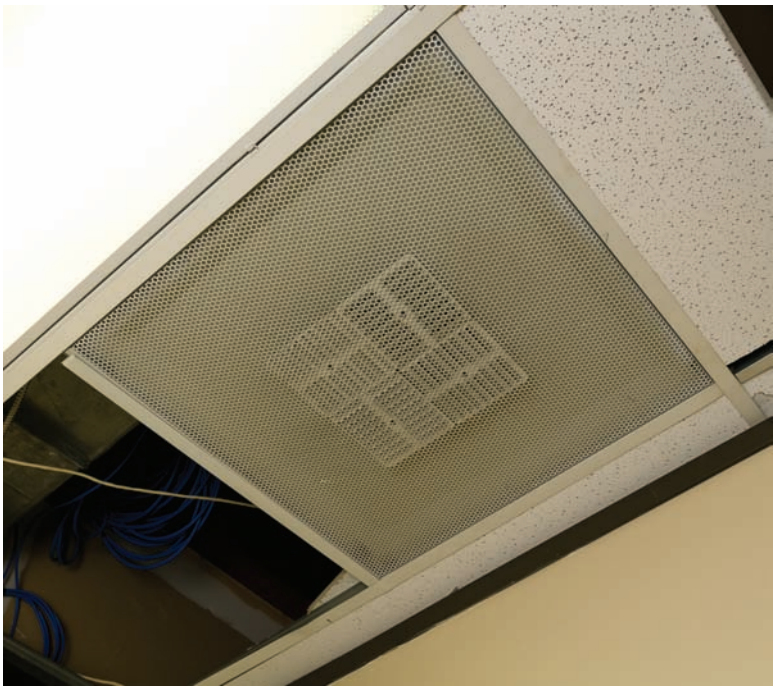
Proper environmental controls help secure servers and workstations from the environmental impact of excessive heat, dust, and humidity. Such *environmental controls* include air conditioning, proper ventilation, air filtration, and monitors for temperature and humidity. A CompTIA A+ technician maintains an awareness of temperature, humidity level, and ventilation, so that he or she can tell very quickly when proper levels or settings are out of whack.

A PC works best in an environment where the air is clean, dry, and room temperature. CompTIA doesn't expect you to become an environmental engineer, but it does expect you to explain and deal with how dirty or humid or hot air can affect a computer. We've covered all of these topics to some extent throughout the book so let's just do a quick overview with security in mind.

Dirty Air Dust and debris aren't good for any electronic components. Your typical office air conditioning does a pretty good job of eliminating the worst offenders, but not all computers are in nice offices. No matter where the computers reside, you need to monitor your systems for dirt. The best



• **Figure 29.2** Dirty fan



• **Figure 29.3** Air-conditioning vent in a small server closet

way to do this is observation as part of your regular work. Dust and debris will show up all over the systems, but the best place to look are the fans. Fans will collect dust and dirt quickly (see Figure 29.2).

All electronic components get dirty over time. To clean them, you need to use either compressed air or a nonstatic vacuum. So which one do you use? The rule is simple: If you don't mind dust blowing all over the place, use compressed air. If you don't want dust blowing all over the place, use a vacuum.

Equipment closets filled with racks of servers need proper airflow to keep things cool and to control dusty air. Make sure that the room is ventilated and air-conditioned (see Figure 29.3) and that the air filters are changed regularly.

If things are really bad, you can enclose a system in a dust shield. Dust shields come complete with their own filters to keep a computer clean and happy even in the worst of environments.

Temperature and Humidity Most computers are designed to operate at room temperature, which is somewhere in the area of 22°C (72°F) with the relative humidity in the 30–40 percent range. Colder and dryer is better for computers (but not for people), so the real challenge is when the temperature and the humidity go higher.

A modern office will usually have good air conditioning and heating, so your job as a tech is to make sure that things don't happen to prevent your air conditioning from doing its job. That means you're pretty much always on ventilation patrol. Watch for the following to make sure air is flowing:

- Make sure ducts are always clear of obstructions.
- Make sure ducts are adjusted (not too hot or too cold).
- Don't let equipment get too closed off from proper ventilation.

Toxic Materials

Every office is filled with chemicals, compositions that invariably get stored, spilled, or dumped. If something spills and it's not something you're

familiar with, refer to the Material Safety Data Sheet (MSDS) for proper documentation for handling and disposal. Always comply with local government regulations when dealing with chemicals, including batteries and the metals on circuit boards.

Tech Tip

Recycling E-Waste

Most cities in the U.S. have one or more environmental services center that you can use to recycle electronic components. For your city, try a Google (or other search engine) search on the term "environmental services" and you'll almost certainly find a convenient place for e-waste disposal.

Security Concepts and Technologies

Once you've assessed the threats to your computers and networks, you need to take steps to protect those valuable resources. Depending on the complexity of your organization, this can be a small job encompassing some basic security concepts and procedures, or it can be exceedingly complex. The security needs for a three-person desktop publishing firm, for example, would differ wildly from those of a defense contractor supplying top-secret toys to the Pentagon.

From a CompTIA A+ certified technician's perspective, you need to understand the big picture (that's the strategic side), knowing the concepts and available technologies for security. At the implementation level (that's the tactical side), you're expected to know where to find such things as security policies in Windows. A CompTIA Network+ or CompTIA Security+ tech will give you the specific options to implement. (The exception to this level of knowledge comes in dealing with malicious software such as viruses, but we'll tackle that subject as the last part of the chapter.) So let's look at three concept and technology areas: access control, data classification and compliance, and reporting.

Cross Check

Securing Windows Resources

Part of establishing local control over resources involves setting up the computer properly in the first place, a topic covered in depth in Chapter 16. Check your memory of proper setup techniques from that chapter and see if you can answer these questions: How do you establish control over a computer's resources? What file system must you use?

Access Control

Access is the key. If you can control access to the data, programs, and other computing resources, you've secured your systems. **Access control** is composed of four interlinked areas that a good security-minded tech should think about: physical security, authentication, users and groups, and security policies. Much of this you know from previous chapters, but this section should help tie it all together as a security topic.

Secure Physical Area and Lock Down Systems

The first order of security is to block access to the physical hardware from people who shouldn't have access. This isn't rocket science. Lock the door to your workspace. Don't leave a PC unattended when logged in. In fact, don't ever leave a system logged in, even as a limited user. God help you if you walk away from a server still logged in as an administrator. You're tempting fate.

• **Figure 29.4** Typical employee badge/smart card

Employee ID badges are now so common that even relatively small organizations use them. Badges are a great way not only to control building access but also to store authentication tools such as radio frequency identification (RFID) or smart cards (see "Authentication" later in this chapter). Figure 29.4 shows a typical badge.

Be aware of the risk of shoulder surfing. One handy tool to prevent this is a privacy filter. A privacy filter is little more than a framed sheet or film that you apply to the front of your monitor. Privacy filters reduce the viewing angle, making it impossible to see the contents on the screen for anyone except those directly in front of the screen (see Figure 29.5).

Security is more of an issue when users walk away from their computers, even for a moment. When you see a user's computer logged in and unattended, do the user and your company a huge favor and lock the computer. Just walk up and press WINDOWS LOGO KEY-L on the keyboard to lock the system. It works in all versions of Windows. Better yet, make a point to make users aware of this issue so they understand the risk and can take the precaution themselves. You should also instruct them how to password-protect their screensaver. When the password feature is enabled, a user won't be able to return to the desktop until they've entered the proper password. It's a little like locking the computer, and good for those who like using screensavers.

While you're looking at a user's monitor, examine around his or her desk. Is the user writing down passwords and putting them in plain sight?

• **Figure 29.5** Privacy filter

If so, tell the user to get rid of them! Teach users to create easy-to-remember passwords. Are critical, personal, or sensitive documents also lying about in plain sight? The user should put them in a closed, secure place. Documents no longer needed should be shredded immediately.

Authentication

Security requires properly implemented **authentication**, which means in essence how the computer determines who can or should access it and, once accessed, what that user can do. A computer can authenticate users through software or hardware, or a combination of both.

You can categorize ways to authenticate into three broad areas: knowledge factors, ownership factors, and inherent factors. A *knowledge factor* is something the user knows, like a password or personal identification number (PIN). An *ownership factor* is something the user has, like an ID card or security token. An *inherent factor* (also called a biometric) is something that is part of the user, like a fingerprint or retinal pattern.

Multifactor authentication provides the best authentication, where a user must use two or more factors to prove his or her identity. Note that multifactor means more than one factor, not just more than one *thing*. Logging in with a user name and password is two things, for example, but because both fall into the category of what a user knows, it's not multifactor authentication.

Many organizations use *two-factor authentication*. An example is a key fob that generates a numeric key. A user authenticates by entering his or her user name and password (something you know) and is then prompted to enter the key (something you have).

A popular way to remember authentication factors is to think of them as something you know (passwords), something about you (biometric), and something you have (badge, key fob, or security token).

Remember the concept of *single sign-on* from Chapter 5? You can log on to any computer in a domain using one set of credentials. In addition to being a time-saver, this is also a great security feature that helps network administrators better control who can gain access to the network.

Software Authentication: Proper Passwords It's still rather shocking to me to power up a friend's computer and go straight to his or her desktop, or with my married-with-kids friends, to click one of the parents' user account icons and not be prompted for a password. This is just wrong! I'm always tempted to assign passwords right then and there—and not tell them the passwords, of course—so they'll see the error of their ways when they try to log on next. I don't do it but always try to explain gently the importance of good passwords.

You know about passwords from Chapter 16, so I won't belabor the point here. Suffice it to say that you must require that your users have proper passwords. Don't let them write passwords down or tape them to the underside of their mouse pads either!

Cross Check

Proper Passwords

So, what goes into making a good password? Turning once again to Chapter 16, see if you can answer these questions: What sorts of characters should make up a password? Should you ask for a user's password when working on that user's PC? Why or why not? If you're in a secure environment and know you'll have to reboot several times, is it okay to ask for a password then? What should you do?

• **Figure 29.6** CMOS access password request

• **Figure 29.7** Keyboard-mounted smart card reader being used for a commercial application (photo courtesy of Cherry Corp.)

It's not just access to Windows that you need to think about. There's always the temptation for people to do other mean things, such as changing CMOS settings, opening up the case, and even stealing hard drives. Any of these actions renders the computer inoperable to the casual user until a tech can undo the damage or replace components. All modern CMOS setup utilities come with a number of tools to protect your computer, such as drive lock, intrusion detection, and of course system access passwords such as the one shown in Figure 29.6. Refer to Chapter 8 to refresh yourself on what you can do at a BIOS level to protect your computer.

Hardware Authentication Smart cards and biometric devices enable modern systems to authenticate users with more authority than mere passwords. **Smart cards** are credit card–sized cards with circuitry that can identify the bearer of the card. Smart cards are relatively common for such tasks as authenticating users for mass transit systems, for example, but are fairly uncommon in computers. Figure 29.7 shows a smart card and keyboard combination.

Security tokens are devices that store some unique information that the user carries on their person. They may be digital certificates, passwords, or biometric data. They may also store an RSA token. *RSA tokens* are random-number generators that are used with user names and passwords to ensure extra security. Most security tokens come in the form of key fobs, as shown in Figure 29.8.

You can also get many types of security tokens as software. Anyone who plays *World of Warcraft* knows that there's an entire illegal industry known as "gold farmers" who like to hack accounts and steal all the hard-earned loot your character collects. It's a terrible feeling to log in to the game only to find your character cleaned out (see Figure 29.9).

• **Figure 29.8** RSA key fob (photo courtesy of EMC Corp.)

Figure 29.9 I've been robbed! My fine armor is gone, my bags are empty, and my bank account only has a few copper pieces!

To counter this problem, Blizzard Entertainment, the folks who own *World of Warcraft*, provide free security tokens. Most folks think "hardware" in the form of key fobs when they hear the words "security tokens," but you can also download a security token as software—Blizzard offers an app for your smartphone, as shown in Figure 29.10.

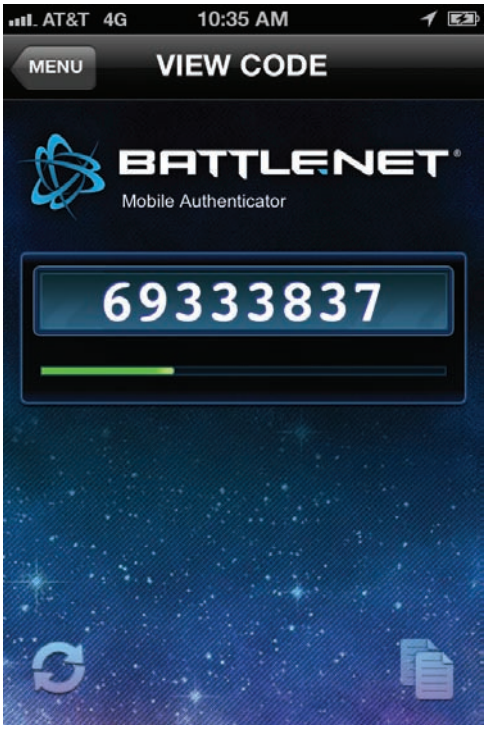


Figure 29.10 Blizzard Entertainment security token for iPhone

People can guess or discover passwords, but it's a lot harder to forge someone's fingerprints. The keyboard in Figure 29.11 authenticates users on a local machine by using fingerprints. Other devices that will do the trick are key fobs and retinal scanners. Devices

Figure 29.11 Microsoft keyboard with fingerprint accessibility

How's this for full disclosure? Microsoft does not claim that the keyboard in Figure 29.11 offers any security at all. In fact, the documentation specifically claims that the fingerprint reader is an accessibility tool, not a security device. Because it enables a person to log on to a local machine, though, I think it falls into the category of authentication devices.

• **Figure 29.12** plusID (photo courtesy of Privaris, Inc.)

that require some sort of physical, flesh-and-blood authentication are called **biometric devices**.

Clever manufacturers have developed key fobs and smart cards that use RFID to transmit authentication information so users don't have to insert something into a computer or card reader. The Privaris plusID combines, for example, a biometric fingerprint fob with an RFID tag that makes security as easy as opening a garage door remotely! Figure 29.12 shows a plusID device.

For some reason, CompTIA lists *retinal scanners* as a form of biometric security. While retinal scanners do exist, I have been in hundreds of high-security facilities and have only seen one retinal scanner in operation in almost 30 years as a tech. CompTIA should remove this silly objective, but until they do, Figure 29.13 shows about the only image of a retinal scanner in operation you'll ever encounter.

NTFS, not FAT32!

The file system on a hard drive matters a lot when it comes to security. On a Windows machine with multiple users, you simply must use NTFS or you have no security at all. Not just primary drives but also any secondary drives in computers in your care should be formatted as NTFS, with the exception of removable drives such as the one you use to back up your system.

When you run into a multiple-drive system that has a second or third drive formatted as FAT32, you can use the **convert** command-line utility to go from FAT to NTFS. The syntax is pretty straightforward. To convert a D: drive from FAT or FAT32 to NTFS, for example, you'd type the following:

```
convert d: /fs:ntfs
```

• **Figure 29.13** Retinal scanner in *Half-Life 2*

You can substitute a mount name in place of the drive letter in case you have a mounted volume. The command has a few extra switches as well, so at the command prompt, type **/?** after the convert command to see all of your options.

Users and Groups

Windows uses user accounts and groups as the bedrock of access control. A user account is assigned to a group, such as Users, Power Users, or Administrators, and by association gets certain permissions on the computer. Using NTFS enables the highest level of control over data resources.

Assigning users to groups is a great first step in controlling a local machine, but this feature really shines once you go to a networked environment. Let's go there now.

User Account Management Through Groups

Access to user accounts should be restricted to the assigned individuals, and those who configure the permissions to those accounts must remember the *principle of least privilege* discussed in Chapter 16: Accounts should have permission to access only the resources they need and no more. Tight control of user accounts is critical to preventing unauthorized access. Disabling unused accounts is an important part of this strategy, but good user account management goes far deeper than that.

Groups are a great way to achieve increased complexity without increasing the administrative burden on network administrators, because all operating systems combine permissions. When a user is a member of more than one group, which permissions does that user have with respect to any particular resource? In all operating systems, the permissions of the groups are *combined*, and the result is what you call the **effective permissions** the user has to access the resource. As an example, if Rita is a member of the Sales group, which has List Folder Contents permission to a folder, and she is also a member of the Managers group, which has Read and Execute permissions to the same folder, Rita will have both List Folder Contents *and* Read and Execute permissions to that folder.

Watch out for *default* user accounts and groups—they can become secret backdoors to your network! All network operating systems have a default Everyone group that can be used to sneak into shared resources easily. This Everyone group, as its name implies, literally includes anyone who connects to that resource. Windows gives full control to the Everyone group by default, for example, so make sure you know to lock this down! The other scary one is the Guest account. The Guest account is the only way to access a system without a user name and password. Unless you have a compelling reason to provide guest access, you should always make sure the Guest account is disabled.

All of the default groups—Everyone, Guest, Users—define broad groups of users. Never use them unless you intend to permit all of those folks access to a resource. If you use one of the default groups, remember to configure them with the proper permissions to prevent users from doing things you don't want them to do with a shared resource!

Security Policies

Although permissions control how users access shared resources, there are other functions you should control that are outside the scope of resources. For example, do you want users to be able to access a command prompt on their Windows system? Do you want users to be able to install software? Would you like to control what systems a user can log on to or at what time of day a user can log on? All network operating systems provide you with some capability to control these and literally hundreds of other security parameters, under what Windows calls *policies*. I like to think of policies as permissions for activities, as opposed to true permissions, which control access to resources.

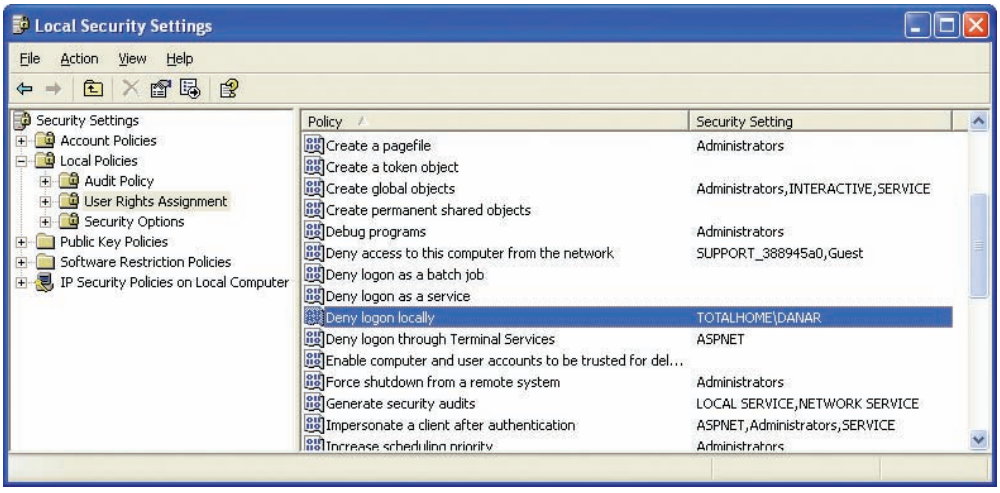
When you open the Local Security Policy tool in Windows XP, note that the program is labeled "Local Security Settings," even though the icon is labeled "Local Security Policy." In Windows Vista and Windows 7, it is always called Local Security Policy.

A policy is usually applied to a user account, a computer, or a group. Let's use the example of a network composed of Windows XP Professional systems with a Windows Server 2008 system. Every Windows XP system has its own local policies program, which enables policies to be placed on that system only. Figure 29.14 shows the tool you use to set local policies on an individual system, called **Local Security Policy**, being used to deny the user account Danar the capability to log on locally.

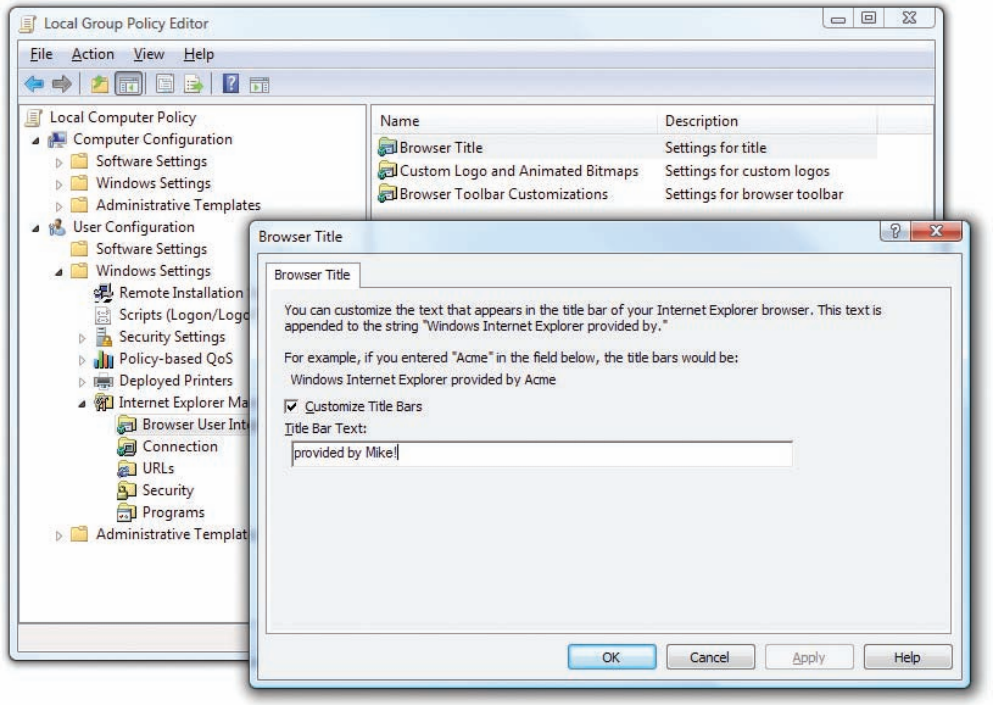
Local policies work great for individual systems, but they can be a pain to configure if you want to apply the same settings to more than one PC on your network. If you want to apply policy settings *en masse*, you need to step up to Windows Active Directory domain-based **Group Policy**. By using Group Policy, you can exercise deity-like—Microsoft prefers to use the term *granular*—control over your network clients.

Want to set default wallpaper for every PC in your domain? Group Policy can do that. Want to make certain tools inaccessible to everyone except authorized users? Group Policy can do that, too. Want to control access to the Internet, redirect home folders, run scripts, deploy software, or just remind folks that unauthorized access to the network will get them nowhere fast? Group Policy is the answer. Figure 29.15 shows Group Policy; I'm about to change the default title on every instance of Internet Explorer on every computer in my domain!

That's just one simple example of the settings you can configure by using Group Policy. You can apply literally hundreds of tweaks through Group Policy, from the great to the small, but don't worry too much about familiarizing yourself with each and every one. Group Policy settings are a big topic on most of the Microsoft certification tracks, but for the purposes of the CompTIA A+ exams, you simply have to be comfortable with the concept behind Group Policy.



• **Figure 29.14** Local Security Policy



• **Figure 29.15** Using Group Policy to make IE title say "provided by Mike!"

Although I could never list every possible policy you can enable on a Windows system, here's a list of some commonly used ones:

- **Prevent Registry Edits** If you try to edit the Registry, you get a failure message.
- **Prevent Access to the Command Prompt** Keeps users from getting to the command prompt by turning off the Run command and the Command Prompt shortcut.
- **Log on Locally** Defines who may log on to the system locally.
- **Shut Down System** Defines who may shut down the system.
- **Minimum Password Length** Forces a minimum password length.
- **Account Lockout Threshold** Sets the maximum number of logon attempts a person can make before being locked out of the account.
- **Disable Windows Installer** Prevents users from installing software.
- **Printer Browsing** Enables users to browse for printers on the network, as opposed to using only assigned printers.

Although the CompTIA A+ exams don't expect you to know how to implement policies on any type of network, you are expected to understand that policies exist, especially on Windows networks, and that they can do amazing things to control what users can do on their systems. If you ever try to get to a command prompt on a Windows system only to discover the Run command is dimmed, blame it on a policy, not the computer!

Data Classification and Compliance

Larger organizations, such as government entities, benefit greatly from organizing their data according to its sensitivity—what's called **data classification**—and making certain that computer hardware and software stay as uniform as possible. In addition, many government and internal regulations apply fairly rigorously to the organizations.

Data classification systems vary by the organization, but a common scheme classifies documents as public, internal use only, highly confidential, top secret, and so on. Using a classification scheme enables employees such as techs to know very quickly what to do with documents, the drives containing documents, and more. Your strategy for recycling a computer system left from a migrated user, for example, will differ a lot if the data on the drive was classified as internal use only or top secret.

Compliance means, in a nutshell, that members of an organization or company must abide by or comply with all of the rules that apply to the organization or company. Statutes with funny names such as Sarbanes-Oxley impose certain behaviors or prohibitions on what people can and cannot do in the workplace.

From a technician's point of view, the most common compliance issue revolves around software, such as what sort of software users can be allowed to install on their computers or, conversely, why you have to tell a user that he can't install the latest application that may help him do the job more effectively because that software isn't on the approved list. This can lead to some uncomfortable confrontations, but it's part of a tech's job.

The concepts behind compliance in IT are not, as some might imagine at first blush, to stop you from being able to work effectively. Rather they're designed to stop users with not quite enough technical skill or knowledge from installing malicious programs or applications that will destabilize their systems. This keeps technical support calls down and enables techs to focus on more serious problems.

Reporting

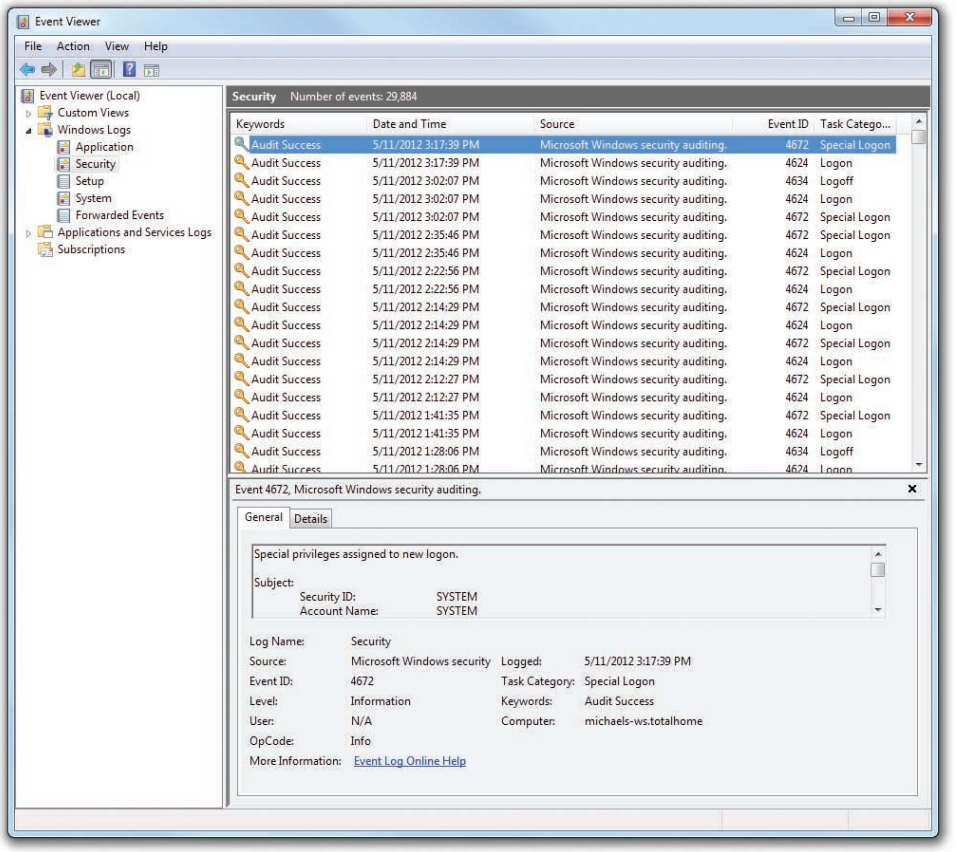
As a final weapon in your security arsenal, you need to report any security issues so a network administrator or technician can take steps to make them go away. You can set up auditing within Windows so that the OS reports problems to you. **Event Viewer** enables you to read the logs created by auditing. You can then do your work and report those problems. Let's take a look.

Auditing

The Security section of Event Viewer doesn't show you anything by default. To unlock the full potential of Event Viewer, you need to set up auditing. *Auditing* in the security sense means to tell Windows to create an entry in the Security Log when certain events happen, such as when a user logs on—called **event auditing**—or tries to access a certain file or folder—called **object access auditing**. Figure 29.16 shows Event Viewer tracking logon and logoff events.

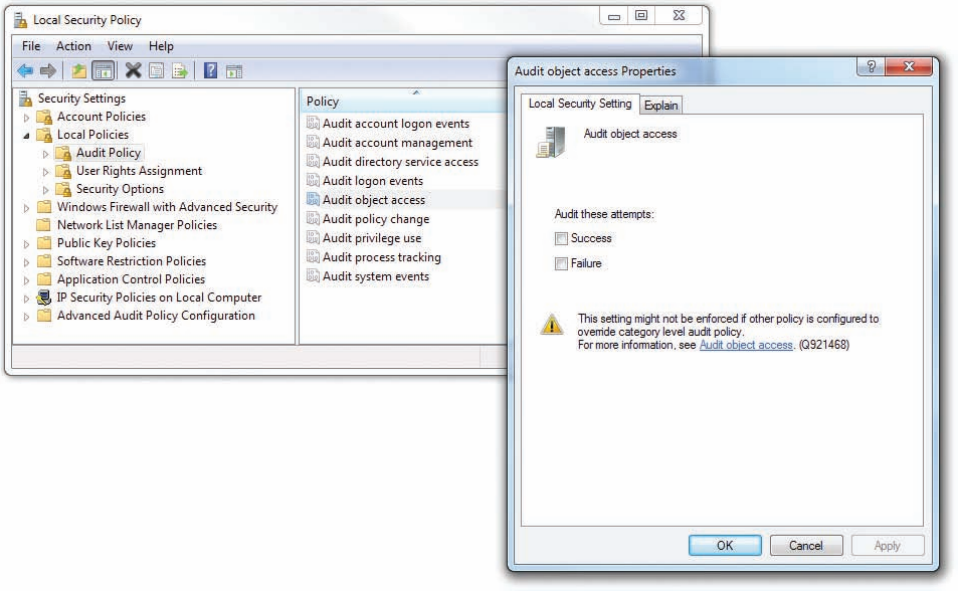
Event Viewer stores log files in %SystemRoot%\System32\Config.

The CompTIA A+ certification exams don't test you on creating a brilliant auditing policy for your office—that's what network administrators



• **Figure 29.16** Event Viewer displaying security alerts

do. You simply need to know what auditing does and how to turn it on or off so you can provide support for the network administrators in the field. To turn on auditing at a local level, go to Local Security Policy in Administrative Tools. Select Local Policies and then click Audit Policy. Double-click one of the policy options and select one or both of the checkboxes in the Properties dialog box that opens. Figure 29.17 shows the Audit object access Properties dialog box.



• **Figure 29.17** Audit object access Properties dialog box, with Local Security Policy open in the background

Incidence Reporting

Once you've gathered data about a particular system or you've dealt with a computer or network problem, you need to complete the mission by telling your supervisor. This is called **incidence**

reporting. Many companies have pre-made forms that you simply fill out and submit. Other places are less formal. Regardless, you need to do this!

Incidence reporting does a couple of things for you. First, it provides a record of work you've accomplished. Second, it provides a piece of information that, when combined with other information you might or might not know, reveals a pattern or bigger problem to someone higher up the chain. A seemingly innocuous security audit report, for example, might match other such events in numerous places in the building at the same time and thus show that conscious, coordinated action rather than a glitch was at work.

Evidence Handling

Look for evidence handling questions on the 220-801 exam.

As a tech, you'll need to deal with people who use company computers in prohibited ways. In most cases, you're not paid to be the police and should not get involved. There are times, however, where something bad—really bad—takes place on one of the systems you support, and if you're the first tech person there, everyone is going to turn to you for action.

A technician should ignore personal information in and around a person's computer. As mentioned back in Chapter 2, you should treat anything said to you and anything you see as a personal confidence, not to be repeated to customers, coworkers, or bosses. Here's Mike's Rule of Confidentiality: "Unless it's a felony or an imminent physical danger, you didn't see nothin'." This includes any confidential customer materials. Try not to look at anything that isn't directly related to your job. (Sometimes that's impossible, but limit your exposure.) If you're waiting on a printout at a printer and suddenly there's a bunch of printed pages coming out of the printer with employee payroll information, set it to the side and pretend you never saw it.

But what about the scary stuff? Obvious espionage? Pornography? People passing out personal information? Hacking? In these cases, you've just become the first line of defense and you need to act accordingly. Let's address the objectives as listed by CompTIA for the 220-801 exam.

The SANS Institute provides an excellent boilerplate Acceptable Use Policy on their Web site: www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf.

Identify the Action or Content as Prohibited Use common sense, but keep in mind that most organizations have an Acceptable Use Policy that employees must sign. The Acceptable Use Policy defines what actions employees may or may not perform on company equipment. Remember that these polices aren't just for obvious issues such as using a computer for personal use. These policies cover computers, phones, printers, and even the network itself. This policy will define the handling of passwords, e-mail, and many other issues.

Report Through Proper Channels In most cases, you'll report any prohibited actions or content directly to your supervisor. There's also a chance your company will have a security officer or incident response leader who you'll contact instead. Do *not* speak to the person committing the infraction unless your supervisor approves that contact.

Data/Device Preservation You might end up in a situation serious enough that a computer or other device becomes evidence. In these cases, the location of the system and who has touched it may come into question, so you need to establish a **chain of custody**: a documented history of who has been

in possession of the system. You'll hopefully have a legal expert to guide you, but the following are fairly common rules:

1. Isolate the system. Shut down the system and store it in a place where no one else can access it.
2. Document when you took control of the system and the actions you took: shutting it down, unplugging it, moving it, and so on. Don't worry about too much detail, but you must track its location.
3. If another person takes control of the system, document the transfer of custody.

802

Network Security

Networks are under threat from the outside as well, so this section looks at issues involving Internet-borne attacks, firewalls, and wireless networking. This content is the security bread and butter for a CompTIA A+ technician, so you need to understand the concepts and procedures and be able to implement them properly.

Malicious Software

The beauty of the Internet is the ease of accessing resources just about anywhere on the globe, all from the comfort of your favorite chair. This connection, however, runs both ways, and people from all over the world can potentially access your computer from the comfort of their evil lairs. The Internet is awash with malicious software that is, even at this moment, trying to infect your systems.

The term **malware** defines any program or code (macro, script, and so on) that's designed to do something on a system or network that you don't want done. Malware comes in quite a variety of guises, such as grayware, spam, viruses, worms, macros, Trojan horses, and rootkits. Let's examine all these malware flavors and then explore how to deal with them.

Grayware

Programs that intrude unwanted into your computing experience but don't actually do any damage to your systems or data—what's called **grayware**—can make that computing experience less than perfect. On most systems, the Internet Web browser client is the most often used piece of software. Over the years, Web sites have come up with more and more ways to try to get you to see what they want you to see: their advertising. When the Web first got underway, we were forced to look at an occasional banner ad. In the past few years, Web site designers have become much more sophisticated, creating a number of intrusive and irritating ways to get you to part with your money in one form or another.

The term *adware* generally refers to programs that support themselves using revenue from ads, like all those "free" Internet game sites. Every once in a while those ads can lead to spyware installing on a system, making many authors lump adware into the grayware category.

There are basically two irritating grayware types: pop-ups and spyware. **Pop-ups** are those surprise browser windows that appear automatically when you visit a Web site, proving themselves irritating and unwanted and nothing else. **Spyware**, meanwhile, defines a family of programs that run in the background on your PC, sending information about your browsing habits to the company that installed it on your system. Of the two, spyware is much less noticeable but far more nefarious.

Pop-Ups Getting rid of pop-ups is actually rather tricky. You've probably noticed that most of these pop-up browser windows don't look like browser windows at all. They have no menu bar, button bar, or address window, yet they are separate browser windows. HTML coding permits Web site and advertising designers to remove the usual navigation aids from a browser window so all you're left with is the content. In fact, as I'll describe in a minute, some pop-up browser windows are deliberately designed to mimic similar pop-up alerts from the Windows OS. They might even have buttons similar to Windows' own exit buttons, but you might find that when you click them, you wind up with more pop-up windows instead! What to do?

The first thing you need to know when dealing with pop-ups is how to close them without actually having to risk clicking them. As I said, most pop-ups have removed all navigation aids, and many are also configured to appear on your monitor screen in a position that places the browser window's exit button—the little *X* button in the upper-right corner—outside of your visible screen area. Some even pop up behind the active browser window and wait there in the background. Most annoying! To remedy this, use alternate means to close the pop-up browser window. For instance, you can right-click the browser window's taskbar icon to generate a pop-up menu of your own. Select Close, and the window should go away. You can also press ALT-TAB to bring the browser window in question to the forefront and then press ALT-F4 to close it.

Most Web browsers have features to prevent pop-up ads in the first place, but I've found that these types of applications are sometimes *too* thorough. That is, they tend to prevent *all* new browser windows from opening, even those you want to view. Applications such as AdSubtract control a variety of Internet annoyances, including pop-up windows, cookies, and Java applets, and are more configurable—you can specify what you want to allow on any particular domain address—but the fully functional versions usually cost at least something, and that much control is too confusing for most novice-level users.

Spyware Some types of spyware go considerably beyond grayware's level of intrusion. They can use your computer's resources to run *distributed computing* applications, capture your keystrokes to steal passwords, reconfigure your dial-up settings to use a different phone number at a much higher connection charge, or even use your Internet connection and e-mail address list to propagate itself to other computers in a virus-like fashion! Are you concerned yet?

Setting aside the legal and ethical issues—and there are many—you should at least appreciate that spyware can seriously impact your PC's performance and cause problems with your Internet connection. The threat is real, so what practical steps can you take to protect yourself? Let's look

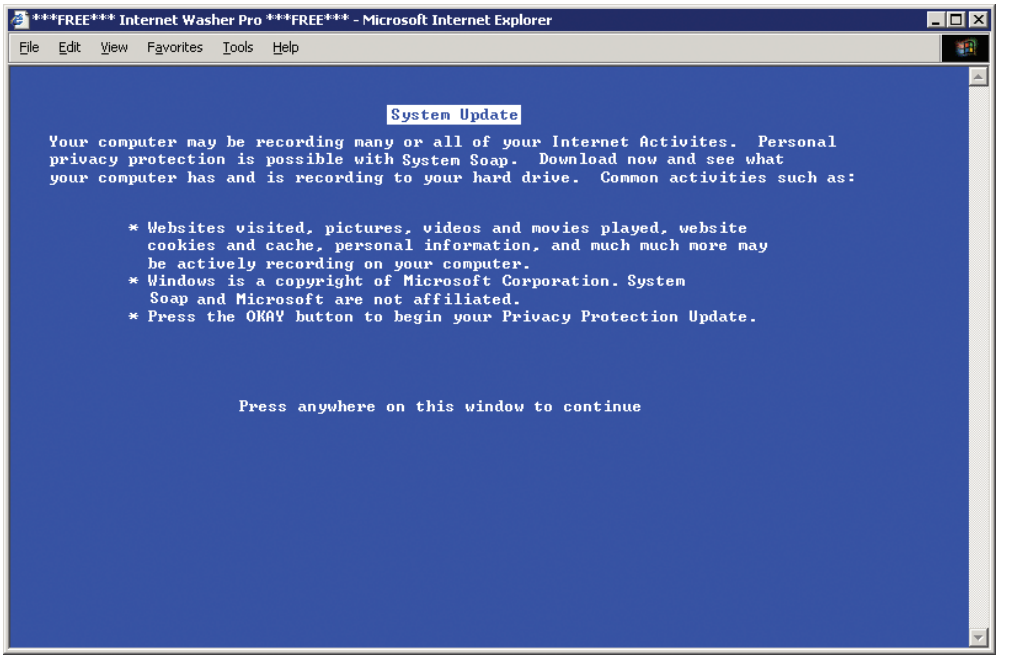
at how to prevent spyware installation and how to detect and remove any installed spyware.

How does this spyware get into your system in the first place? Obviously, sensible people don't download and install something that they know is going to compromise their computers. Makers of spyware know this, so they bundle their software with some other program or utility that purports to give you some benefit.

What kind of benefit? In 2005, Movieland (otherwise known as Movieland.com and Popcorn.net) released a "handy" movie download service. They didn't tell users, of course, that everyone who installed the software was "automatically enrolled" in a three-day trial. If you didn't cancel the "trial," a pop-up window filled your screen demanding you pay them for the service that you never signed up for. The best part, however, was that you couldn't uninstall the application completely. The uninstaller redirected users to a Web page demanding money again. (Movieland was shut down in 2007.) As you can see, spyware doesn't need to force its way into a PC. Instead, it saunters calmly through the front door.

Another popular spyware method is to use pop-up browser windows crudely disguised as Windows' own system warnings (see Figure 29.18). When clicked, these may trigger a flood of other browser windows, or may even start a file download.

If Movieland was a problem back in 2005, what are the big spyware applications today? Unfortunately, I can't tell you—not because it's a secret, but because we don't know about them yet. Look at Figure 29.19: the dialog box asks the user if she trusts the Gator Corporation (a well-known spyware producer from several years ago). Because everyone eventually knew not to trust Gator, they would click No, and the company faded away several years ago. Gator, however, was incredibly well-known at the time. What about those small, unknown applications waiting in the dark corners



• **Figure 29.18** A spyware pop-up browser window, disguised as a Windows alert

• **Figure 29.19** Gator Corporation's acknowledgment warning

of the Internet—the ones that just might have spyware hiding inside? How do you protect yourself from them?

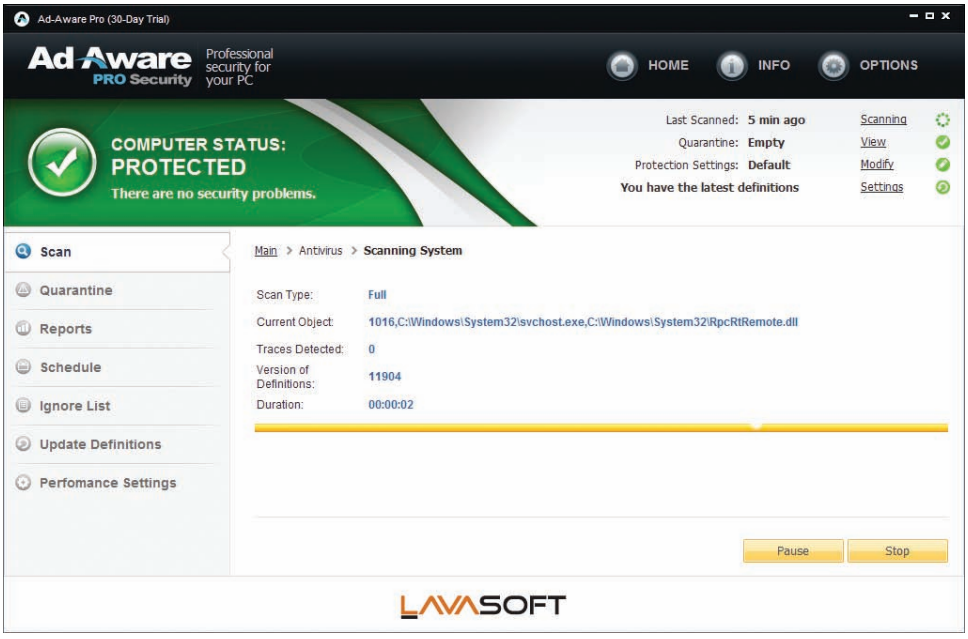
The lesson here is simple: *Don't install these programs*, at least not without researching the program first. Careful reading of the software's license agreement before you install a program is a good idea, but realistically, it does little to protect your PC. With that in mind, here are a couple of preventive measures you can take to keep parasitic software off of your system.

If you visit a Web site that prompts you to install a third-party application or plug-in that you've never heard of, *don't install it*. Well-known and reputable plug-ins, such as Adobe's Shockwave or Flash, are safe, but be suspicious of any others. Don't click *anywhere* inside of a pop-up browser window, even if it looks just like a Windows alert window or DOS command-line prompt—as I just mentioned, it's probably fake and the Close button is likely a hyperlink. Instead, use other means to close the window, such as pressing ALT-F4 or right-clicking the browser window's icon on the taskbar and selecting Close.

You can also install spyware detection and removal software on your system and run it regularly. Let's look at how to do that.

Some spyware makers are reputable enough to include a routine for uninstalling their software. Gator, for instance, made it fairly easy to get rid of their programs; you just used the Windows Add/Remove Programs or Programs and Features applet in the Control Panel. Others, however, aren't quite so cooperative. In fact, because spyware is so—well, *sneaky*—it's entirely possible that your system already has some installed that you don't even know about. How do you discover it?

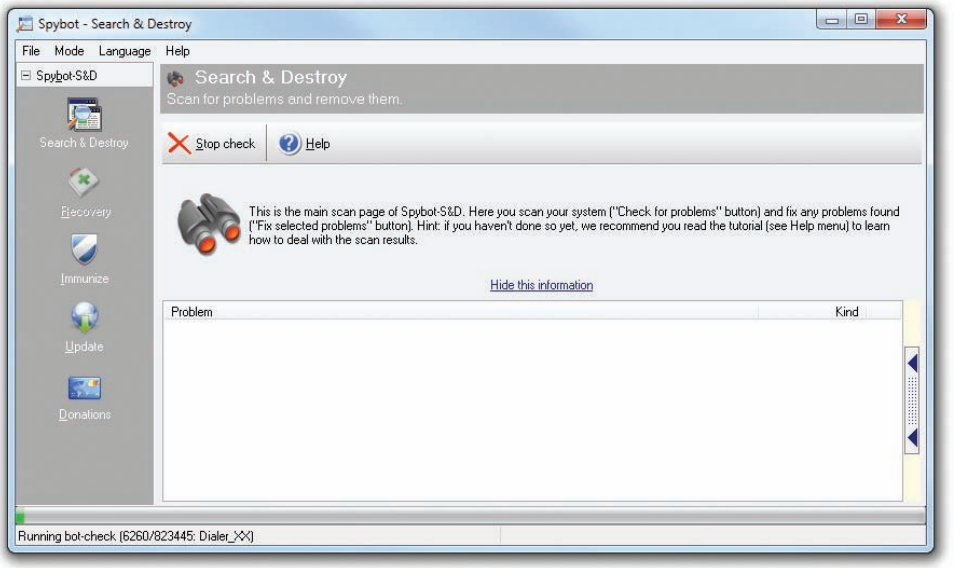
Windows comes with Windows Defender, a fine tool for catching most spyware, but it's not perfect. The better solution is to back up Windows Defender with a second spyware removal program. There are several on the market, but two that I highly recommend are Lavasoft's Ad-Aware (see Figure 29.20) and Safer Networking's Spybot Search & Destroy.



• **Figure 29.20** Lavasoft's Ad-Aware

Both of these applications work exactly as advertised. They detect and delete spyware of all sorts—hidden files and folders, cookies, Registry keys and values, you name it. Ad-Aware is free for personal use, while Spybot Search & Destroy is shareware (see Figure 29.21).

Many times I've used both programs at the same time because one tends to catch what the other misses.



• **Figure 29.21** Spybot Search & Destroy

Spam

E-mail that comes into your Inbox from a source that's not a friend, family member, or colleague, and that you didn't ask for, can create huge problems for your computer and you. This unsolicited e-mail, called **spam**, accounts for a huge percentage of traffic on the Internet. Spam comes in many flavors, from legitimate businesses trying to sell you products to scammers who just want to take your money. Hoaxes, pornography, and get-rich-quick schemes pour into the Inboxes of most e-mail users. They waste your time and can easily offend.

You can use several options to cope with the flood of spam. The first option is defense. Never post your e-mail address on the Internet. One study tested this theory and found that *over 97 percent* of the spam received during the study went to e-mail addresses they had posted on the public Internet.

Filters and filtering software can block spam at your mail server and at your computer. Google Mail has powerful blocking schemes, for example, that drop the average spam received by its subscribers by a large percentage, usually more than 90 percent. You can set most e-mail programs to block e-mail from specific people—good to use if someone is harassing you—or to specific people. You can block by subject line or keywords. Most people use a third-party antispam program instead of using the filters in their e-mail program.

A lot of spam contains malware or points to dangerous Web sites. Never click on any link or open an e-mail from someone you don't know! You might just save your computer.

Spam is also notorious for phishing scams. Phishing works by sending you an e-mail message that looks legitimate, like a bill or account information, hoping you will enter important personal information. If you receive an e-mail from Amazon.com, ebay.com, or some other site (like your bank), don't click on it! Like Admiral Ackbar said in *Star Wars*, "It's a trap!"

Try This!

Spybot

If you haven't done this already, do it now. Go to www.safer-networking.org and download the latest copy of Spybot Search & Destroy. Install it on your computer and run it. Did it find any spyware that slipped in past your defenses?

Try This!

Fight Spam Right!

Spam filtering software that you purchase and put on your computer can help, but you have to do some research to see which software offers the best performance. You want to avoid software that causes *false positives*—mislabeling acceptable e-mail as spam—because you'll miss legitimate e-mail messages from family and friends. So, fire up your trusty Web browser and do some searching.

Start by going to Google and searching for **antispam software reviews**. One of the first sites that should come up takes you to *PC Magazine*'s review list, which is kept up to date. What's the current Editor's Choice? What other options do you have?

Virus

A **virus** is a program that has two jobs: to replicate and to activate. *Replication* means it makes copies of itself, often as code stored in boot sectors or as extra code added to the end of executable programs. *Activation* is when a virus does something like erase the boot sector of a drive. A virus only replicates to other drives, such as thumb drives or optical media. It does not replicate across networks. Plus, a virus needs human action to spread.

Worm

A **worm** functions similarly to a virus, though it replicates exclusively through networks. A worm, unlike a virus, doesn't have to wait for someone to use a removable drive to replicate. If the infected computer is on a network, a worm will immediately start sending copies of itself to any other computers on the network it can locate. Worms can exploit inherent flaws in program code like *buffer overflows*, where a buffer cannot hold all the data sent to it.

Macro

A **macro** is any type of virus that exploits application macros to replicate and activate. A *macro* is also programming within an application that enables you to control aspects of the application. Macros exist in any application that has a built-in macro language, such as Microsoft Excel, that users can program to handle repetitive tasks (among other things).

Trojan Horse

A **Trojan horse** is a piece of malware that looks or pretends to do one thing while, at the same time, doing something evil. A Trojan horse may be a game, like poker, or a free screensaver. The sky is the limit. The more "popular" Trojan horses turn an infected computer into a server and then open TCP or UDP ports so a remote user can control the infected computer. Trojan horses can be used to capture keystrokes, passwords, files, credit card information, and more. Trojan horses do not replicate.

Rootkit

For a virus or Trojan horse to succeed, it needs to come up with some method to hide itself. As awareness of malware has grown, anti-malware programs make it harder to find new locations on a computer to hide malware. A **rootkit** is a Trojan horse that takes advantage of very low-level operating system functions to hide itself from all but the most aggressive of anti-malware tools. Worse, a rootkit, by definition, gains privileged access to the computer. Rootkits can strike operating systems, hypervisors, and even firmware.

The most infamous rootkit appeared a few years ago as an antipiracy attempt by Sony on its music CDs. Unfortunately for the media giant, the rootkit software installed when you played a music CD and opened a backdoor that could be used for malicious intent.

Malware Signs and Symptoms

If your PC has been infected by malware, you'll bump into some strange things before you can even run an anti-malware scan. Like a medical condition, malware causes unusual symptoms that should stand out from your everyday computer use. You need to become a PC physician and understand what each of these symptoms means.

Malware's biggest strength is its flexibility: it can look like anything. In fact, a lot of malware attacks can feel like normal PC "wonkiness"—momentary slowdowns, random one-time crashes, and so on. Knowing when a weird application crash is actually a malware attack is half the battle.

A slow PC can mean you're running too many applications at once or you've been hit with malware. How do you tell the difference? In this case, it's the frequency. If it's happening a lot, even when all of your applications are closed, you've got a problem. This goes for frequent lockups, too. If Windows starts misbehaving (more than usual), run your anti-malware application right away.

Malware, however, doesn't always jump out at you with big system crashes. Some malware tries to rename system files, change file permissions, or hide files completely. Most of these issues are easily caught by a regular anti-malware scan, so as long as you remain vigilant, you'll be okay.

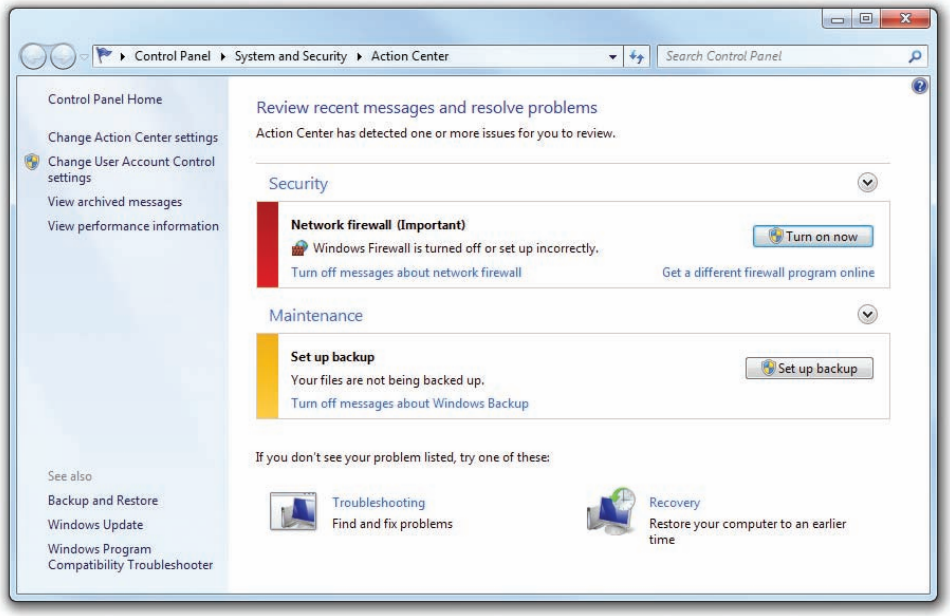
Some malware even fights back, defending itself from your many attempts to remove it. If your Windows Update feature stops working, preventing you from patching your PC, you've got malware. If other tools and utilities throw up an "Access Denied" road block, you've got malware. If you lose all Internet connectivity, either the malware is stopping you or removing the malware broke your connection. In this case, you might need to reconfigure your Internet connection: reinstall your NIC and its drivers, reboot your router, and so on.

Even your browser and anti-malware applications can turn against you. If you type in one Web address and end up at a different site than you anticipated, a malware infection might have overwritten your HOSTS file. The HOSTS file overrules any DNS settings and can redirect your browser to whatever site the malware adds to the file. Most browser redirections

While it's not necessarily a malware attack, watch out for hijacked e-mail accounts, too, belonging either to you or to someone you know. Hackers can hit both e-mail clients and Webmail users. If you start receiving some fishy (or phishy) e-mail messages, change your Webmail user name and password or scan your PC for malware.

point you to phishing scams or Web sites full of free downloads (that are, of course, covered in malware). In fact, some free anti-malware applications are actually malware—what techs call a *rogue anti-malware* program. You can avoid these rogue applications by sticking to the recommended lists of anti-malware software found online.

Watch for security alerts in Windows, either from Windows' built-in security tools or from your third-party anti-malware program. Windows XP (SP2 and later) and Windows Vista include the Security Center, a Control Panel applet that monitors your software firewall, automatic updates, malware protection, and more. Windows 7 includes a similar tool, but calls it the Action Center, which you learned about back in Chapter 19 (see Figure 29.22). You don't actually configure much using these applets; they just tell you whether or not you are protected. Both of these tools place an icon and pop up a notification in the notification area whenever Windows detects a problem. Windows XP and Vista use a red shield with a white × to notify you, while Windows 7 uses a white flag.



• **Figure 29.22** Windows 7 Action Center

Malware Prevention and Recovery

The only way to protect your PC permanently from getting malware is to disconnect it from the Internet and never permit any potentially infected software to touch your precious computer. Because neither scenario is likely these days, you need to use specialized anti-malware programs to help stave off the inevitable assaults. Even with the best anti-malware tools, there are times when malware still manages to strike your computer. When you discover infected systems, you need to know how to stop the spread of the malware to other computers, how to fix infected computers, and how to remediate (restore) the system as close to its original state as possible.

Dealing with Malware

You can deal with malware in several ways: anti-malware programs, training and awareness, patch management, and remediation.

At the very least, every computer should run an anti-malware program. If possible, add an appliance that runs anti-malware programs against incoming data from your network. Also remember that an anti-malware program is only as good as its updates—keep everyone's definition file (explained a bit later) up to date with, literally, nightly updates! Users must be trained to look for suspicious ads, programs, and pop-ups, and

understand that they must not click these things. The more you teach users about malware, the more aware they'll be of potential threats. Your organization should have policies and procedures in place so everyone knows what to do if they encounter malware. Finally, a good tech maintains proper incident response records to see if any pattern to attacks emerges. He or she can then adjust policies and procedures to mitigate these attacks.

One of the most important malware mitigation procedures is to keep systems under your control patched and up to date through proper *patch management*. Microsoft does a very good job of putting out bug fixes and patches as soon as problems occur. If your systems aren't set up to update automatically, then perform manual updates regularly.

Anti-Malware Programs

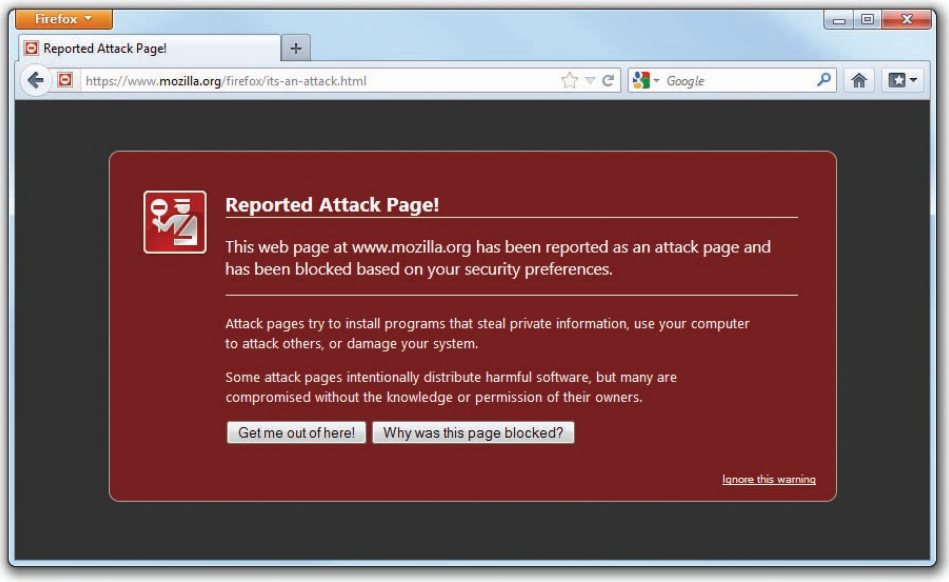
An **anti-malware program** such as a classic **antivirus program** protects your PC in two ways. It can be both sword and shield, working in an active seek-and-destroy mode and in a passive sentry mode. When ordered to seek and destroy, the program scans the computer's boot sector and files for viruses and, if it finds any, presents you with the available options for removing or disabling them. Antivirus programs can also operate as **virus shields** that passively monitor a computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

The term *antivirus* (and antispyware, or anti-anything) is becoming obsolete. Viruses are only a small component of the many types of malware. Many people continue to use the term as a synonym for anti-malware.

Antivirus programs use different techniques to combat different types of viruses. They detect boot sector viruses simply by comparing the drive's boot sector to a standard boot sector. This works because most boot sectors are basically the same. Some antivirus programs make a backup copy of the boot sector. If they detect a virus, the programs use that backup copy to replace the infected boot sector. Executable viruses are a little more difficult to find because they can be on any file in the drive. To detect executable viruses, the antivirus program uses a library of signatures. A **signature** is the code pattern of a known virus. The antivirus program compares an executable file to its library of signatures. There have been instances where a perfectly clean program coincidentally held a virus signature. Usually the antivirus program's creator provides a patch to prevent further alarms. Now that you understand the types of viruses and how antivirus programs try to protect against them, let's review a few terms that are often used when describing certain traits of viruses.

Polymorphic/Polymorphs A **polymorph virus** attempts to change its signature to prevent detection by antivirus programs, usually by continually scrambling a bit of useless code. Fortunately, the scrambling code itself can be identified and used as the signature—once the antivirus makers become aware of the virus. One technique used to combat unknown polymorphs is to have the antivirus program create a checksum on every file in the drive. A *checksum* in this context is a number generated by the software based on the contents of the file rather than the name, date, or size of that file. The algorithms for creating these checksums vary among different antivirus programs (they are also usually kept secret to help prevent virus makers from coming up with ways to beat them). Every time a program is run, the antivirus program calculates a new checksum and compares it with the earlier calculation. If the checksums are different, it is a sure sign of a virus.

Stealth The term "stealth" is more of a concept than an actual virus function. Most **stealth virus** programs are boot sector viruses that use various methods to hide from antivirus software. The AntiEXE stealth virus hooks on to a little-known but often-used software interrupt, for example, running only when that interrupt runs. Others make copies of innocent-looking files.



• **Figure 29.23** Attack site warning

Mozilla provides a sample Web site that displays the attack site sign—a great way to show users what it looks like: www.mozilla.org/firefox/its-an-attack.html.

User Education

A powerful tool to prevent malware attacks and to reduce the impact of malware attacks when they happen is to educate your users. Teach users to be cautious of incoming e-mail they don't clearly recognize and to never click on an attachment or URL in an e-mail unless they are 100 percent certain of the source.

Explain to users the dangers of going to questionable Web sites and teach them how to react when they see questionable actions take place. Let's look at a few of the more evil ones. All Web browsers have built-in attack site warnings like the one shown in Figure 29.23.

Nobody wants their systems infected with malware. Users are motivated and happy when you give them the skills necessary to protect themselves. The bottom line is that educated and aware users will make your life a lot easier.

Malware Prevention Tips

The secret to preventing damage from a malicious software attack is to keep from getting malware on your system in the first place. As discussed earlier, for example, all good antivirus programs include a virus shield that scans e-mail, downloads, running programs, and so on automatically (see Figure 29.24).

• **Figure 29.24** A virus shield in action

Use your antivirus shield. It is also a good idea to scan PCs daily for possible virus attacks. All antivirus programs include terminate-and-stay resident programs (TSRs) that run every time the PC is booted. Last but not least, know the source of any software before you load it. Although the chance of commercial, shrink-wrapped software having a virus is virtually nil (there have been a couple of well-publicized exceptions), that copy of *Call of Duty: Modern Warfare 3* you borrowed from a local hacker should definitely be inspected with care.

Keep your antivirus and anti-malware programs updated. New viruses and other malware appear daily, and your programs

need to know about them. The list of virus signatures your antivirus program can recognize, for example, is called the **definition file**, and you must keep that definition file up to date so your antivirus software has the latest signatures. Fortunately, most antivirus programs update themselves automatically. Further, you should periodically update the core anti-malware software programming—called the *engine*—to employ the latest refinements the developers have included.

Try This!

Scoring Excellent Anti-Malware Programs

You can download many excellent anti-malware programs for free, either for extended trial periods or for indefinite use. Since you need these programs to keep your systems happy, Try This! Download one or more anti-malware programs, such as the following:

- **Windows Defender** Windows Defender is a good antispyware program, but it won't protect you against any other form of malware. It's free with Windows, however, and better than nothing.
- **Microsoft Security Essentials** Recognizing the shortcomings of Windows Defender and no longer willing to count on users to download and install third-party programs, Microsoft offers a complete anti-malware solution called Microsoft Security Essentials. You can download this program for free from Microsoft (search for Microsoft Security Essentials). This program automatically shuts off Windows Defender when installed.
- **Malwarebytes Anti-Malware (www.malwarebytes.org)** Malwarebytes' Anti-Malware program rocks the house in terms of dealing with malicious software. They offer both a free version that scans your computer for malware and quarantines it and a PRO version that actively protects against any incoming malware. Anti-Malware is my first choice in dealing with malware on a client's computer.
- **Lavasoft Ad-Aware (www.lavasoft.com)** Ad-Aware is an excellent antispyware program. Ad-Aware will root out all sorts of files and programs that can cause your computer to run slowly (or worse).
- **Spybot Search & Destroy (www.safer-networking.org)** Spybot Search & Destroy from Safer Networking Ltd. is another superb antispyware program. Many folks use both Ad-Aware and Spybot—though sometimes the two programs detect each other as spyware!
- **AVG Anti-Virus (http://free.avg.com)** AVG offers a free version of their antivirus software for noncommercial use. Updated regularly to add the latest virus signatures, the software will keep your system clean and bug free.

Boot CD Anti-Malware Tools

If you run anti-malware software and your computer still gets infected, especially after a reboot, you need a more serious anti-malware tool. Many anti-malware companies provide bootable CDs or flash drives (or show you how to make one) that enable you to boot from a known-clean OS and run the same anti-malware software, but this time not corrupted by the malware on your system.

Malware Recovery Tips

When the inevitable happens and either your computer or one of your user's computers gets infected by malware such as a computer virus, you need to follow certain steps to stop the problem from spreading and get the computer back up safely into service. Try this five-step process.

1. Recognize
2. Quarantine
3. Search and destroy
4. Remediate
5. Educate

Recognize and Quarantine The first step is to identify and recognize that a potential malware outbreak has occurred. If you're monitoring network traffic and one computer starts spewing e-mail, that's a good sign. Or users might complain that a computer that was running snappily the day before seems very sluggish.

Many networks employ software such as the open source PacketFence that automatically monitors network traffic and can cut a machine off the network if that machine starts sending suspicious packets. You can also quarantine a computer manually, by disconnecting the network cable. Once you're sure the machine isn't capable of infecting others, you're ready to find the virus or other malware and get rid of it.

At this point, you should disable System Restore. If you make any changes going forward, you don't want the virus to be included in any saved restore points. To turn off System Restore in Windows XP, open the Start menu, right-click on My Computer, and select Properties. Switch to the System Restore tab and select Turn off System Restore. On the dialog box that pops up, confirm your selection by clicking Yes. To turn off System Restore in Windows Vista/7, open the Start menu, right-click on Computer, and select Properties. Click on the *System protection* link. In the Protection Settings section, select a drive and click on Configure. In the System Protection dialog box that opens, select *Turn off system protection*. Repeat the procedure for each hard drive on your Windows Vista/7 system.

Search and Destroy Once you've isolated the infected computer (or computers), you need to get to a safe boot environment and run anti-malware software. You can try Windows Safe Mode first, because it doesn't require anything but a reboot. If that doesn't work, or you suspect a boot sector virus, you need to turn to an external bootable source, such as a bootable CD or flash memory drive.

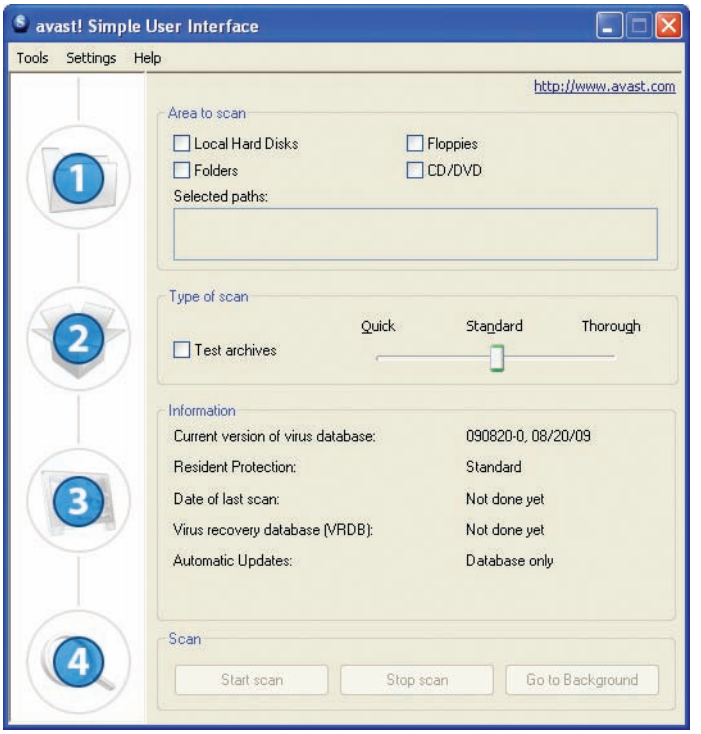
Get into the habit of keeping around a bootable anti-malware flash drive or optical media. If you suspect a virus or other malware, use the disc, even if your anti-malware program claims to have eliminated the problem. Turn off the PC and reboot it from the anti-malware disc. (You might have to change CMOS settings to boot to optical media.) This will put you in a clean boot environment that you know is free from any boot sector viruses. If you only support fairly recent computers, most have an option to boot to a USB flash drive, so you can put a boot environment on a thumb drive for even faster start-up speeds.

You have several options for creating the bootable optical disc or flash drive. First, some antivirus software comes in a bootable version, such as the avast! Virus Cleaner Tool (see Figure 29.25).

Second, you can download a copy of Linux that offers a live CD option such as Ubuntu. With a live CD, you boot to the CD and install a complete working copy of the operating system into RAM, never touching or accessing the hard drive, to give you full Internet-ready access to many online anti-malware sites. (You'll obviously need Internet access for those tools.) Kaspersky Labs provides a nice option at www.kaspersky.com.

Finally, you can download and burn a copy of the Ultimate Boot CD. It comes stocked with several antivirus and anti-malware programs, so you wouldn't need any other tool. Find it at www.ultimatebootcd.com. The only downside is that the anti-malware engines will quickly be out of date, as will their malware libraries.

Once you get to a boot environment, run your anti-malware program's most comprehensive scan. (Make sure you have all the latest updates for the software.) Then check all removable media that were exposed to the system, and any other machine that might have received data from the



• **Figure 29.25** avast! Virus Cleaner Tool

system or that is networked to the cleaned machine. A virus or other malicious program can often lie dormant for months before anyone knows of its presence.

E-mail is still a common source of viruses, and opening infected e-mails is a common way to get infected. Viewing an e-mail in a preview window opens the e-mail message and exposes your computer to some viruses. Download files only from sites you know to be safe and avoid the less reputable corners of the Internet, the most likely places to pick up computer infections.

CompTIA considers the process of removing a virus part of the remediation step. Since you can't remediate a PC until after a virus is gone, I've laid out the steps as you see here.

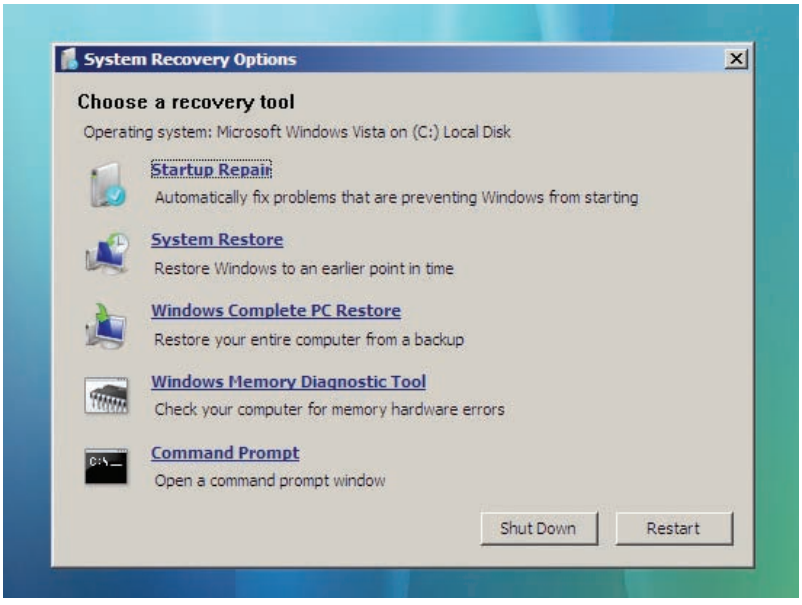
Remediate Malware infections can do a lot of damage to a system, especially to sensitive files needed to load Windows, so you might need to remediate formerly infected systems after cleaning off the drive or drives. **Remediation** simply means that you fix things the virus or other malware harmed. This can mean replacing corrupted Windows Registry files or even startup files.

If you can't start Windows after the malware scan is finished, you need to follow the steps outlined in Chapter 19 to boot to the Recovery Console in Windows XP, or boot from the Windows Preinstallation Environment into the Windows Recovery Environment in Windows Vista or Windows 7.

In the Windows XP Recovery Console, you'll have access to tools to repair the boot sector (or *boot blocks*, as CompTIA calls them) through the fixmbr and fixboot commands. You can run bootcfg to rebuild a corrupted boot.ini file.

Remember to re-enable System Restore and create a new restore point once the system has been repaired.

With the Windows Vista/7 Recovery Environment, you have access to more repair tools, such as Startup Repair, System Restore, Windows Complete PC Restore (System Image Recovery in Windows 7), and the command prompt (see Figure 29.26). Run the appropriate option for the situation and you should have the machine properly remediated in a jiffy.



• **Figure 29.26** System Recovery options in Windows Vista

Educate The best way to keep from having to deal with malware and grayware is education. It's your job as the IT person to talk to users, especially the ones whose systems you've just spent the last hour cleaning of nasties, about how to avoid these programs. Show them samples of dangerous e-mails they should not open, Web sites to avoid, and the types of programs they should not install and use on the network. Any user who understands the risks of questionable actions on their computers will usually do the right thing and stay away from malware.

Finally, have your users run antivirus and antispyware programs regularly. Schedule them while interfacing with the user so you know it will happen.

Cross Check

Recovery Environment

You saw the Windows Vista and Windows 7 Recovery Environments (also known as the System Recovery Options menu) back in Chapter 19, so check your memory now. What's the major difference between System Restore and Windows Complete PC Restore (System Image Recovery in Windows 7)? In what circumstances would you choose one tool over the other? What are the dangers, if any, in either tool?

Firewalls

Firewalls are an essential tool in the fight against malicious programs on the Internet. **Firewalls** are devices or software that protect an internal network from unauthorized access to and from the Internet at large. Firewalls use a number of methods to protect networks, such as hiding IP addresses and blocking TCP/IP ports.

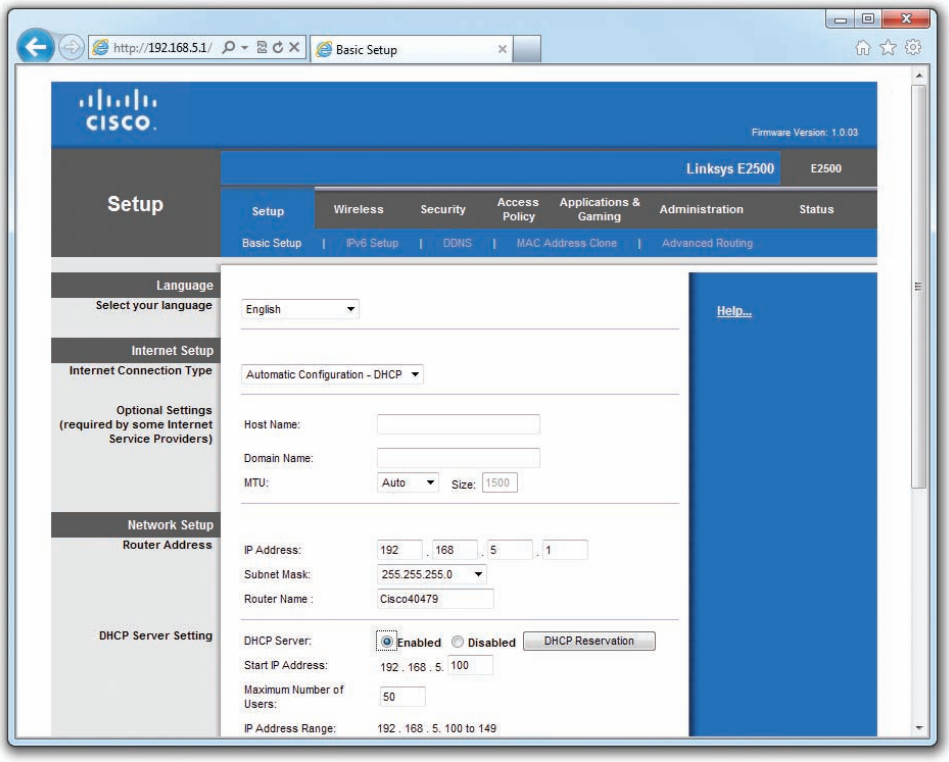
A typical network uses one of two types of firewalls: *hardware firewalls*, often built into routers, and *software firewalls* that run on your computers. Both types of firewall protect your computer and your network. You also run them at the same time. Let's look at both a typical SOHO router's firewall features and your computer's software firewall to see how they protect your network and your computers.

Hardware Firewall Settings

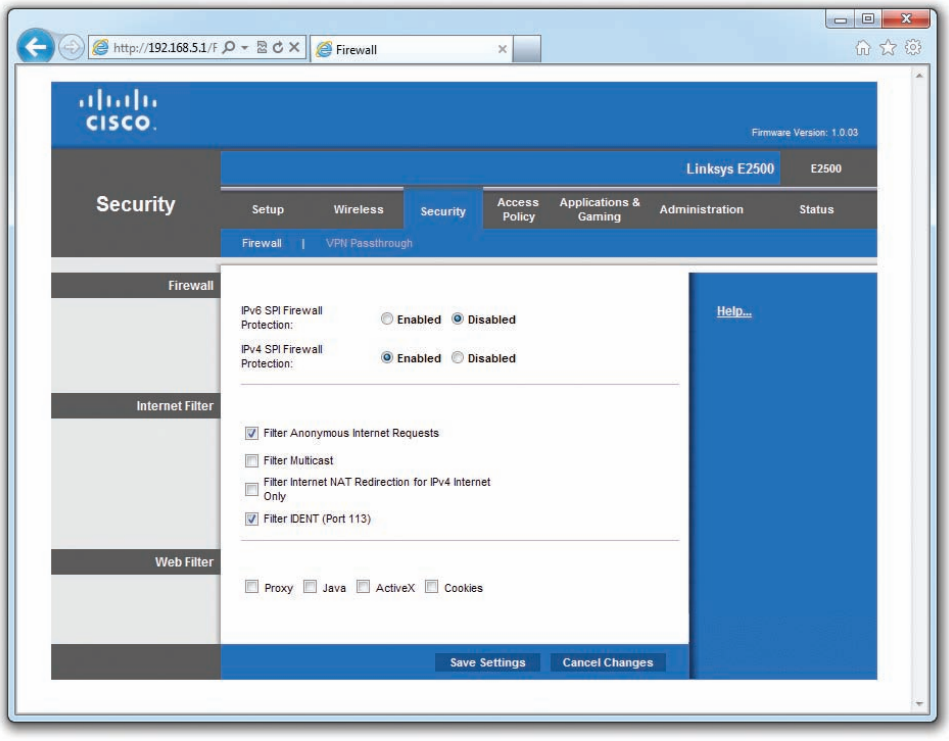
Most SOHO networks use a hardware firewall, often as a feature built into a router like the Linksys model you saw back in Chapter 24, shown in Figure 29.27. A hardware firewall hides and separates your internal LAN from outside connections like the Internet by using Network Address Translation (NAT), which you learned about back in Chapter 24. Routers, however, have a few other tricks up their sleeves. From the router's browser-based settings screen, you can configure a hardware firewall (see Figure 29.28). Let's walk through a few of the available settings.

A hardware firewall watches for and stops many common threats—all you have to do is turn it on (see Figure 29.29). Hardware firewalls use *Stateful Packet Inspection* (*SPI*) to inspect each incoming packet individually. SPI also blocks any incoming traffic that isn't in response to your outgoing traffic. You can even disable ports entirely, blocking all traffic in or out. But what if you want to allow outside users access to a Web server on the LAN? Because NAT hides the true IP address of that system, you'll need a way to allow incoming traffic past the router/firewall and a way to redirect that traffic to the right PC.

• **Figure 29.27** Linksys router as a firewall



• **Figure 29.28** Default Web interface

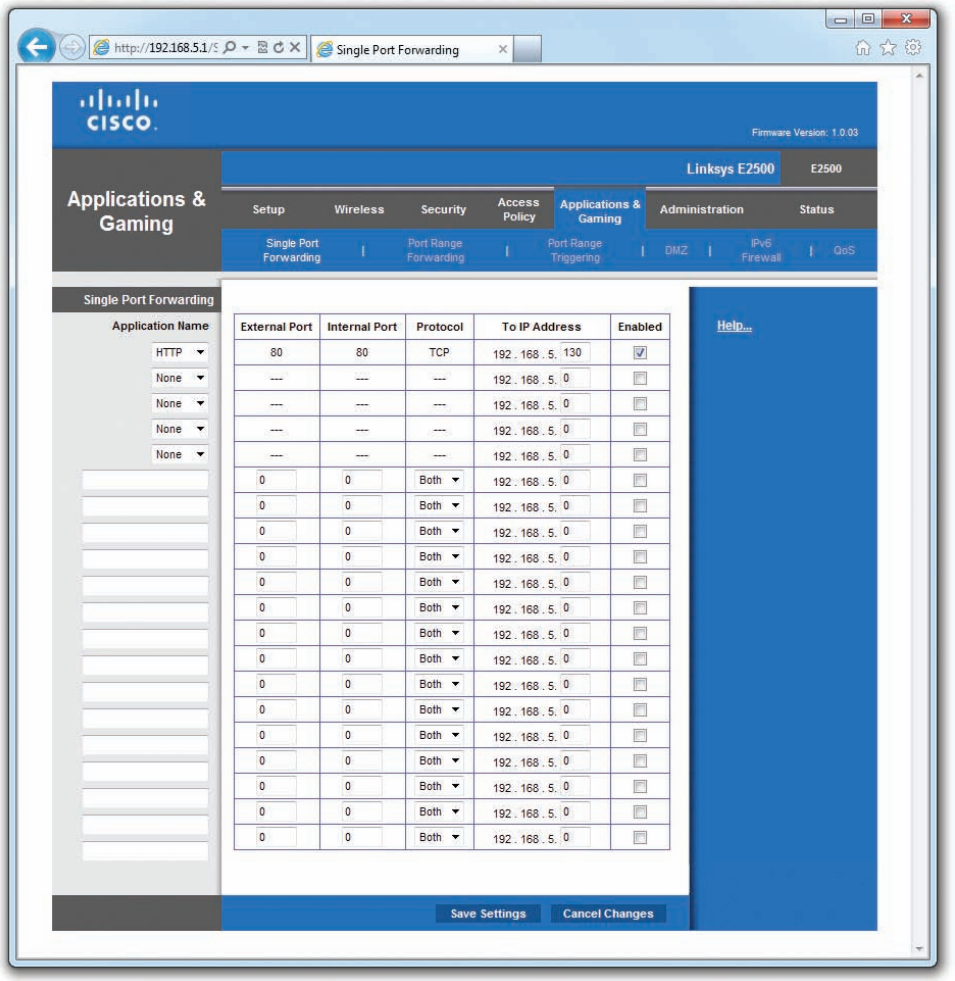


• **Figure 29.29** SPI firewall settings

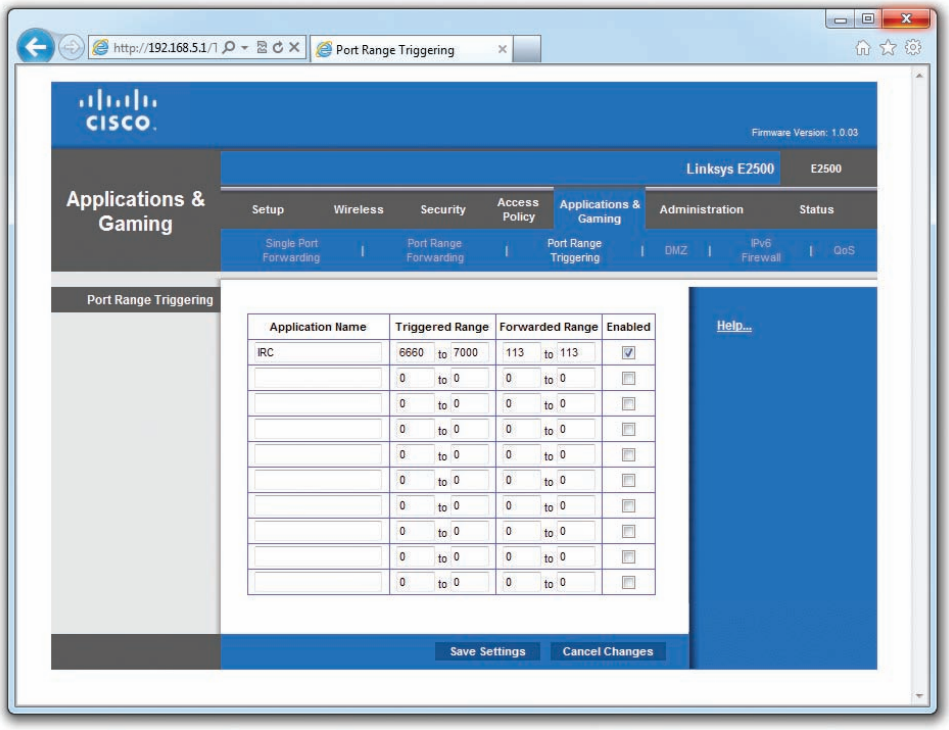
Port forwarding enables you to open a port in the firewall and direct incoming traffic on that port to a specific IP address on your LAN. In the case of the Web server referenced in the previous paragraph, you would open port 80 (for HTTP packets) and instruct the router to send all incoming traffic to the server machine. Figure 29.30 shows port forwarding configured to send all HTTP packets to an internal Web server.

Port forwarding isn't the only way to open ports on a firewall. **Port triggering** enables you to open an incoming connection to one computer automatically based on a specific outgoing connection. The *trigger port* defines the outgoing connection, and the *destination port* defines the incoming connection. If you set the trigger port to 3434 and the destination port to 1234, for example, any outgoing traffic on port 3434 will trigger the router to open port 1234 and send any received data back to the PC with the original outgoing traffic. Figure 29.31 shows a router set up for port triggering of an Internet Relay Chat (IRC) server.

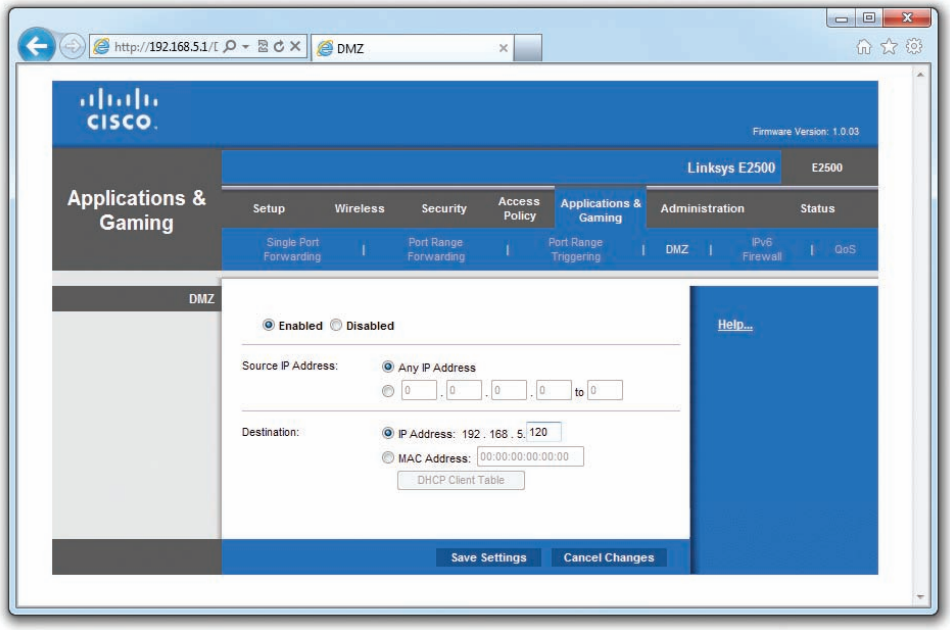
If you want to go beyond port forwarding and port triggering and open every port on a machine, you need a demilitarized zone (DMZ). A DMZ puts systems with the specified IP addresses outside the protection of the



• **Figure 29.30** Port forwarding



• **Figure 29.31** Port triggering



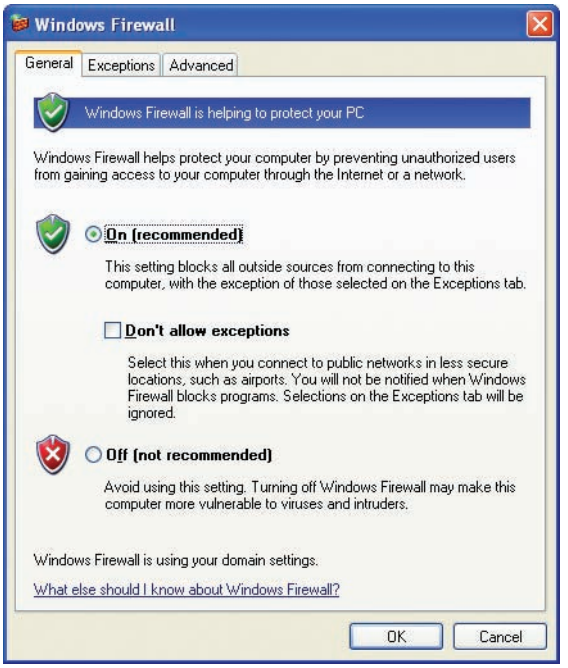
• **Figure 29.32** DMZ set up on a SOHO router

firewall, opening all ports and enabling all incoming traffic (see Figure 29.32). If you think this sounds incredibly dangerous, you are right! Any PC inside the DMZ will be completely exposed to outside attacks. Don't use it!

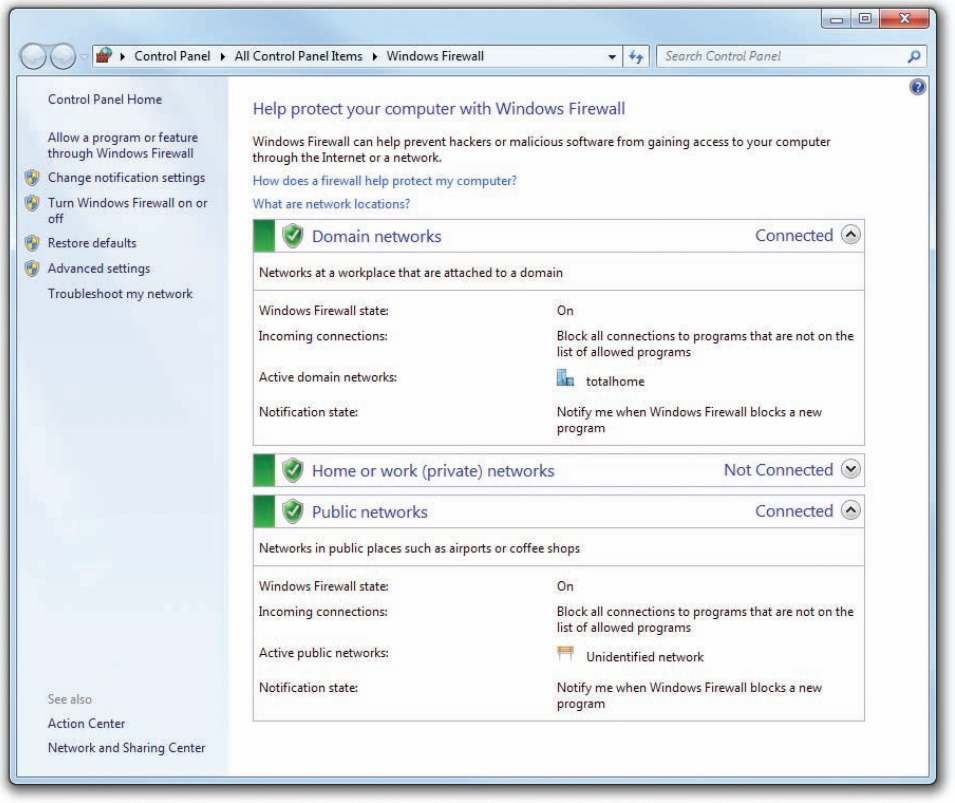
Software Firewalls

While a hardware firewall does a lot to protect you from outside intruders, you should also use a software firewall, such as the firewalls built into each version of Windows, called (appropriately) Windows Firewall. Windows Firewall handles the heavy lifting of port blocking, security logging, and more.

You can access Windows Firewall in Windows XP by opening the Windows Firewall applet in the Control Panel. The Windows XP's Windows Firewall applet (see Figure 29.33) looks a lot different from the one available in Windows 7 (see Figure 29.34), though their primary function remains



• **Figure 29.33** Windows XP's Firewall applet



• **Figure 29.34** Windows 7 Firewall applet

To turn Windows Firewall off (which I don't recommend doing), open the Windows Firewall applet. In Windows XP, click on the *Off (not recommended)* radio button. In Windows Vista, click on *Turn Windows Firewall on or off*, then select *Off (not recommended)*. In Windows 7, select *Turn Windows Firewall on or off*, then select *Turn off Windows Firewall (not recommended)* for each network type you use.

the same. Configuring Windows Firewall involves turning it on or off, and choosing which programs and services can pass through the firewall, known as *exceptions*. If you wanted to play *Starcraft 2* (a PC game that requires an Internet connection), for example, it would need to be on the list of exceptions for your firewall—most programs you install add themselves to this list automatically, otherwise Windows Firewall prompts you the first time you run it and asks if you want to add the program as an exception.

The Windows XP firewall's biggest shortcoming is that it fails to consider that a single PC, especially a portable, might connect to multiple networks. You don't necessarily want the same firewall settings used for both public and private networks. Microsoft needed to develop a way for you to separate trustworthy networks (like the one in your house or at the office) from non-trustworthy networks (like a public Wi-Fi Internet connection at the airport). To accomplish this, Microsoft included three network types in Windows Vista/7: Domain, Private, and Public.

- A *Domain* network is a Windows network controlled by a Windows domain controller. In this case, the domain controller itself tells your machine what it can and cannot share. You don't need to do anything when your computer joins a domain.
- A *Private* network enables you to share resources, discover other devices, and allow other devices to discover your computer safely.
- A *Public* network prevents your computer from sharing and disables all discovery protocols.

When your computer connects to a network for the first time, Windows Vista and 7 will prompt you to choose the network type: Home, Work, or Public location (see Figure 29.35).

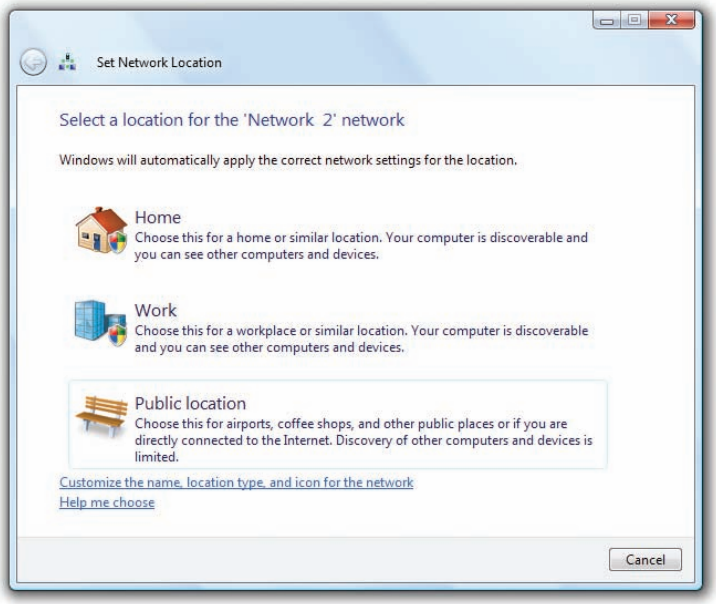


Figure 29.35 Set Network Location in Vista

First, notice that Domain is not an option. There's a good reason for this: If your computer is on a domain, you won't see the dialog box in Figure 29.35. When your computer joins a domain, Windows automatically sets your network location to Domain (unless your domain controller chooses something different, which is unlikely).

So what exactly does Windows do when you select Home, Work, or Public location? Windows configures Windows Firewall to block or unblock discovery and sharing services. When running on a Private (Home or Work) network, Windows enables Network Discovery and File and Printer Sharing as exceptions. When running on a Public network, Windows disables these exceptions.

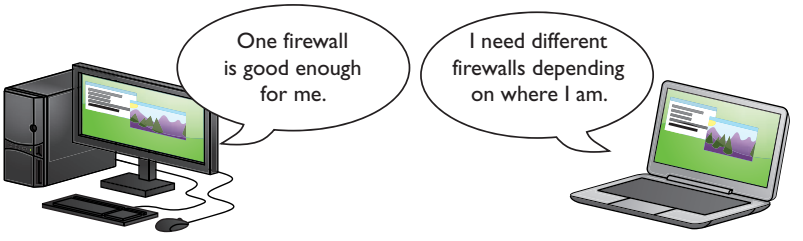
The Network Discovery setting dictates whether a computer can find other computers or devices on a network and vice versa. Even with Network Discovery activated, several firewall settings can overrule certain connections.

In Windows Vista, Microsoft cleverly used Windows Firewall and the network type to turn services on and off, but Microsoft made one mistake: the firewall configuration and network type remain the same for every connection. If your Windows machine never changes networks, you won't have a problem. But what about machines (mainly laptops) that hop from one network to another (see Figure 29.36)? In that case, you need different firewall settings for each network the system might encounter.

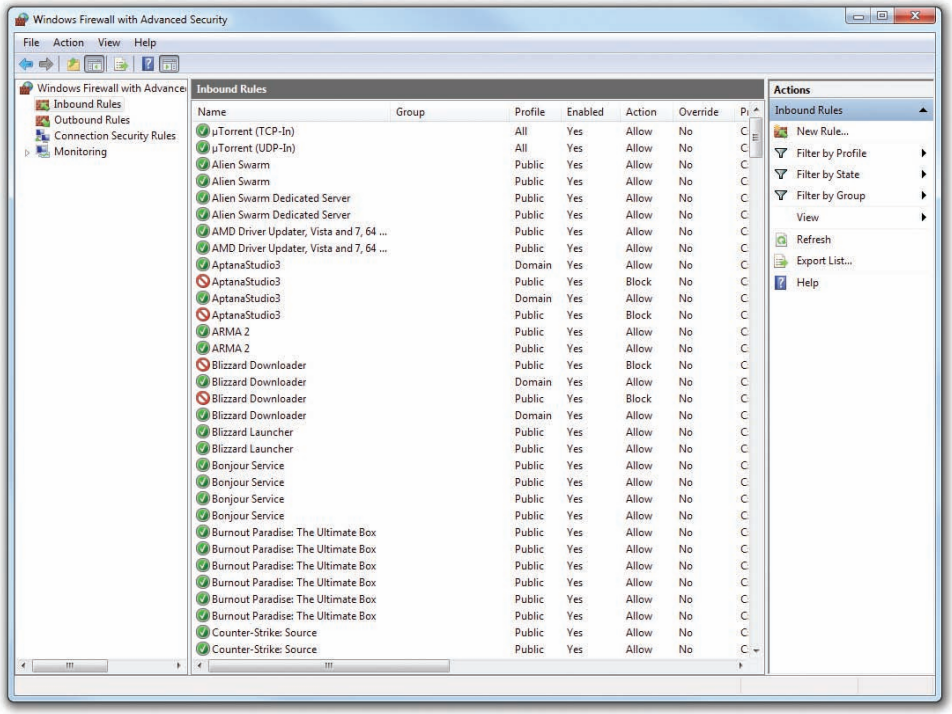
In this regard, Windows 7 makes a big departure from Windows Vista. In Windows 7, the Set Network Location dialog box appears every time you connect to a new network. Windows 7 even includes three different firewall settings: one for Domains, one for Private networks (Home or Work), and one for Public networks.

Once you've picked a network type, you might want to customize the firewall settings further. If you click the Advanced Settings option in Windows Vista/7's Firewall applet, you'll discover a much deeper level of firewall configuration, one very different from the settings found in Windows XP (see Figure 29.37). In fact, it's an entirely different tool called Windows Firewall with Advanced Security.

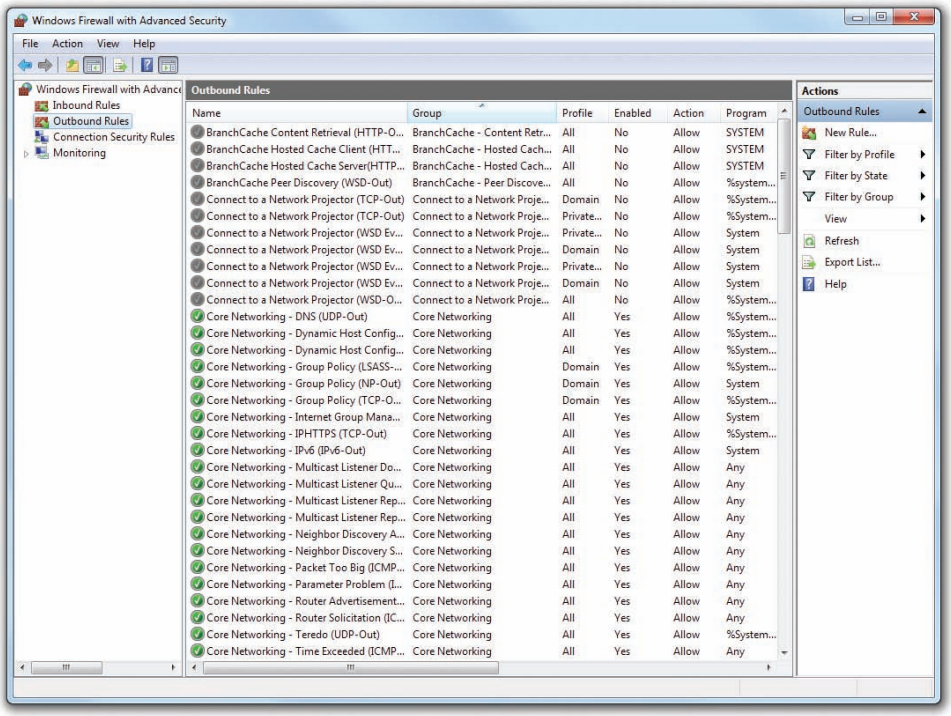
Microsoft enhanced how Windows Vista/7 treat exceptions. In Windows XP, you can only choose a program and make it an exception, giving it permission to pass through the firewall. But programs both send and receive network data; Windows XP ignores the "inbound" and "outbound" aspect of firewalls. Windows Vista/7 takes the exceptions concept and expands it to include custom rules for both inbound and outbound data. Figure 29.38 shows the outbound rules for a typical Windows Vista/7 system.



• **Figure 29.36** Many machines need more than one network setting.



• **Figure 29.37** Windows Firewall with Advanced Security



• **Figure 29.38** Outbound Rules list

A rule always includes at least the following:

- The name of the program
- Group: an organizational group that helps sort all the rules
- The associated profile (All, Domain, Public, Private)
- Enabled/disabled status
- Remote and local address
- Remote and local port number

You can add, remove, and customize any rule to your liking. It quickly gets complicated, so unless you need to set a lot of custom rules, stick to the standard Windows Firewall applet.

Authentication and Encryption

You know from previous chapters that the first step in securing data is authentication, through a user name and password. But when you throw in networking, you're suddenly not just a single user sitting in front of a computer and typing. You're accessing a remote resource and sending login information over the Internet. What's to stop someone from intercepting your user name and password?

Firewalls do a great job of controlling traffic coming into a network from the Internet and going out of a network to the Internet, but they do nothing to stop interceptor hackers who monitor traffic on the public Internet looking for vulnerabilities. Worse, once a packet is on the Internet itself, anyone with the right equipment can intercept and inspect it. Inspected packets are a cornucopia of passwords, account names, and other tidbits that hackers can use to intrude into your network. Because we can't stop hackers from inspecting these packets, we must turn to **encryption** to make them unreadable.

Network encryption occurs at many levels and is in no way limited to Internet-based activities. Not only are there many levels of network encryption, but each encryption level also provides multiple standards and options, making encryption one of the most complicated of all networking issues. You need to understand where encryption comes into play, what options are available, and what you can use to protect your network.

Network Authentication

Have you ever considered the process that takes place each time a person types in a user name and password to access a network, rather than just a local machine? What happens when this *network* authentication is requested? If you're thinking that when a user types in a user name and password, that information is sent to a server of some sort to be authenticated, you're right—but do you know how the user name and password get to the serving system? That's where encryption becomes important in authentication.

In a local network, authentication and encryption are usually handled by the OS. In today's increasingly interconnected and diverse networking environment, there is a motivation to enable different operating systems

to authenticate any client system from any other OS. Modern operating systems such as Windows and Mac OS X use standard authentication encryptions such as MIT's **Kerberos**, enabling multiple brands of servers to authenticate multiple brands of clients. These LAN authentication methods are usually transparent and work quite nicely, even in mixed networks.

Data Encryption

Encryption methods don't stop at the authentication level. There are a number of ways to encrypt network *data* as well. The choice of encryption method is dictated to a large degree by the method used by the communicating systems to connect. Many networks consist of multiple networks linked together by some sort of private connection, usually some kind of WAN connection such as DSL or T1. Microsoft's encryption method of choice for this type of network is called **IPSec** (derived from *IP security*). IPSec provides transparent encryption between the server and the client. IPSec also works in VPNs, but other encryption methods are more commonly used in those situations.

Application Encryption

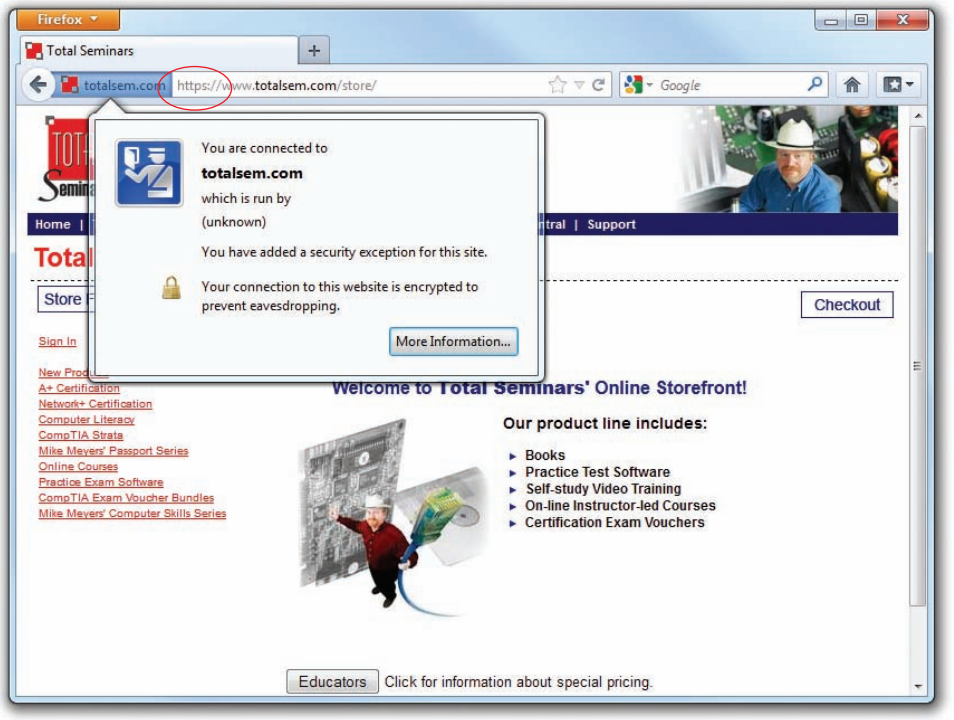
When it comes to encryption, even TCP/IP applications can get into the swing of things. The most famous of all application encryptions is Netscape's **Secure Sockets Layer (SSL)** security protocol, which is used to create secure Web sites. Microsoft incorporates SSL into its more far-reaching **HTTPS** (HTTP over SSL) protocol. These protocols make it possible to create the secure Web sites people use to make purchases over the Internet. You can identify HTTPS Web sites by the *https://* (rather than http://) included in the URL (see Figure 29.39).

To make a secure connection, your Web browser and the Web server must encrypt their data. That means there must be a way for both the Web server and your browser to encrypt and decrypt each other's data. To do this, the server sends a public key to your Web browser so the browser knows how to decrypt the incoming data. These public keys are sent in the form of a **digital certificate**. This certificate is signed by a trusted authority that guarantees that the public key you are about to get is actually from the Web server and not from some evil person trying to pretend to be the Web server. A number of companies issue digital certificates to Web sites, probably the most famous being VeriSign, Inc.

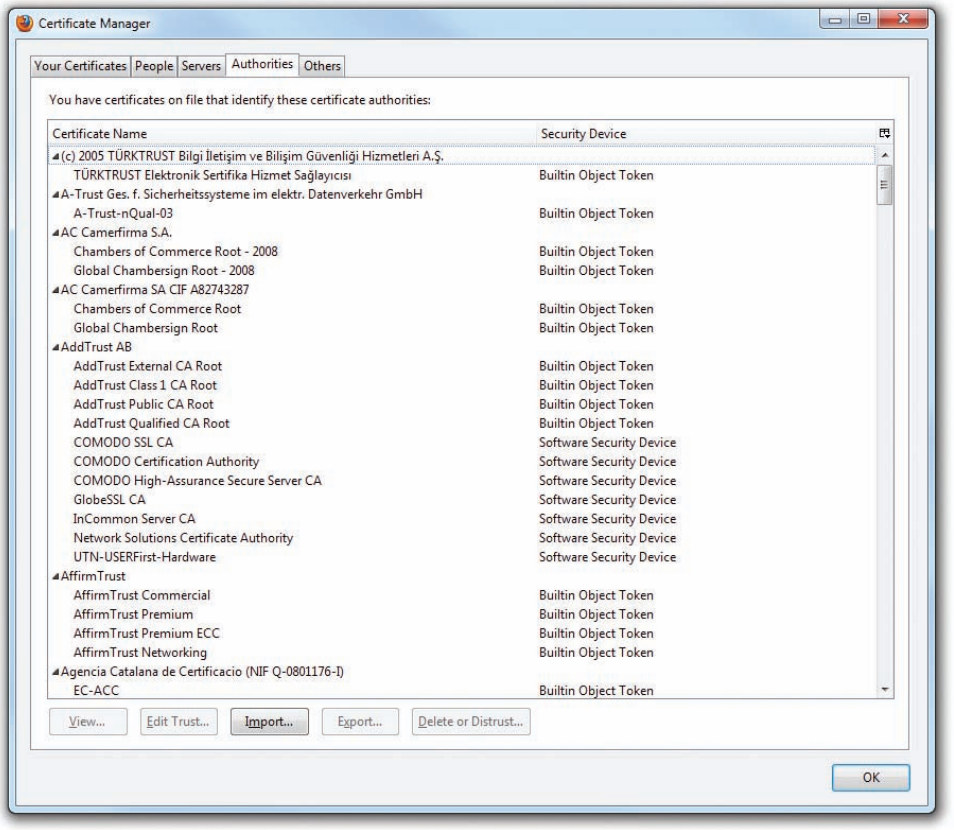
Your Web browser has a built-in list of trusted authorities. If a certificate comes in from a Web site that uses one of these highly respected companies, you won't see anything happen in your browser; you'll just go to the secure Web page, where a small lock will appear in the corner of your browser. Figure 29.40 shows the list of trusted authorities built into the Firefox Web browser.

If you receive a certificate from someone *not* listed in your browser, however, the browser will warn you and ask you if you wish to accept the certificate, as shown in Figure 29.41.

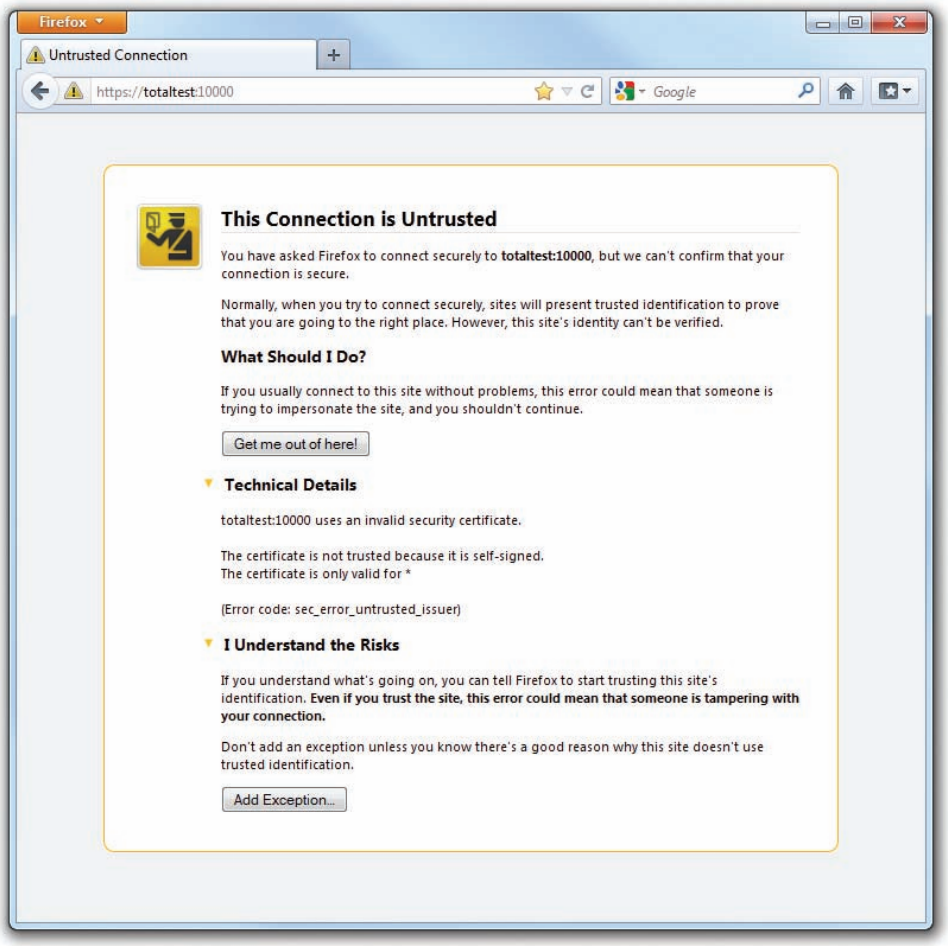
What you do here is up to you. Do you wish to trust this certificate? In most cases, you simply say yes, and this certificate is added to your SSL cache of certificates. An accepted certificate may become invalid, however, usually because of something boring; for instance, it may go out of date or



• **Figure 29.39** A secure Web site



• **Figure 29.40** Trusted authorities



• **Figure 29.41** Incoming certificate

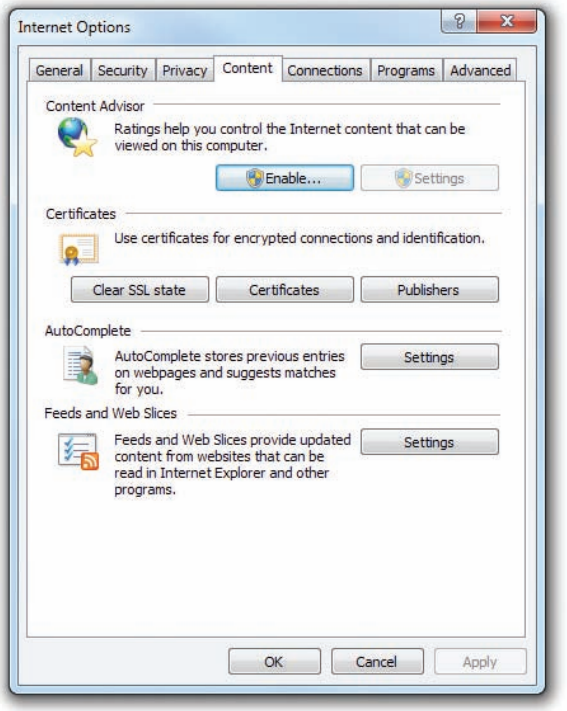
the public key may change. This never happens with the "big name" certificates built into your browser—you'll see this more often when a certificate is used, for example, in-house on a company intranet and the administrator forgets to update the certificates. If a certificate goes bad, your browser issues a warning the next time you visit that site. To clear invalid certificates, you need to clear the SSL cache. The process varies in every browser, but in Internet Explorer, go to the Content tab under Internet Options and click the *Clear SSL state* button (see Figure 29.42).

Wireless Issues

Wireless networks add a whole level of additional security headaches for techs to face, as you know from Chapter 23. Some of the points to remember or to go back and look up are as follows:

- Set up wireless encryption, at least WEP but preferably WPA or the more secure WPA2, and configure clients to use it.
- Disable DHCP and require your wireless clients to use a static IP address.

- If you need to use DHCP, only allot enough DHCP addresses to meet the needs of your network, to avoid unused wireless connections.
- Change the WAP's SSID from default.
- Filter by MAC address to allow only known clients on the network.
- Change the default user name and password. Every hacker has memorized the default user names and passwords.
- Update the firmware as needed.
- If available, make sure the WAP's firewall settings are turned on.



• **Figure 29.42** Internet Options Content tab in Internet Explorer

Cross Check

Securing Wireless Networks

Wireless networks are all the rage right now, from your local Starbucks to the neighbors around you. Securing wireless networks has, therefore, become an area that CompTIA A+ certified technicians must master. You read a lot about wireless networks in Chapter 23, so turn there now and see if you can answer these questions.

What is the minimum level of encryption to secure a wireless network? What types of wireless will you find for connecting at your local coffee shop?

Chapter Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about computer security.

Explain the threats to your computers and data

- Threats to your data come from two sources: accidents and malicious people.
- Unauthorized access occurs when a user accesses resources in an unauthorized way. Not all unauthorized access is malicious and some is even accidental. Authorized access can lead to data destruction by users who do not intend to be malicious. When users have access to a file or database, they typically believe the system won't let them make any changes they are not authorized to make.
- Most computer attacks are accomplished through social engineering rather than hacking. Telephone scams are one of the most common social engineering tactics. Dumpster diving involves physically going through an organization's trash looking for documents that might reveal user names, passwords, or other sensitive information. Be sure to secure your computer equipment in a locked room to prevent physical theft.
- Computers, hard drives, and power all fail. As a tech, you need to plan for redundancy in these areas. You also need to protect your computers against viruses distributed through the network and removable media. You should implement good access policies and implement methods for tracking computer usage.
- Protect your PC from environmental dangers such as power surges, dirty or humid air, heat, or toxic hazards.

Describe key security concepts and technologies

- Controlling access to programs, data, and other computing resources is the key to securing your system. Access control includes four interlinked areas requiring your attention: physical security, authentication, users and groups, and security policies.
- Store computers with sensitive data in a locked room and never walk away from your computer while logged on. Log out or lock the computer by pressing WINDOWS LOGO KEY-L. Some companies lock down computer rooms with ID badges that act as key cards, using RFID or smart cards for authentication. Be aware of those around you in the space, and watch out for shoulder surfers looking at your monitor while you work.
- The three forms of authentication include knowledge factors (something the user knows, like a password or PIN), ownership factors (something the user has, like a key or card), and inherent factors (something about the user, such as a fingerprint).
- Accounts should be given permissions to access only what they need and no more. Unused accounts should be disabled.
- When a user account is a member of several groups, and permissions have been granted to groups, the user account will have a set of combined permissions that may conflict. The resulting permissions that ultimately control access are referred to as the effective permissions.
- Make sure to lock down the default Everyone group of which all users are automatically members. Never use the default Everyone or Users groups or the default Guest account unless you intend to permit all those accounts access to resources.
- Policies control permissions for activities, such as installing software, accessing a command prompt, or logging on at a particular time of day. A policy is usually applied to a user account, computer account, or a group. Use the Local Security Policy tool to manage policies for an individual computer.
- Group Policy enables you to control such things as deploying software or setting each computer in a domain to use the same wallpaper. Commonly used policies include Prevent Registry Edits, Prevent Access to the Command Prompt, Log On Locally, and Minimum Password Length.
- Data classification systems vary by the organization, but a common scheme classifies

documents as public, internal use only, highly confidential, top secret, and so on. Using a classification scheme enables employees such as techs to know very quickly what to do with documents, drives containing documents, and more.

- Compliance means that members of an organization or company must abide by or comply with all of the rules that apply to the organization or company. From a technician's point of view, the most common compliance issue revolves around software, such as what sort of software users can be allowed to install on their computers. Compliance keeps technical support calls down and enables techs to focus on more serious problems.
- Use Event Viewer to track activity on your system. By default, the Security section doesn't show you everything, so it is good practice to enable event auditing and object access auditing. Event auditing creates an entry in the Security Log when certain events happen, such as a user logging on, while object access auditing creates entries in response to object access, such as someone trying to access a certain file or folder.
- Incidence reporting means telling your supervisor about the data you've gathered regarding a computer or network problem. This provides a record of what you've done and accomplished. It also provides information that, when combined with other information you may or may not know, may reveal a pattern or bigger problem to someone higher up the chain.
- Try to avoid any personal information on a PC. If you find something private (that isn't illegal), ignore it and forget about it. If you find something illegal, you must follow the proper procedures. If a device you work on becomes evidence in legal proceedings, isolate the system and document everything that happens going forward. Pay special attention to the chain of custody, or whoever is currently in control of the machine.

Explain how to protect computers from network threats

- Malware includes grayware, spam, viruses, worms, macros, Trojan horses, and rootkits, all of which can wreak havoc on your system.
- Irritating Web browser problems include pop-ups and spyware. Many pop-ups remove the navigation aids from the browser window or mimic Windows dialog boxes. To safely close a pop-up, right-click the pop-up's taskbar icon and choose Close, or press ALT-TAB until the pop-up window is active and then press ALT-F4 to close it.
- Spyware can use your computer's resources to run distributed computing applications, capture keystrokes to steal passwords, or worse. Spyware typically disguises itself as useful utilities, so be vigilant about what you install. Some spyware can be removed via Add Remove Programs, but for stubborn spyware, use a third-party tool such as Lavasoft's Ad-Aware or Safer Networking's Spybot Search & Destroy.
- Unsolicited e-mail is called spam. Never post your e-mail address on the Internet; over 97 percent of spam goes to e-mail addresses posted online. Spam filters can block spam at the mail server or at your computer. You can set most e-mail programs to block e-mail sent from specific people or to a specific person.
- A virus is a piece of malicious software that is passed from computer to computer and is designed to attach itself to another program on your computer. A worm is a freestanding program that takes advantage of security flaws and copies itself over and over again, thereby bogging down a network.
- A macro is any type of virus that exploits application macros to replicate and activate. Trojan horses are freestanding programs that do something other than the user expects it to do when run, such as expecting a game to run but erasing CMOS settings instead.
- A rootkit is a Trojan horse that takes advantage of very low-level operating system functions to hide itself from all but the most aggressive of anti-malware tools. Rootkits can strike operating systems, hypervisors, and even firmware.
- To help protect a computer from malware, make sure to run up-to-date antivirus software, use a firewall, and apply all security patches for your software and operating system. Run Windows Update automatically, or at least weekly if you choose to configure it for manual updates.
- Antivirus software works in active mode to scan your file system for viruses and in passive mode by monitoring your computer's activity and checking for viruses in response to an action, such as running a program or downloading a file. The

software detects boot sector viruses by comparing the drive's boot sector to a standard boot sector. To detect executable viruses, a library of virus signatures is used.

- Polymorph viruses attempt to change their signature to prevent detection by antivirus software. Fortunately, the scrambled code itself can be used as a signature. A checksum, based on file contents, can be created for every file on the drive. If the checksum changes, it is a sign of a virus infection. Most stealth viruses are boot sector viruses that hide from antivirus software.
- The best way to prevent damage from a virus is to keep from getting a virus in the first place. Use your passive antivirus shield, scan the PC daily, know where software has come from before you load it, and keep your antivirus definitions updated. Don't view e-mail messages in a preview window, and only download files from sites you know to be safe.
- Some of the common symptoms of a malware infection include: browser redirections, crashes, unresponsiveness, changed file permissions, hidden files, missing system files, and so on.
- When the inevitable happens and either your computer or one of your user's computers is infected by a computer virus or other malware, you need to follow a process to stop the problem from spreading and get the computer back up safely into service. First, recognize the symptoms of a computer malware attack, such as a suddenly very sluggish computer. Follow up by quarantining the infected computer to make certain the virus or other malware doesn't spread. Third, boot the computer in Safe Mode or an alternative safe boot environment and run anti-malware software. To finish up, remediate the formerly infected machine by fixing boot sector problems and so on, and educate your users so infection doesn't happen again.
- Hardware firewalls protect networks by hiding IP addresses and blocking TCP/IP ports. Port forwarding and port triggering enable traffic to pass through the firewall on specific ports to specific machines.
- Windows XP and later come with a built-in software firewall that is accessible from the Windows Firewall Control Panel applet.
- Encryption makes network packets unreadable by hackers who intercept network traffic. You are especially vulnerable when using the Internet over a public network. Modern operating systems use Kerberos to encrypt authentication credentials over a local network.
- Network data can be encrypted similar to authentication credentials. Microsoft's encryption method of choice is called IPSec. Netscape's Secure Sockets Layer (SSL) creates secure Web sites. Microsoft's HTTPS protocol incorporates SSL into HTTP. Web sites whose URL begins with https:// (rather than http://) are used to encrypt credit card purchases.
- To secure a wireless network, use wireless encryption and disable DHCP. Require wireless clients to use a static IP address, or allot only enough DHCP addresses to meet the needs of your network. Definitely change the default administrator user name and password on the WAP!

Key Terms

access control *(1107)*
anti-malware program *(1127)*
antivirus program *(1127)*
authentication *(1109)*
biometric device *(1112)*
chain of custody *(1118)*
compliance *(1116)*
convert *(1112)*
data classification *(1116)*
definition files *(1129)*
digital certificate *(1142)*
dumpster diving *(1102)*
effective permissions *(1113)*
encryption *(1141)*
event auditing *(1116)*
Event Viewer *(1116)*
firewall *(1133)*
grayware *(1119)*
Group Policy *(1114)*
HTTPS *(1142)*

incidence reporting *(1117)*
IPSec *(1142)*
Kerberos *(1142)*
Local Security Policy *(1114)*
macro *(1124)*
malware *(1119)*
object access auditing *(1116)*
phishing *(1103)*
polymorph virus *(1127)*
pop-up *(1120)*
port forwarding *(1135)*
port triggering *(1135)*
remediation *(1132)*
rootkit *(1125)*
Secure Sockets Layer (SSL) *(1142)*
shoulder surfing *(1102)*
signature *(1127)*
smart card *(1110)*
social engineering *(1102)*
spam *(1123)*
spyware *(1120)*
stealth virus *(1127)*
tailgating *(1102)*
telephone scam *(1103)*
Trojan horse *(1124)*
unauthorized access *(1101)*
virus *(1124)*
virus shield *(1127)*
worm *(1124)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. Mary's company routinely labels data according to its sensitivity or potential danger to the company if someone outside accesses the data. This is an example of _____.
2. A(n) _____ masquerades as a legitimate program, yet does something different than what is expected when executed.
3. Antivirus software uses updatable _____ to identify a virus by its _____.
4. Enable _____ to create Event Viewer entries when a specific file is accessed.
5. Although not all _____ is malicious, it can lead to data destruction.
6. Most attacks on computer data are accomplished through _____.
7. A(n) _____ protects against unauthorized access from the Internet.
8. Many companies authenticate access to secure rooms using an ownership factor such as a(n) _____.
9. Before making a credit card purchase on the Internet, be sure the Web site uses the _____ security protocol, which you can verify by checking for the _____ protocol in the address bar.
10. A virus that changes its signature to prevent detection is called a(n)_____.

Multiple-Choice Quiz

1. What is the process of using or manipulating people to gain access to network resources?
   A. Cracking
   B. Hacking
   C. Network engineering
   D. Social engineering
2. Which of the following might offer good hardware authentication?
   A. Strong password
   B. Encrypted password
   C. NTFS
   D. Smart card

3. Which of the following tools would enable you to stop a user from logging on to a local machine but still enable him to log on to the domain?
   - **A.** AD Policy filter
   - **B.** Group Policy Auditing
   - **C.** Local Security Policy
   - **D.** User Settings
4. Which hardware firewall feature enables incoming traffic on a specific port to reach an IP address on the LAN?
   - **A.** Port forwarding
   - **B.** NAT
   - **C.** DMZ
   - **D.** Multifactor authentication
5. Zander downloaded a game off the Internet and installed it, but as soon as he started to play he got a Blue Screen of Death. Upon rebooting, he discovered that his My Documents folder had been erased. What happened?
   - **A.** He installed spyware.
   - **B.** He installed a Trojan horse.
   - **C.** He broke the Group Policy.
   - **D.** He broke the Local Security Policy.
6. Which of the following should Mary set up on her Wi-Fi router to make it the most secure?
   - **A.** NTFS
   - **B.** WEP
   - **C.** WPA
   - **D.** WPA2
7. A user account is a member of several groups, and the groups have conflicting rights and permissions to several network resources. The culminating permissions that ultimately affect the user's access are referred to as what?
   - **A.** Effective permissions
   - **B.** Culminating rights
   - **C.** Last rights
   - **D.** Persistent permissions
8. What is true about virus shields?
   - **A.** They automatically scan e-mails, downloads, and running programs.
   - **B.** They protect against spyware and adware.
   - **C.** They are effective in stopping pop-ups.
   - **D.** They can reduce the amount of spam by 97 percent.
9. What does Windows use to encrypt the user authentication process over a LAN?
   - **A.** PAP
   - **B.** TPM
   - **C.** HTTPS
   - **D.** Kerberos
10. Which threats are categorized as social engineering? (Select all that apply.)
    - **A.** Telephone scams
    - **B.** Dumpster diving
    - **C.** Trojan horses
    - **D.** Spyware
11. A user calls to complain that his computer seems awfully sluggish. All he's done so far is open his e-mail. What should the tech do first?
    - **A.** Educate the user about the dangers of opening e-mail.
    - **B.** Quarantine the computer so the suspected virus does not spread.
    - **C.** Run antivirus software on the computer.
    - **D.** Remediate the infected system.
12. Which of the following are good examples of remediation? (Select two.)
    - **A.** Boot to the Recovery Console in Windows XP and run fixmbr or fixboot to repair boot sector damage.
    - **B.** Boot to the Windows Recovery Environment in Windows Vista/7 and run System Restore.
    - **C.** Boot to a safe environment and run antivirus software.
    - **D.** Remove a computer suspected of having a virus from the network, effectively quarantining the computer.
13. Which of the following are examples of grayware? (Select two.)
    - **A.** Pop-up
    - **B.** Spyware
    - **C.** Trojan horse
    - **D.** Virus

14. A user calls and complains that the technician who fixed his computer removed some software he used to listen to music on the Internet. A check of approved software does not include the LimeWire application, so what should the supervisor do?
    - **A.** Applaud the technician for proper compliance.
    - **B.** Educate the user about the legal issues involved with music downloads.
    - **C.** Add the LimeWire application to the approved software list and make the technician apologize and reinstall the software.
    - **D.** Check with the user's supervisor about adding LimeWire to the approved software list.
15. Cindy wants to put a policy in place at her company with regard to virus prevention or at least limitation. What policies would offer the best solution?
    - **A.** Install antivirus software on every computer. Instruct users on how to run it.
    - **B.** Install antivirus software on every computer. Set the software up to scan regularly.
    - **C.** Install antivirus software on every computer. Set the software up to update the definitions and engine automatically. Set the software up to scan regularly.
    - **D.** Install antivirus software on every computer. Set the software up to update the definitions and engine automatically. Set the software up to scan regularly. Educate the users about what sites and downloads to avoid.

Essay Quiz

1. Your boss is considering getting an Internet connection for the office so employees have access to e-mail, but she is concerned about hackers getting into the company server. What can you tell your boss about safeguards you will implement to keep the server safe?
2. A coworker complains that he is receiving a high amount of spam on his home computer through his personal e-mail account. What advice can you give him to alleviate his junk mail?
3. An intern in your IT department has asked for your help in understanding the differences between a virus, a worm, and a Trojan horse. What advice can you offer?
4. The boss's assistant has been asked to purchase a new coffee machine for the break room but is nervous about shopping online with the company credit card. What can you tell her about secure online purchases?

Lab Projects

• Lab Project 29.1

You have learned a little bit about the Local Security Policy in Windows. Fire up your Web browser and do a search for Local Security Policy. Make a list of at least five changes you might consider making to your personal computer by using the Local Security Policy tool. Be sure to include what the policy is, what it does, and where in the tool it can be configured.

• Lab Project 29.2

You know you must run antivirus and antispyware software on any computer connected to the Internet, and many companies will sell you good, bad, and indifferent software. Using the Internet, find free antivirus and free antispyware programs and make sure these are legitimate and reputable programs and not spyware masquerading as legitimate programs! What free antivirus did you find? What free antispyware did you find? How do you know these are reputable? Would you install these on your own personal computer? Why or why not?

chapter 30

Virtualization

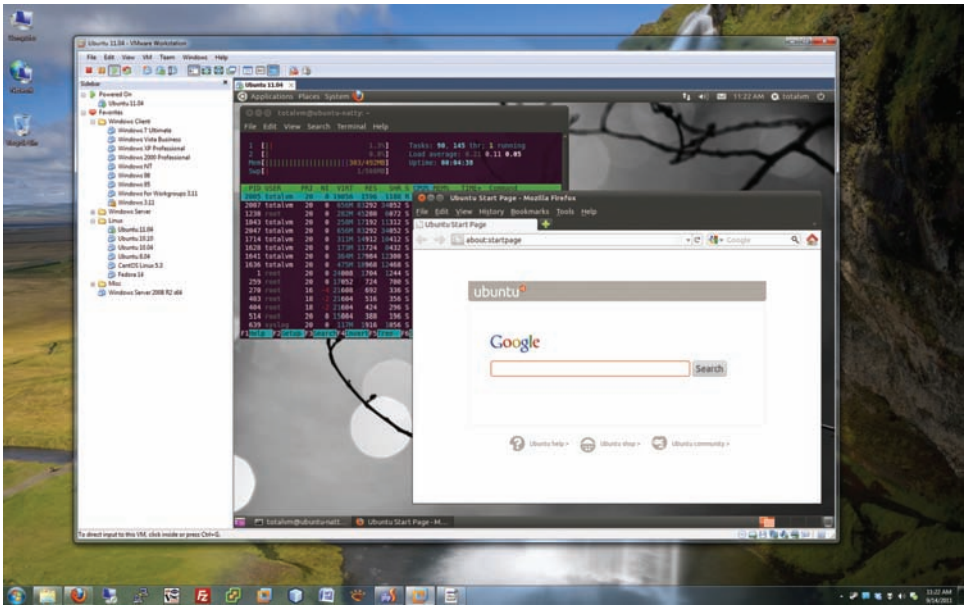
On virtualization: "Once the world figures this stuff out, this is going to be a huge change to the corporate landscape."

—Jeff Birnbaum, Merrill Lynch

In this chapter, you will learn how to

- **Describe the concepts of virtualization**
- **Explain why PC and network administrators have widely adopted virtualization**
- **Describe how virtualization manifests in modern networks**

Virtualization takes your everyday notion of computing and turns it on its head. Left becomes right. Red becomes blue. Physical computers become virtual computers. It might sound complicated—properly configuring a real computer is hard enough—but once you see it in action, it makes perfect sense. In the simplest terms, *virtualization* is the process of using special software—a class of programs called *hypervisors* or *virtual machine managers*—to create a complete environment in which a guest operating system can function as though it were installed on its own computer. That guest environment is called a **virtual machine (VM)**. You learned about one very important virtual machine back in Chapter 19 called Windows XP Mode, which uses a program called Windows Virtual PC to run a virtual Windows XP operating system in Windows 7. Figure 30.1 shows another example: a system running Windows 7 using a program called VMware Workstation to host a virtual machine running Ubuntu Linux.



• **Figure 30.1** VMware running Linux

This chapter begins by explaining the ideas behind virtualization. The chapter then explores the motivating factors behind the widespread adoption of virtualization throughout the IT industry. The chapter concludes with an in-depth look at how modern networks implement virtualization. Some of the details presented here go beyond the CompTIA A+ 220-802 exam, but I include them to help you understand the scope and power of virtualization.

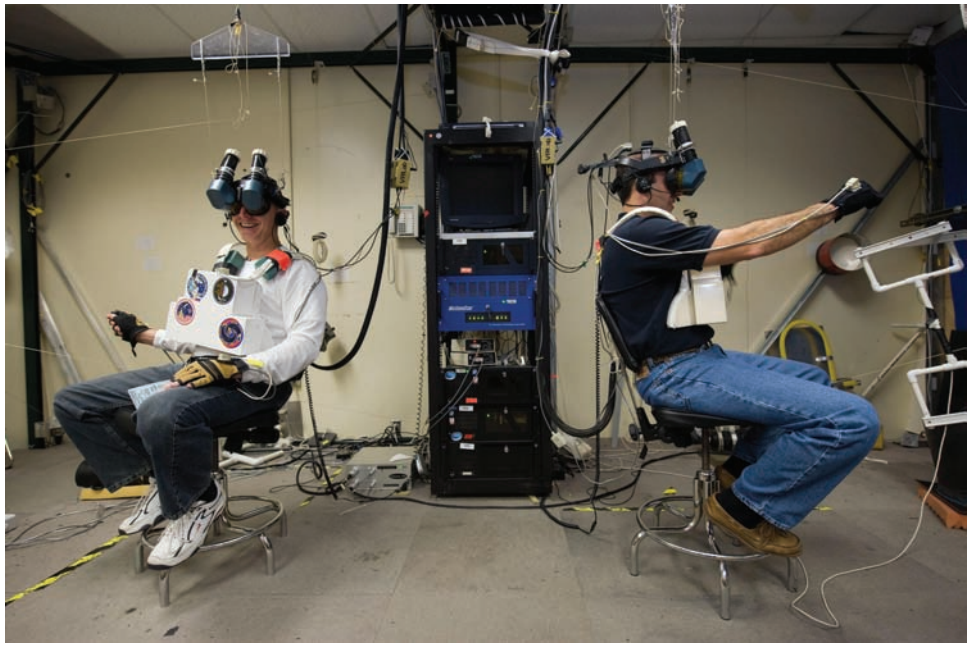
Historical/Conceptual

What Is Virtualization?

Ask 100 people what the term *virtual* means and you'll get a lot of different answers. Most people define *virtual* with words like "fake" or "pretend," but these terms only begin to describe it. Let's try to zero in on virtualization using a term that you've likely heard: *virtual reality*. For most of us, the idea of virtual reality starts with someone wearing headgear and gloves, as shown in Figure 30.2.

The headgear and the gloves work together to create a simulation of a world or environment that appears to be real, even though the person wearing them is located in a room that doesn't resemble the simulated space. Inside this virtual reality, you can see the world by turning your head, just as you do in the real world. Software works with the headset's inputs to emulate a physical world. At the same time, the gloves enable you to touch and move objects in the virtual world.

To make virtual reality effective, the hardware and software need to work together to create an environment convincing enough for a human



• **Figure 30.2** Virtual reality training (photo courtesy of NASA)

to work within it. Virtual reality doesn't have to be perfect—it has limitations—but it's pretty cool for teaching someone how to fly a plane or do a spacewalk, for example, without having to start with the real thing (see Figure 30.3).

Virtualization on a computer is virtually (sorry, can't pass up the pun) the same as virtual reality for humans. Just as virtual reality creates an environment that convinces humans they're in a real environment, virtualization convinces an operating system it's running on its own hardware.

• **Figure 30.3** Using virtual reality to practice spacewalking (photo courtesy of NASA)

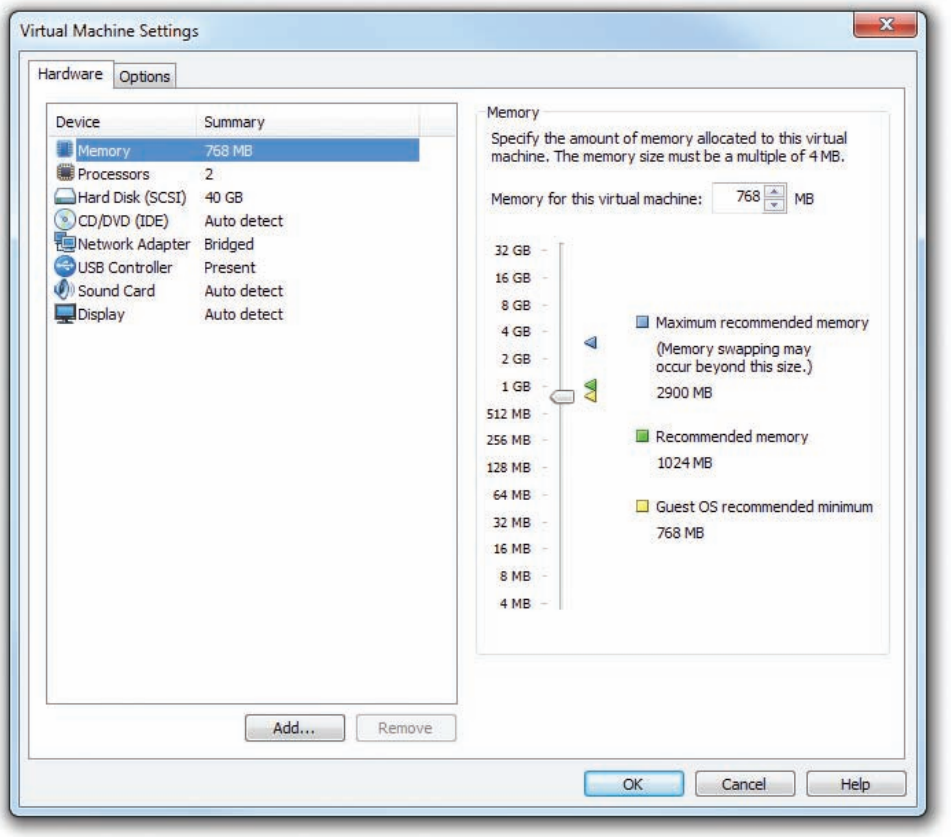
Meet the Hypervisor

A normal operating system uses programming called a *supervisor* to handle very low-level interaction among hardware and software, such as task scheduling, allotment of time and resources, and so on.

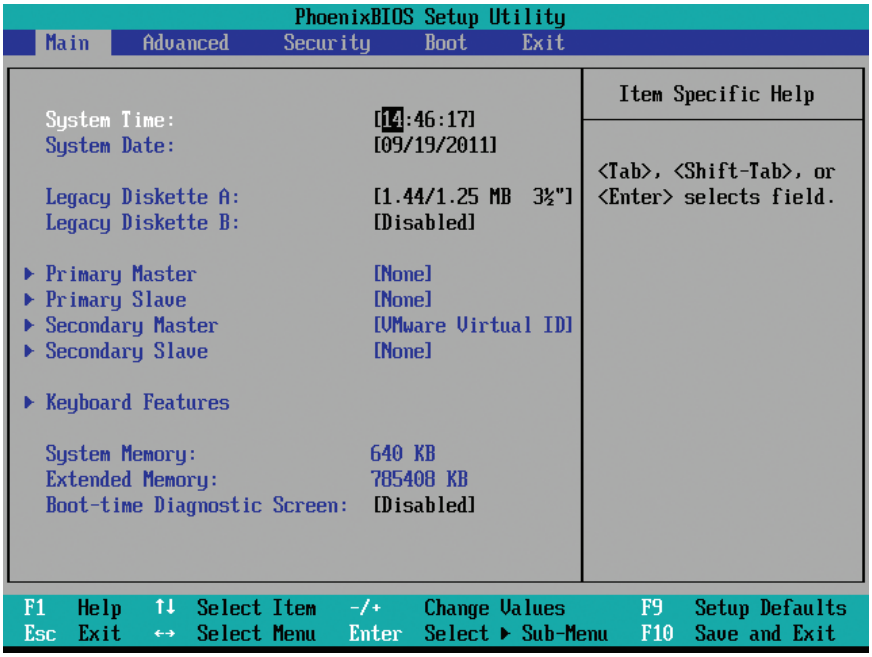
Because virtualization enables one machine—called the **host**—to run multiple operating systems simultaneously, full virtualization requires an extra layer of sophisticated programming to manage the vastly more complex interactions. One common method calls this extra programming a **hypervisor** or **virtual machine manager (VMM)**.

A hypervisor has to handle every input and output that the operating system would request of normal hardware. With a good hypervisor like VMware Workstation, you can easily add and remove virtual hard drives, virtual network cards, virtual RAM, and so on. Figure 30.4 shows the Hardware tab of the Virtual Machine Settings dialog box in VMware Workstation.

Virtualization even goes so far as to provide a virtualized BIOS and system setup utility for every virtual machine. Figure 30.5 shows VMware Workstation displaying the system setup utility, just like you'd see it on a regular computer.



• **Figure 30.4** Configuring virtual hardware in VMware Workstation



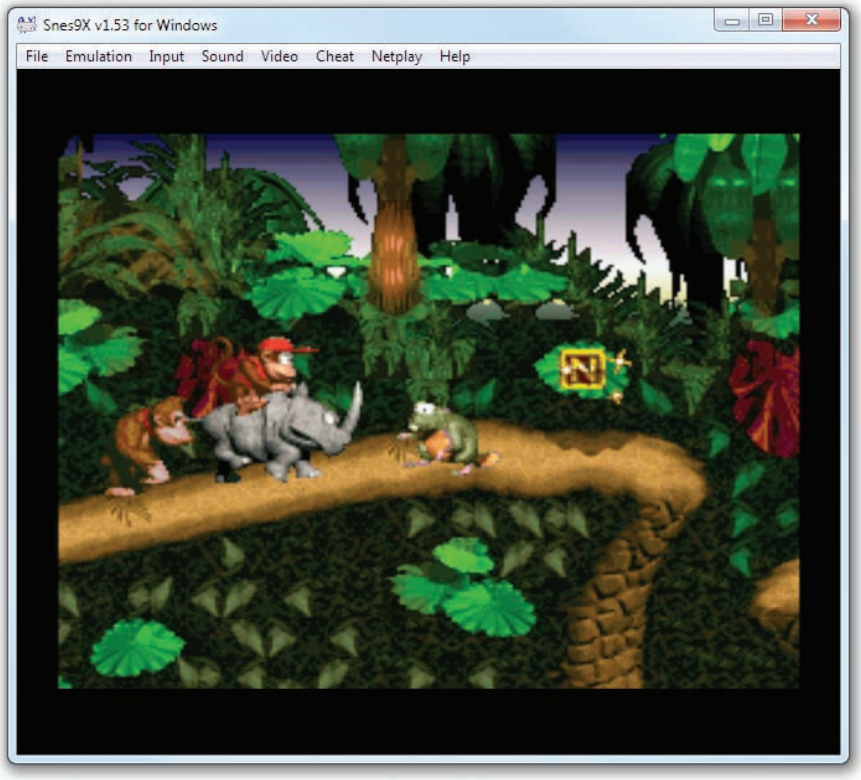
• **Figure 30.5** System setup utility in VMware Workstation

While the CompTIA A+ 220-802 exam objectives include emulation as a part of virtualization, the concepts are not the same. For the sake of completeness, however, know that emulating another platform (using a PC to run Sony PlayStation 2 games, for example) requires hardware several times more powerful than the platform being emulated.

Emulation Versus Virtualization

Virtualization takes the hardware of the host system and segments it into individual virtual machines. If you have an Intel system, a hypervisor creates a virtual machine that acts exactly like the host Intel system. It cannot act like any other type of computer. For example, you cannot create on an Intel system a virtual machine that acts like a Sony PlayStation 3. Hypervisors simply pass the code from the virtual machine to the actual CPU.

Emulation is very different from virtualization. An **emulator** is software or hardware that converts the commands to and from the host machine into an entirely different platform. Figure 30.6 shows a Super Nintendo Entertainment System emulator, Snes9X, running a game called *Donkey Kong Country* on a Windows system.



• **Figure 30.6** Super Nintendo emulator running on Windows

Sample Virtualization

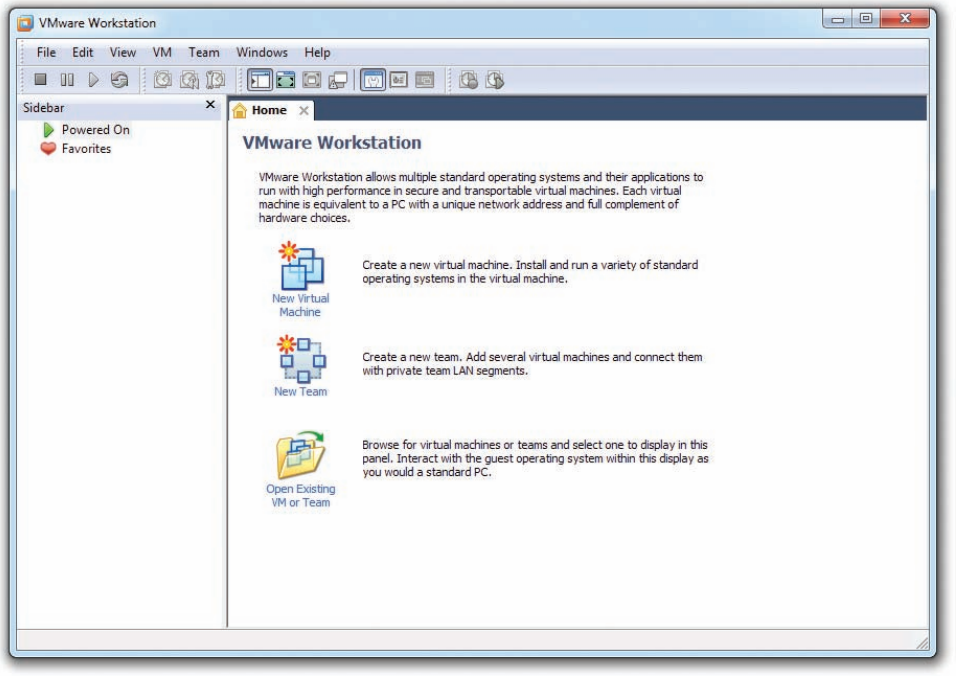
You can perform virtualization in a number of ways; this chapter will show you several of them. Before I go any further, though, let's take the basic pieces you've learned about virtualization and put them together in one of its simpler forms. In this example, I'll use the popular VMware Workstation on a Windows 7 system and create a virtual machine running Ubuntu Linux.

Begin by obtaining a copy of VMware Workstation. This program isn't free, but VMware will give you a 30-day trial. Go to www.vmware.com to get a trial copy. A freshly installed copy of VMware Workstation looks like Figure 30.7.

Clicking New Virtual Machine prompts you for a Typical or Custom setup (see Figure 30.8). These settings are only for backward-compatibility with earlier versions of VMware, so just click Next.

The next dialog box is where the fun starts. Here, VMware Workstation asks for an operating system installation disc. Just because you're creating a virtual machine, don't think the operating system and applications aren't real. You need to install an operating system on that virtual machine. You do this just as you would on a machine without virtualization, using some form of optical media. Would you like to use Microsoft Windows in your virtual machine? No problem, but know that every virtual machine you create on which you install Windows requires a separate, legal copy of Windows.

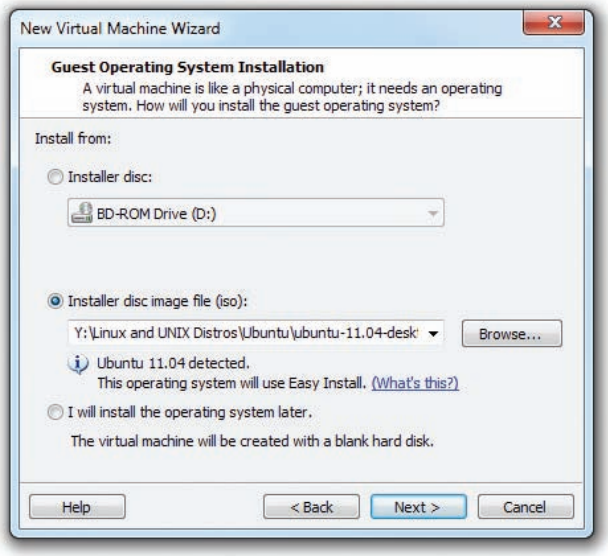
Because virtual machines are so flexible on hardware, VMware Workstation enables you to use either the host machine's optical drive or an ISO file. I'm installing Ubuntu, so I downloaded the latest ISO image from the Ubuntu Web site (www.ubuntu.com), and as Figure 30.9 shows, I've pointed the dialog box to that image.



• **Figure 30.7** VMware Workstation

Microsoft's Virtual PC is a free competitor to VMware Workstation. Virtual PC works well, but it lacks some of the more interesting features included in VMware Workstation.

• **Figure 30.8** Selecting a Typical or Custom setup

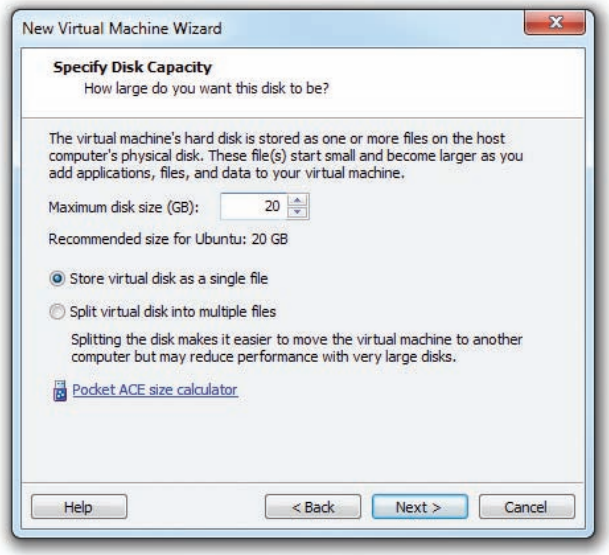


• **Figure 30.9** Selecting the installation media

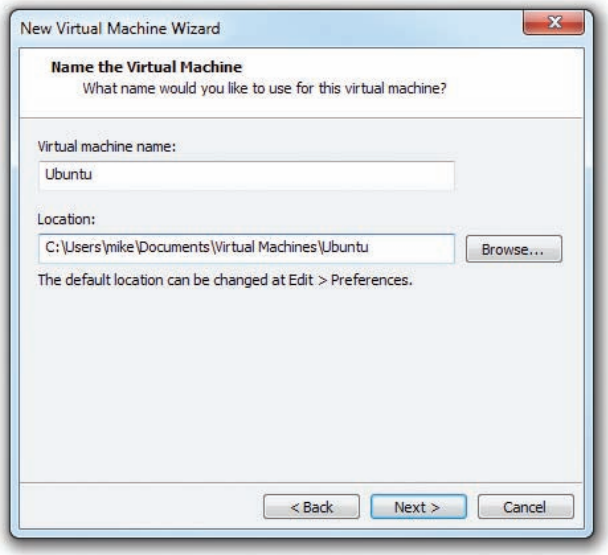
Use descriptive names for virtual machines. This will save you a lot of confusion when you have multiple VMs on a single hypervisor.

Compared to some other virtualization programs, VMware Workstation is a powerful, easy-to-use program. If you look closely at Figure 30.9, you'll see that VMware reads the installation media (note the "Ubuntu 11.04 Detected"). Because VMware knows this operating system, it configures all of the virtual hardware settings automatically: amount of RAM, virtual hard drive size, and so on. You can change any of these settings, either before or after the virtual machine is created. Refer to Figure 30.4 to see these settings. Next, you need to accept the size of the virtual drive, as shown in Figure 30.10.

You also need to give the virtual machine a name (see Figure 30.11). By default, VMware Workstation uses a simple name. For this overview, accept



• **Figure 30.10** Setting the virtual drive size



• **Figure 30.11** Entering a VM name and location

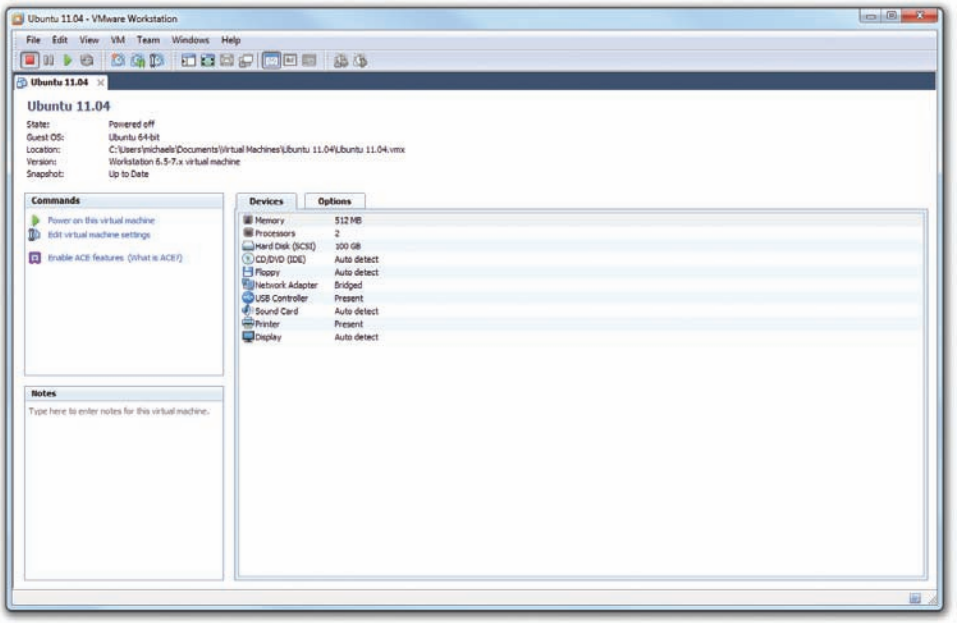
the default name: Ubuntu. This dialog box also lets you decide where you want to store the files that comprise the virtual machine. Note that VMware uses a folder in the user's Documents folder called Virtual Machines.

After you've gone through all the configuration screens, you can start using your virtual machine. You can start, stop, pause, add, or remove virtual hardware.

VMware is very convenient; it even configures the boot order in the virtual system setup to boot first from the installation media, making the Ubuntu installation automatic (see Figure 30.12).

After the virtual machine installs, you then treat the VM exactly as though it were a real machine. The only big difference is that VMware replaces CTRL-ALT-DELETE with CTRL-ALT-INSERT. Figure 30.13 shows VMware Workstation with the single VM installed but not running. A VM goes through a POST process just like any computer, as shown in Figure 30.14.

• **Figure 30.12** Ubuntu installing into the new virtual machine



• **Figure 30.13** VMware Workstation with a single VM

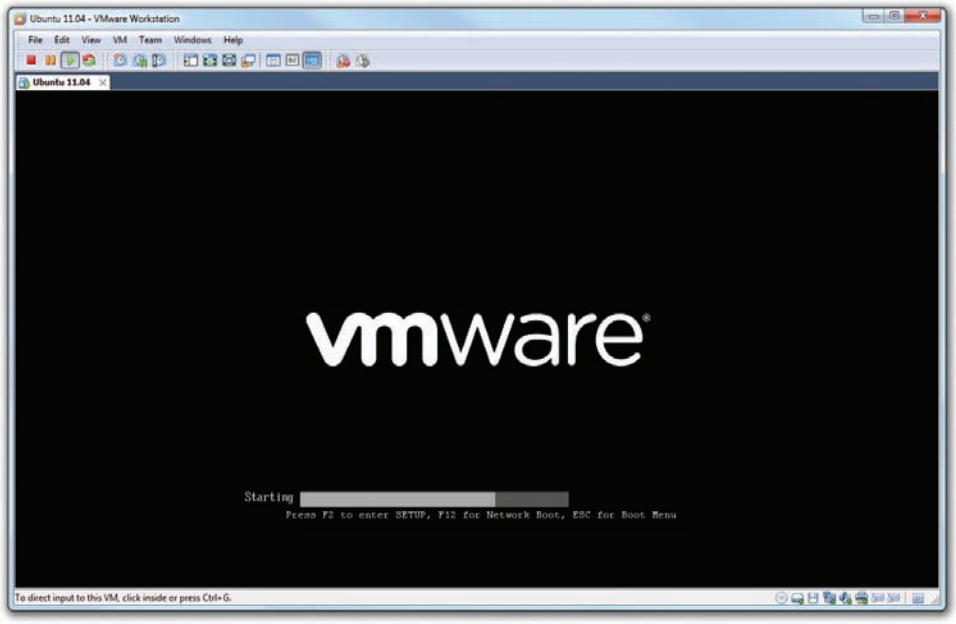


Figure 30.14 POST in a virtual machine

If you wish, you can even access a complete virtual system setup utility by pressing the DELETE key just like on a real system.

Congratulations! You've just installed a *virtual desktop*. Virtual desktops were the first type of popular virtual machines seen in the PC world, championed by VMware and quickly copied by other virtualization programs.

There's a lot more to virtualization than just virtual desktops, however, but before I dive in too far, let's step back a moment and understand a very important question: Why do we virtualize?

Why Do We Virtualize?

Virtualization has taken the computing world by storm, but for those who have never seen virtualization, the big question has got to be: Why? Let's talk about the benefits of virtualization. While you read this section, keep in mind two important things:

- A single hypervisor on a single system will happily run as many virtual machines as its RAM, CPU, and drive space allow.
- A virtual machine that's shut down is little more than a file (or two) sitting on a hard drive.

While you're reading about the benefits of virtualization, don't forget about the costs. To run one or more virtual machines, you'll need a powerful machine—fast processor, loads of RAM (this is usually the limiting factor in how many virtual machines you can run at the same time), and a good amount of hard drive space. If you want the virtual PC to connect to a network, your physical PC needs a NIC.

Virtualized operating systems use the same security features as real operating systems. For each virtual machine user account, you'll need to keep track of user names, passwords, permissions, and so on, just like on a normal PC.

Power Saving

Before virtualization, each installed OS needed to be on a unique physical system. With virtualization, you can place multiple virtual PCs on a single physical system, reducing electrical power use substantially. Rather than one machine running Windows Server 2008 (or Server 2008 R2) and acting as a file server and DNS server, and a second machine running Linux for a DHCP server, for example, the same computer can handle both operating systems simultaneously. Expand this electricity savings over an enterprise network or on a data server farm and the savings—both in terms of dollars spent and electricity used—are tremendous.

Hardware Consolidation

Similar to power saving, why buy a high-end server, complete with multiple processors, RAID arrays, redundant power supplies, and so on, and only run a single server? With virtualization, you can easily beef up the RAM and run a number of servers on a single box.

Rebooting virtual machines is easy, but keep an eye on your physical machine. If your PC goes down, it brings all your virtual machines down with it! Be sure to back up mission-critical virtual machines to an external hard drive—remember that a virtual machine is just a file on your hard drive. You can always install the backed-up virtual machines on another physical machine if necessary.

System Recovery

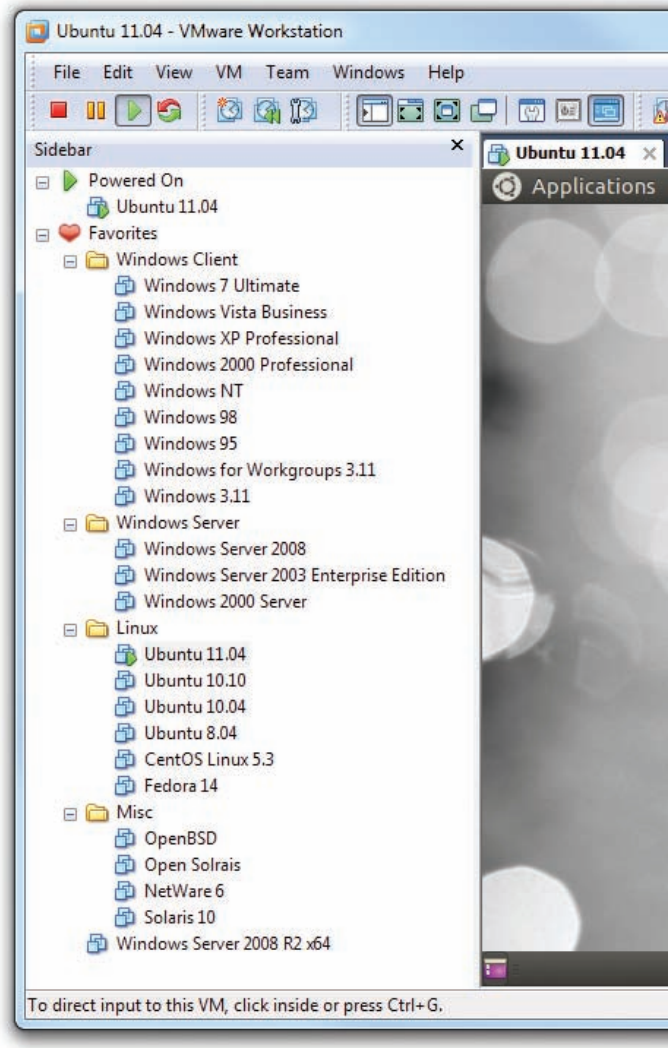
Possibly the most popular reason for virtualizing is to keep uptime percentage as high as possible. Let's say you have a Web server installed on a single system. If that system goes down—due to hacking, malware, or so on—you need to restore the system from a backup, which may or may not be easily at hand. With virtualization, you merely need to shut down the virtual machine and reload an alternative copy of it.

Think of virtual machines like you would a word processing document. Virtual machines don't have a "File | Save" equivalent, but they do have something called a **snapshot** that enables you to save an extra copy of the virtual machine as it is exactly at the moment the snapshot is taken. Figure 30.15 shows VMware Workstation saving a snapshot.

• **Figure 30.15** Saving a snapshot

System Duplication

Closely tied to system recovery, system duplication takes advantage of the fact that VMs are simply files, and like any file, they can be copied. Let's say you want to teach 20 students about Ubuntu Linux. Depending on the hypervisor you choose (VMware does this extremely well), you can simply install



• **Figure 30.16** Lots of VMs used for research

a hypervisor on 20 machines and copy a single virtual machine to all the computers. Equally, if you have a virtualized Web server and need to add another Web server (assuming your physical box has the hardware to support it), why not just make a copy of the server and fire it up as well?

Research

Here's a great example that happens in my own company. I sell my popular Total Tester test banks: practice questions for you to test your skills on a broad number of certification topics. As with any distributed program, I tend to get a few support calls. Running a problem through the same OS, even down to the service pack, helps me solve the problem. In the days before virtualization, I commonly had seven to ten PCs, using dual-boot, each keeping copies of a particular Windows version. Today, a single hypervisor enables me to support a huge number of Windows versions on a single machine (see Figure 30.16).

Clearly there are a number of good reasons to virtualize some of the computers in a network. Let's look at implementation now.

Virtualization in Modern Networks

You've already seen virtualization in action with the example shown using VMware Workstation earlier in this chapter. Many networks use a few virtual machines to augment and refine a traditional network closet. VMware Workstation is how I first performed virtualization on PCs, but the technology and power have grown dramatically over the past few years.

VMware Workstation requires an underlying operating system (such as Windows), so it functions essentially like a very powerful desktop application. What if you could remove the OS altogether and create a bare-metal implementation of virtualization?

VMware introduced ESX in 2001 to accomplish this goal. ESX is a hypervisor that's powerful enough to replace the host operating system on a physical box, turning the physical machine into a machine that does nothing but support virtual machines; no Windows, no Ubuntu—just ESX.

ESX by itself isn't much to look at; it's a tiny operating system/hypervisor that's usually installed on something other than a hard drive. Figure 30.17 shows how I loaded my copy of ESX: via a small USB thumb drive. Power up the server; the server loads ESX off the thumb drive; and in short order, a very rudimentary interface appears where I can input

The system shown in Figure 30.16 could obviously never run all those VMs at the same time.

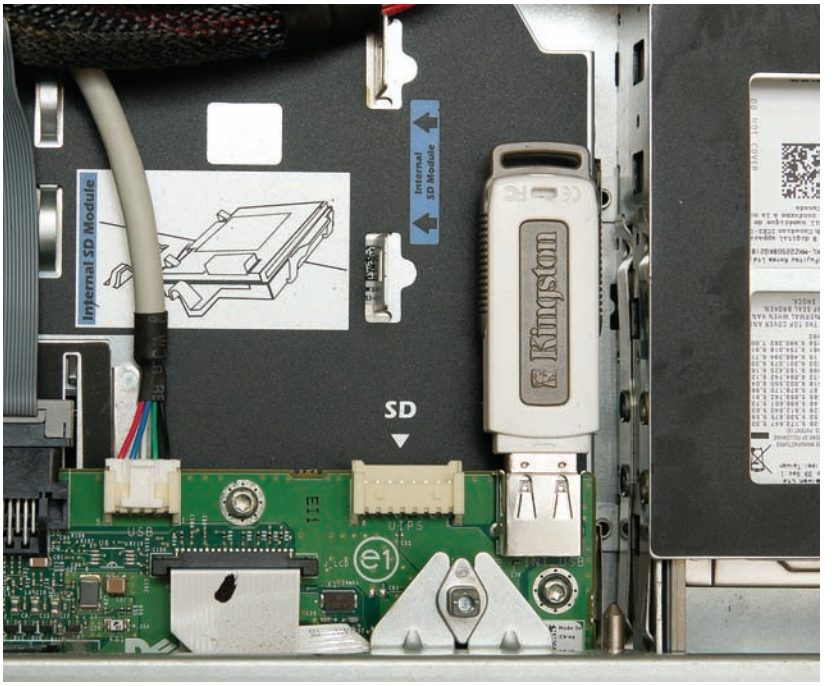
For all you abbreviation lovers, I have some good news and some bad news about "ESX." Officially, it means nothing. Unofficially, it stands for "Elastic Sky," which is probably why it officially means nothing.

essential information, such as a master password and a static IP address.

Don't let ESX's small size fool you. It's small because it only has one job: to host virtual machines. ESX is an extremely powerful operating system/hypervisor.

Notice the built-in USB port shown in Figure 30.17. The popularity of hypervisors on dedicated servers makes these ports extremely common in a serious server box like the Dell system shown.

Powerful hypervisors like ESX are rarely administered directly at the box. Instead you use tools such as VMware's vSphere Client, so you can create, configure, and maintain virtual machines on the hypervisor server from the comfort of a client computer running this program. Once the VM is up and running, you can close the vSphere client, but the VM will continue to run happily on the server. For example, let's say you create a VM and install a Web server on that VM. As long as everything is running well on the Web server, you will find yourself using the vSphere client only to check on the Web server for occasional maintenance and administration.



• **Figure 30.17** USB drive on server system

So you now really have two different ways to virtualize: using virtual machine managers like VMware's Workstation to manage virtual desktops, and using powerful hypervisors like ESX to manage virtual servers. Granted, you could run a server like a Web browser in VMware Workstation, and you also could run a copy of Windows 7 Ultimate from an ESX system. Nothing is wrong with doing either of these.

Thus far, this chapter sounds like an advertisement for VMware. VMware really brought virtualization to the PC world and still holds a strong presence, but there are a number of alternatives to VMware products. Let's see what else is available.

A free version of ESX is available. Called ESXi, it lacks a number of ESX's features but is still quite powerful.

Tech Tip

VMM Versus Hypervisor

Some writers will use the term virtual machine manager *to describe virtual machine software that runs on top of a host operating system. They'll use the term* hypervisor *to describe only software that does not need a host operating system. Using this terminology, VMware Workstation is a virtual machine manager and ESX is a hypervisor.*

Other writers call both the hosted and bare-metal—or native*—virtualization software products* hypervisors, *but make a distinction in other descriptive words (such as* hosted *or* native*).*

Virtual Machine Managers

When it comes to the more basic virtual machine managers, you have a huge number of choices. The one you use is going to be determined by features and prices.

VMware Workstation

The granddaddy and front leader for virtualization, VMware Workstation, comes in both Windows and Linux versions. VMware Workstation runs virtually (pun!) on any operating system you'll ever need and is incredibly stable and proven. Too bad it's not free.

One of the more interesting features of VMware Workstation is VMTools. VMTools adds useful features such as copy/cut and paste between the virtual desktop and the real desktop.

Try This!

Creating a Virtual Machine

It's difficult to understand how virtual machines work (and how amazing they are) until you've made one yourself. VMware sells many different virtualization products, most of which are too powerful and too expensive for our experimentation purposes. Fortunately, they also offer VMware Player, a basic virtual machine manager that's easy enough for anyone to use, so Try This!

Go to VMware's Web site (www.vmware.com) and search for VMware Player. Follow the Download link and choose the version of VMware Player that matches your OS. (You'll need to sign up for an account before you can download the application.)

While that's downloading, go to the Ubuntu Linux Web site (www.ubuntu.com) and follow the links to download the latest version of Ubuntu. Don't use the Windows installer listed on the Ubuntu Download Web page. Instead, download the installation image using the Start download button.

When the downloads have finished, run the VMware Player executable file. Follow the instructions as you would with any other application. When finished, open VMware Player. Accept the End User License Agreement (EULA), then click on Create a New Virtual Machine.

Use the Easy Install method. VMware Player will build the virtual machine and install the Ubuntu operating system at the same time. You'll need to find where you saved the Ubuntu installation image. Use the default settings provided by the wizard, and create a user name and password when prompted.

After the virtual machine has been installed, you can launch it from the main VMware Player screen by selecting it from the list of machines and clicking *Play Virtual Machine*. Congratulations! You've just created a virtual machine on your PC.

Virtual PC

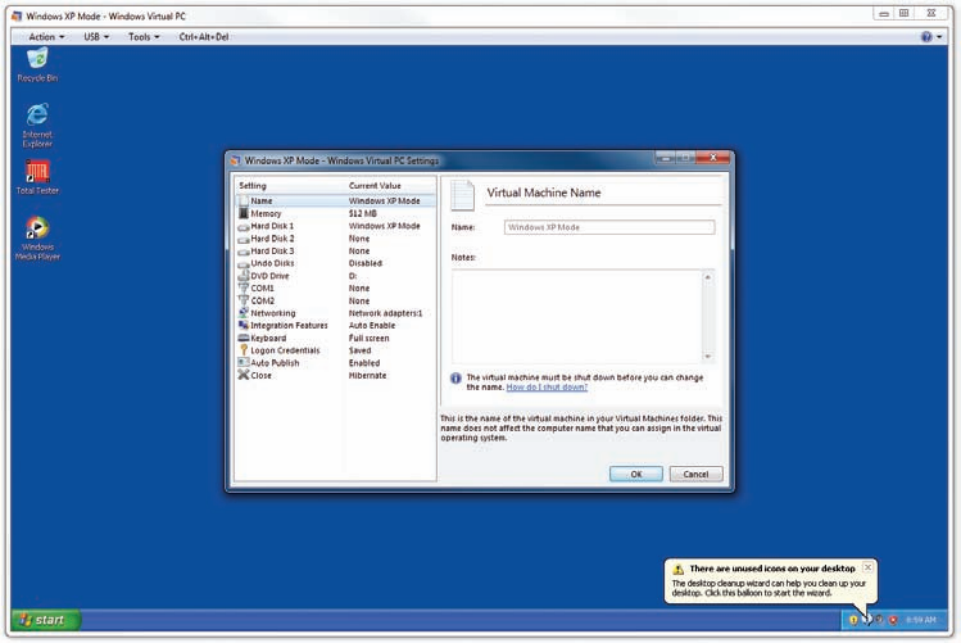
Microsoft has offered a few different virtual machine managers over the years, with the current mainstream product being Windows Virtual PC (see Figure 30.18). Windows Virtual PC is free, but has some serious limitations. First, it only works on Windows 7 Professional, Ultimate, and Enterprise. Second, it only officially supports Windows VMs, although a few intrepid souls have managed to get Linux working.

Remember Windows XP Mode from Chapter 19? It uses Virtual PC and a copy of Windows XP to create a virtual machine on your PC!

Cross Check

Compatibility

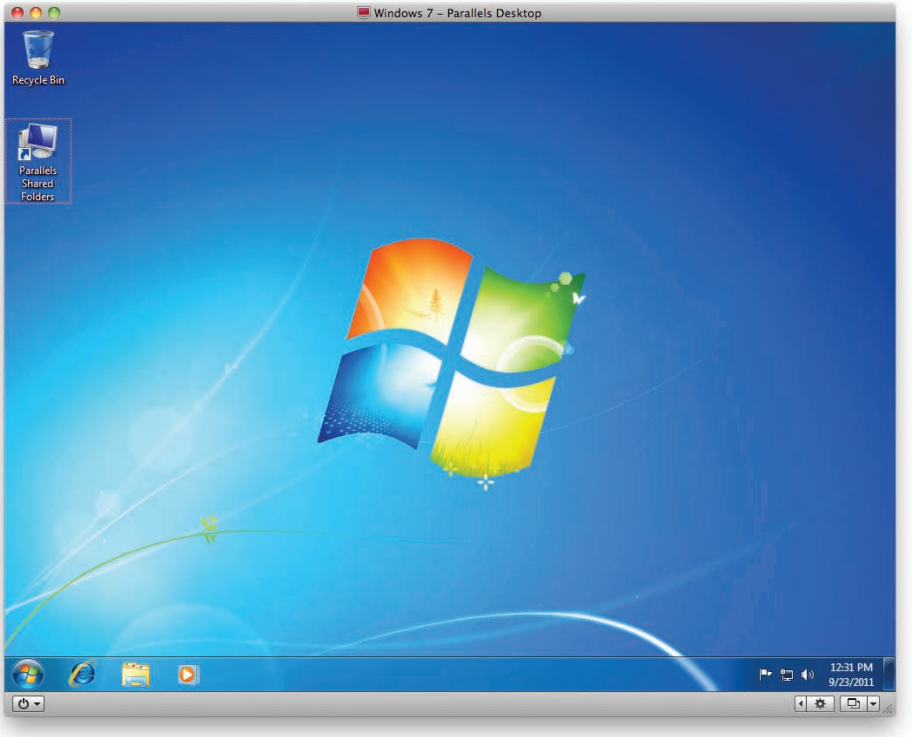
You learned about Windows XP Mode and other compatibility modes back in Chapter 19. Remember that Windows XP Mode is really just a virtual OS running inside Microsoft's Virtual PC. What other compatibility features does Windows 7 include? Which editions of Windows 7 include Windows XP Mode? Does Windows Vista include Windows XP Mode?



• **Figure 30.18** Windows Virtual PC

Parallels

Parallels is the most popular virtualization manager for Mac OS X (see Figure 30.19), although VMware Fusion is a close second. Parallels supports all popular operating systems, and even has a fair degree of 3-D graphics support; more so than even the mighty VMware. Parallels also offers Windows and Linux versions.



• **Figure 30.19** Parallels for Mac

KVM

Of course, the open source world has its players too. While picking a single product to represent the Linux/Unix world is hard, no one who knows virtualization would disagree that KVM from Red Hat is a dominant player. Unlike the other virtual machine managers discussed, KVM also supports a few non-x86 processors.

Don't think for a moment that this list is complete! There are lots of other virtual machine options for your desktop, especially if your host machine runs Linux. The most fun you'll have learning about

virtualization is the playtime involved experimenting with the many options available.

Hypervisors

While you have lots of choices when it comes to virtual machine managers, your choices for real embedded hypervisors are limited to the two biggies: VMware's ESX and Microsoft's HyperV. There are others, such as Oracle's VM Server, but nothing has the market share of ESX or HyperV.

ESX

I've already discussed a few aspects of ESX, so instead I'll delve into the features that make ESX so popular. When it comes to real server virtualization, VMware truly leads the pack with a host of innovations (some of which are add-on products) that make ESX almost unstoppable. Here are a few examples:

- **Interface with large storage** ESX virtual machines easily integrate with network attached storage (NAS) and storage area networks (SANs) to handle massive data storage.
- **Transparent fault tolerance** ESX can monitor and automatically recover failed VMs with little or no input.
- **Transparent server transfer** You can move a *running* VM from one machine to another. How cool is that?
- **High virtual CPUs** Most hypervisors support a limited number of virtual CPUs, usually two at most. ESX can support up to 32 CPUs, depending on the vSphere product version you purchase to support it.

HyperV

Although HyperV can't stand toe-to-toe with ESX, it has a few aces up its sleeve that give it some intrigue. First, it's free. This is important in that ESX, with only a few extra add-ons, can cost thousands of dollars. Second, it comes as a stand-alone product or as part of Windows Server 2008 and even on some versions of Windows 7, making it easy for those who like to play to access it. Third, its simplicity makes it easier to learn for those new to using hypervisors. Watch HyperV. If Microsoft does one thing well, it's taking market share away from arguably better, more powerful competitors, while slowly making its product better.

Chapter 30 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about virtualization.

Describe the concepts of virtualization

- Virtual reality creates a simulation of a world or environment that appears to be real, even though the person wearing the headgear and gloves is located in a room that doesn't resemble the simulated space. Virtual computing follows a similar concept.
- In virtual computing, software called a hypervisor or virtual machine manager creates one or more environments, called virtual machines (VMs), on a single machine. You can install an OS into each VM and thus run several OSs simultaneously on a single machine.
- The hypervisor handles the communication between the OSs installed and the hardware. The hypervisor can easily add and remove hard drives, memory space, networking capabilities, and more.
- Emulation differs from virtualization: emulation software translates commands from an application into machine language the host computer can understand, whereas virtualization creates an environment that is native to the application—an operating system, in this case—requiring no translation.

Explain why PC and network administrators have widely adopted virtualization

- Going virtual enables companies to combine multiple servers onto fewer machines than in traditional computing. This offers tremendous savings in hardware purchases, electricity use, and the space used for computing.
- Because a VM is only a single file or two, a hacked or corrupted server can rapidly be replaced with a snapshot (a backup) taken of the properly working server. This provides better uptime than in a traditional server setup. Likewise, the minimal file numbers make it easy to duplicate a VM.
- The capability to run many operating systems on a single physical machine makes multiplatform testing and research much easier and less costly than with traditional setups.

Describe how virtualization manifests in modern networks

- The simplest way virtualization manifests in networks is through one or more VMs performing chores that would have taken multiple physical boxes previously. VMware Workstation is the most common VM implementation tool in these sorts of networks.
- More aggressive network needs can use bare-metal virtualization software that removes the need for an operating system on the VM-supporting machine. These hypervisors, such as VMware ESX, take up minuscule space. You manage them remotely through client software, rather than at the server box.
- The more popular virtual machine managers include the aforementioned VMware Workstation, plus Microsoft Virtual PC, Parallels for OS X, and KVM on the Linux side. The more popular native hypervisors include ESX and HyperV.

Key Terms

emulator *(1156)*
host *(1155)*
hypervisor *(1155)*
snapshot *(1161)*
virtual machine (VM) *(1152)*
virtual machine manager (VMM) *(1155)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all the terms will be used.

1. A(n) _____ is a complete environment for a guest operating system to function as though that operating system were installed on its own computer.
2. A machine that runs multiple operating systems simultaneously is called a(n) _____.
3. A bare-metal machine that supports virtualization software without needing a host operating system is commonly called a(n) _____.
4. A(n) _____ can convert the commands to and from a host machine to an entirely different platform.
5. You can create a(n) _____ as a backup for a virtual machine.

Multiple-Choice Quiz

1. Tom is installing a Windows 7 Ultimate virtual machine onto a copy of VMware Workstation. Which of the following does he need?
   - **A.** A valid copy of Windows 7 Ultimate installation media
   - **B.** The IP address for the virtual machine host
   - **C.** A disk image of another computer's installed Windows 7 Ultimate
   - **D.** A valid ESX key
2. The number of running virtual machines on a single host is limited by what factor?
   - **A.** Physical RAM
   - **B.** Virtual RAM
   - **C.** Physical NICs
   - **D.** Virtual NICs
3. When a virtual machine is not running, how is it stored?
   - **A.** Firmware
   - **B.** RAM drive
   - **C.** Optical disc
   - **D.** Files
4. VMware Workstation replaces CTRL-ALT-DELETE with which of the following?
   - **A.** A mouse click
   - **B.** CTRL-ALT-INSERT
   - **C.** CTRL-ALT-TAB
   - **D.** CTRL-ALT-SHIFT
5. Which of the following would *not* run on VMware Workstation for Windows?
   - **A.** Windows XP
   - **B.** Sony PlayStation 2
   - **C.** Ubuntu Linux
   - **D.** Windows Vista
6. Which of the following virtualization programs works well with Mac OS X? (Select the best answer.)
   - **A.** ESX
   - **B.** KVM
   - **C.** Parallels
   - **D.** Virtual PC
7. The boss flies into your office yelling that the virtualized Web server has been hacked and now displays only purple dinosaurs. Which of the following would be the fastest way to fix the problem?
   - **A.** Restore from backup
   - **B.** Run System Restore
   - **C.** Reinstall Windows
   - **D.** Load an earlier snapshot
8. Which of the following is *not* a good reason for virtualization?
   - **A.** Power saving
   - **B.** Hardware consolidation
   - **C.** System recovery
   - **D.** Reduced hardware costs

9. Powerful hypervisors like ESX are often booted from _____.
   - **A.** Floppy diskettes
   - **B.** USB thumb drives
   - **C.** Firmware
   - **D.** Windows

10. Which players dominate the entire hypervisor market? (Select two.)
   - **A.** ESX
   - **B.** HyperV
   - **C.** Parallels
   - **D.** KVM

Essay Quiz

1. A company has three discrete servers: a file server running Linux, a contact and e-mail server running Windows Server, and a DNS and DHCP server running an earlier version of Windows Server. Make a case for or against going virtual with this setup.

2. Write a comparative essay on VMware Workstation and ESX. What are the strengths of each type of virtualization setup? When would you use ESX over VMware Workstation?

Lab Projects

• Lab Project 30.1

Acquire a copy of VMware Workstation or another virtualization program and create some virtual machines. If you can add the VM host to a working network, then attempt to access the different VMs running and access other computers from any of the VMs. This should be a fun lab. Here are links to VM software:

www.vmware.com/products/workstation/overview.html

www.virtualbox.org/wiki/Downloads

www.microsoft.com/windows/virtual-pc/

• Lab Project 30.2

Analyze the current server setup at your school or office. Does it use virtualization? If so, which programs does it use for which purposes? If not, discuss how virtualization could be implemented to make the network more efficient.

chapter 31

The Right PC for You

"If you build it, he will come."

—*Field of Dreams*

In this chapter, you will learn how to

- **Research and build a standard thick client**
- **Customize a professional PC**
- **Build a specialized consumer PC**

Now that you've learned all about PCs, you have the great joy of being able to build the PC of your desire, choose your favorite video card or motherboard, and assemble, from the ground up, the perfect system for you or your client. People will turn to you for advice, too: Which parts do I need? Where should I buy them? What do you think about this?

There's nothing wrong with buying a prebuilt system from a local brick-and-mortar or online store. If you want solid warranties, repair agreements, and so on, Dell or HP can help you out. But off-the-shelf computers aren't for everyone. Your needs or your client's needs might be too specific. In that case, it's time for you to do one of the most fun things a PC tech can do: the custom PC build!

For the first time in the history of the CompTIA A+ exams, CompTIA requires you to understand how to build certain types of PCs. This chapter will help you define these PC types, understand the issues involved in building these computers, and, at the same time, have a little fun.

Because this is a first for CompTIA, the creative team at Total Seminars took extra time to understand what CompTIA was trying to say. In general, we agree with the definitions of the custom configurations with the exception of the following two types. From the 220-801 exam objectives:

1.9 Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs.

- Standard thick client
  - Desktop applications
  - Meets recommended requirements for running Windows
- Thin client
  - Basic applications
  - Meets minimum requirements for running Windows

I'm not a fan of the term "client." It's outdated. What CompTIA calls a *thick client*, I'd call a *basic desktop*, and instead of a *thin client*, I'd call it a *single-purpose machine* (because that's all a thin client can handle). To CompTIA, the only real separation between a thick client and a thin client is meeting the "recommended" or "minimum" requirements for Windows, respectively. It's oversimplified. Even *that* might be okay, except Microsoft no longer provides minimum requirements for Windows 7. Oh well. We can only guess what CompTIA was thinking.

This chapter begins by explaining how to find the parts for a custom PC—you'll be doing a lot of reading, that's for sure. The rest of the chapter discusses the components you need for each custom build: thick clients, thin clients, virtualization and media workstations, home theater and server PCs, and (best of all) gaming PCs.

801

Building Your First PC

There's almost no better feeling than when you realize you know enough about PCs that you can say: "I think I'm comfortable building my own PC!" If you don't feel ready, let the information in this chapter be that extra push that takes you over the edge.

Building your first PC is both fun and scary. This is the first time you bring together everything you know about hardware. You'll make mistakes, and some brand-new piece of equipment you buy won't work the first time. You'll mount the CPU wrong and the system won't boot. That huge tower case with 23 fans will make too much noise and you'll hate it. But for all these mistakes, don't lose track of the fact that you're building your own PC. Your computer . . . your . . . precious (see Figure 31.1)!

• Figure 31.1 Mike and "Precious," his favorite self-built PC

Evaluating Parts

The most difficult (and most fun) part of buying a PC is picking which parts you want. Knowing which parts to buy for each type of PC is the cornerstone of this entire chapter. Let's take a moment to consider the processes and steps you can use to discover and evaluate the right parts for specific system types.

Read the Reviews

Every component has a review somewhere. Go to Google, type in the name and model number of a part, and add the word "review" at the end. There are two types of reviews: industry reviews written by professionals, and personal reviews written by people who purchased and use the part. Let the Google search I described show you how to the find the professional reviews. Newegg.com is one of my favorite places to read personal reviews.

Read the Fine Print

Learn everything you can about the part. Take some time to read the technical specifications. Check the return and warranty policy of the manufacturer and the retailer. Make sure you have some recourse if the part breaks or doesn't function as advertised.

Compare

Before you buy a part, see what folks say about the competitors' parts. Are there other parts that cost less, have better reviews, or use less power?

Put It in *Y*our Hand

If you're lucky enough to live near a big retailer like Fry's Electronics or Micro Center, get in your car and go check out the part. Look for a display model. Look at the back of the box. See what extra parts are included. Talk to the salespeople about their experiences and the returns they've seen; ask about alternatives they like better.

Thick Client

CompTIA wants to call a general-purpose SOHO computer a **thick client**. Fine—let's have a laugh at the guy wearing the belt and suspenders, and then come up with some guidelines for building a thick client.

Thick clients are general-purpose machines. That means they don't have the fastest drives or the best video cards, but, by the same token, they don't use low-end parts, either. You need to create a platform that will support 90 percent of the folks wanting to use a computer in the home or office.

To begin researching parts for a thick client, look at the recommended hardware requirements for the operating system you intend to use. In this case, I want to install Windows 7 Ultimate 64-bit. I like Ultimate because it gives me the most flexibility, and the extra cost means nothing down the road if I later decide to join a Windows domain.

Here are the recommended system requirements for Windows 7 Ultimate 64-bit edition:

- 1 gigahertz (GHz) or faster 64-bit (x64) processor
- 2 GB RAM
- 20 GB available hard disk space
- DirectX 9 graphics device with WDDM 1.0 or higher driver

See Figure 31.2 for my opinion of the requirements.

• **Figure 31.2** Mike laughing uncontrollably

You can do a lot better. Here's my opinion of reasonable and modest hardware for a 64-bit thick client. These values aren't on the exam, but they should be.

- 2 GHz or faster 64-bit (x64) processor with at least two cores
- 4 GB RAM
- Blank 500-GB hard disk
- DirectX 11 video card

You should always go for a 64-bit edition of Windows when building a new PC—why limit yourself?

Size Matters

You can get into all kinds of mental confusion trying to decide how large of a case you want to use, but do yourself a favor and just get a mid-tower. Mid-towers have plenty of drive bays for future expansion without being so massive that they get in the way. A mid-tower will also support almost any motherboard you might choose to install. Take your time finding that perfect case. Unlike manufacturers of most other components, case manufacturers tend to keep making the same case model for many years (see Figure 31.3).

• **Figure 31.3** My Antec 900 mid-tower (because everything's bigger in Texas)

CPU and Motherboard

You begin the system build by deciding on the CPU/motherboard combination for your new system. I'm not going to tell you to buy an Intel or an AMD CPU. Do your own research and draw your own conclusions. I use plenty of both brands. Because this is a thick client and we don't need the most powerful CPU available, consider the following:

- Get a modern socket. You can get great deals on CPUs that use older sockets, but try to stick to whatever socket is current. This makes it possible to upgrade the CPU in the future.
- Avoid the low end *and* the high end. Both Intel and AMD make three levels of CPUs. Try to stick to the middle. Avoid the slowest and the fastest. Don't buy the CPU with the most cores or the fewest cores.
- When it comes to price, the sweet spot should be around $150 to $300. It's amazing, but CPU price points haven't changed much in over a decade. You can spend a lot more or a lot less, but either way is a waste of money or cheating yourself on power.

Now that you've got a CPU, it's time to find that magic motherboard. Your first big choice is the chipset. Take some time to learn about current chipsets that support the CPU of your choice and compare features. Consider the following:

- Total RAM support
- RAID support
- USB, including versions and number of ports
- Onboard video
- Onboard wireless

Once you narrow down your choice to a particular chipset, see which motherboards fit your plans:

- Just because a chipset supports certain features, don't assume the motherboard will as well. Double-check RAM limits, RAID support, USB ports and types, and so on.
- Check the manufacturer's reputation. Good names like ASUS and Intel are going to be better quality motherboards, but there are plenty of other good manufacturers, too.
- Read reviews of the motherboards you like. What are people saying about them?
- Think about how many expansion slots you need. Your motherboard should have at least one PCIe ×16 slot and a few smaller PCIe slots.
- Do you want to use integrated video? Many folks will think the onboard video is acceptable, and certainly well above Windows 7's Aero requirements. If not, you've always got that PCIe ×16 slot waiting for a new, dedicated video card.

Video

Regardless of whether you choose onboard or a dedicated video card, a thick client isn't going to push a graphics card very hard. Even lower-end cards include at least 1 GB of GDDR3 (or better) video RAM, solid processors, and plenty of extras like HDMI ports. You probably don't need to spend any more than about $150. If you spend more money than that, you're stretching into gaming PC territory.

Be sure to check the reviews on a prospective video card and always be sure to do a Google search for a card's model number followed by "noise." Some videos cards are too loud—they'll drive you bonkers.

Try This!

Finding the Right Graphics Card

If you hadn't noticed already, there are a lot of PC components to choose from, covering all levels of price and performance. In the case of the average thick client, you need to keep costs down. If you want or need the power of a dedicated graphics card, however, you should be ready to research prices for your clients, so Try This!

1. Go to www.tomshardware.com. Following the *Articles* link at the top or using the available search box, find their latest "Best Graphics Cards for the Money" article.
2. Read through the list of recommended cards. Using a budget of about $150, which graphics cards do they recommend? What if you spend a little bit more money? What if you spend less?

Monitors

Monitors are a personal choice, but remember that a good monitor will outlast several system builds, so don't be afraid to get a better monitor. A good-quality, widescreen, LED-backlit LCD monitor no smaller than 20 inches diagonally across will serve you well for a long time.

Storage

A thick client will do just fine with a single hard drive. Today's multiple-terabyte drives will store anything you might imagine and then some, and if you actually manage to fill a drive, your mid-tower will easily accept a second or even third drive.

Setting up a RAID array is probably not necessary. Of course, the system needs backup capability, but RAID might be overkill. At the same time, the low cost of drives and the ease of RAID installation makes at least RAID 1 a compelling option for your thick client.

Applications

The typical thick client is going to need a Web browser (or two) and some Microsoft Office–type applications. The recommended 4 GB of RAM won't have any difficulty supporting these types of applications or much more.

Workstation PCs

In modern times, people need computers to get work done. The type of computer you need is defined by the work you do and the way that your IT department decides to organize and network. For the most part, the thick client described earlier is the "go to" workstation PC, but CompTIA defines two other workstation types: the thin client and the virtualization workstation.

Thin Client

A **thin client** is a system designed to handle only very basic applications with an absolute minimum amount of hardware required by the operating system. Thin clients often serve as single-purpose systems, like point-of-sale machines (cash registers). Thin clients can be very small compared to a thick client, which makes them perfect when you want the PC tucked away.

Virtualization Workstations

Virtualization has taken the world of computing by storm over the past few years. As discussed in the previous chapter, virtualization is a powerful technology that enables you to run more than one operating system at the same time on a single computer. With virtualized servers, you can consolidate multiple, power-hungry machines into one box, saving floor space, electricity, and a lot of running around. With workstations, virtualization is most often used to run a second OS on top of the OS installed on the computer's hard drive.

For good performance on a virtualization workstation, install lots and lots of RAM. Each virtualization workstation needs enough memory to run the native operating system, the guest operating system, and any applications running in either OS, so RAM is the most important thing in virtualization. A powerful 64-bit CPU that supports hardware virtualization will also help virtual machines run smoothly. Many desktop computers can run virtual machines, but if you want the best possible performance, you want lots of RAM and a good CPU.

You'll need lots of RAM and a fast CPU to get good performance out of a virtualization workstation.

Media Workstations

When George Lucas made the first *Star Wars* movie, he used camera tricks, miniature models, and stop-motion animation to create the illusion of massive spaceships and robots battling it out in a galaxy far, far away. Twenty years later, he filmed the *Star Wars* prequels in front of massive green screens and used computer-generated imagery (CGI) to transform the bland sets into exotic planets and space stations. I won't get into an argument about which approach produced better movies, but the fact remains that the act of creating films has changed. It's not just films, either—computers have changed the way we create all types of media, including movies, television shows, photography, music, and more.

Computer-aided design (CAD) and *computer-aided manufacturing (CAM)* software enable engineers to create and build components in an industrial setting.

If you want to get involved in this creative revolution, you're going to need a mighty powerful computer. Workstations for creative professionals are customized for the type of media they create. We'll start by looking at graphics workstations (by which I mean workstations for editing still images and using computer-aided design/computer-aided manufacturing software), then move on to audio workstations and video workstations.

Graphics Workstations

Professional photographers and graphic designers first and foremost need to have the clearest view possible of their images and image editing software. Whether you're editing photos in Adobe Photoshop or drafting mechanical

components in SolidWorks, you need to make sure you can see what you're working on! Because of this, the primary need for a graphics workstation is a large, high-quality monitor. A $200 LCD panel from Best Buy won't help you here—you need to make sure that the colors you see on the screen are as accurate as possible. Expensive monitors will have higher contrast ratios for more vibrant images and they'll also give you more control over the image they output.

You learned in Chapters 21 and 25 that monitors and video cards use different techniques to display colors. For a workstation to display colors accurately on a monitor, you must properly calibrate the monitor. This is a simple process of using a small sensor, like the tool shown in Figure 31.4, on the screen to create a **profile** that enables the monitor to display more accurate colors. You can use a similar device with a printer to create a profile for it, too. That way, your printouts will match what you see on the monitor.

• **Figure 31.4** A monitor calibrator

With a good enough monitor, almost any computer can be used as a graphics workstation, but ideally you'll want a fast, multicore 64-bit CPU and lots of RAM. If the processor is too slow or if the computer doesn't have enough RAM, it can take a long time to make changes to an image you're editing. A large hard drive is also a plus, since CAD files and photographs take up a lot of space. You'll also want to have an external drive to back up your work. If you're working with CAD/CAM software, you'll want a professional-level graphics card, such as an NVIDIA Quadro card (see Figure 31.5), though photo editing software won't see much of an advantage from such a card. Unlike typical graphics cards, these professional cards can cost thousands of dollars.

• **Figure 31.5** An NVIDIA Quadro graphics card (photo courtesy of NVIDIA)

• **Figure 31.6** Painting with a Wacom tablet

• **Figure 31.7** Audio interface device (photo courtesy of PreSonus)

Graphic designers frequently make use of specialized input devices, too, such as digitizer tablets. These tablets enable designers to paint on their computers as if they were painting on a canvas, as shown in Figure 31.6.

Digital Audio Workstations

The requirements for audio workstations are very similar to those for graphics workstations—a fast, multicore CPU, gobs of RAM, a large monitor, and a big, high-speed hard drive. The difference is that you'll also need a high-quality audio interface.

An **audio interface** is a box that you hook up to your PC with inputs that enable you to connect professional microphones and instruments (see Figure 31.7). Functionally, an audio interface is just a really high-end sound card, though they usually connect to your computer via USB or FireWire rather than plug into the motherboard. Audio interfaces range in size from an interface you can fit in your hand, to one that will take up most of your desk. A more expensive interface includes more inputs and produces higher-quality sound, though you'll also need some expensive speakers to hear the difference.

Just like with graphics workstations, audio workstations frequently make use of specialized input devices. These devices, referred to as *control surfaces*, mimic the look and feel of older, analog mixing consoles. They have a large number of programmable inputs that make controlling the software much faster and more accurate than with just a mouse and keyboard. These control surfaces range in size from small desktop units, all the way up to room-filling behemoths that are used in recording studios. Some of these boards also contain an audio interface.

Video Workstations

Video workstations combine the requirements of a graphics workstation and an audio workstation. Video editors often use two or more color-calibrated monitors so they can view the video stream they're working on with one monitor and see their video editor open on the other, making multiple monitors very useful. Video workstations require a very powerful CPU paired with as much RAM as possible, since video editing is a far more intensive process than graphics or audio editing. High-speed, high-capacity hard drives are also life-savers, since video files often take up multiple gigabytes

of space. Many video workstations have multiple hard drives set up in a RAID for added storage capacity and read/write speed.

Video workstations, like CAD/CAM workstations, benefit enormously from a professional-level graphics card. This is almost as important as the fast CPU and piles of RAM, and you'll rarely see a video workstation without one.

Because video workstations are frequently used as audio workstations, too, you will often find video workstations with the same audio interfaces and control surfaces as you'd see on an audio workstation. There are also video interfaces that enable editors to connect to various cameras. Additionally, many video editors use custom keyboards that have special labels and controls for popular video editing software.

Specialized Consumer PCs

Once you move away from the office and into the house, your computing needs change. Home is for leisure, and the workplace is for, well, work! The three common types of home systems are home servers that store everything from your music collection to last year's income tax return, home theater PCs to play your music and your movies, and gaming PCs to play powerful, video-intensive games.

Building a Home Server PC

How many computing devices are in your house right now? If you're like me, the answer is "a lot." Between multiple smartphones, iPods, tablets, portables, and desktop computers, you might shock yourself with the count.

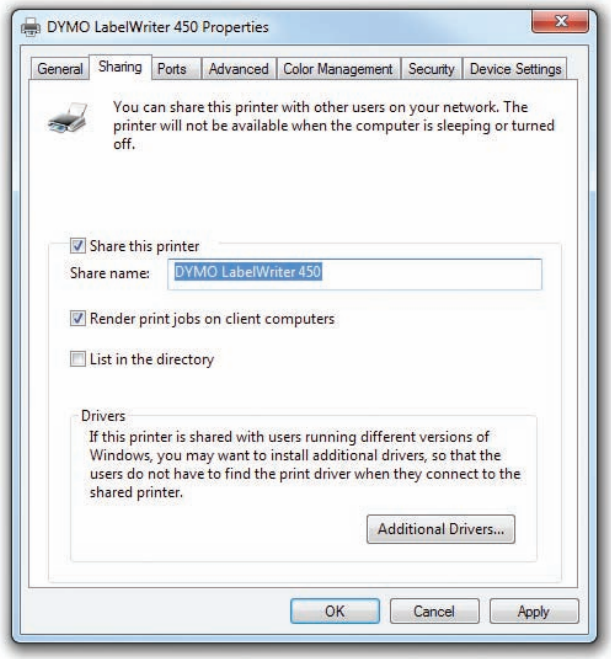
As more and more computing devices move into the home environment, there's a need for a centralized storage space, a **home server PC** to dish out files and folders on demand—a place for all your media to stream to multiple devices. This home server PC has very specialized needs that take it beyond the typical thick client.

A home server PC supplies three discrete functions: media streaming, file sharing, and print sharing. Media streaming often uses specialized software. Just like file and print sharing, though, it works fine through the default tools in Windows and Mac OS X. The home server PC has to have a very fast network connection and gobs of storage. Plus, that storage needs to be fault tolerant. Losing your video collection because of a hard drive crash would make for a very bad day.

Software

Any modern operating system enables you to share files and folders through standard sharing features. The same is true of sharing a printer. To turn that PC into a print server, open the Devices and Printers applet in the Control Panel, right-click on an installed printer, choose *Printer properties*, and then check the *Share this printer* checkbox on the Sharing tab (see Figure 31.8).

Microsoft makes a perfectly fine server OS called Windows Home Server that you can use to set up a sweet home server machine. You probably won't find the OS on the CompTIA A+ exams, however.



• **Figure 31.8** Sharing a printer

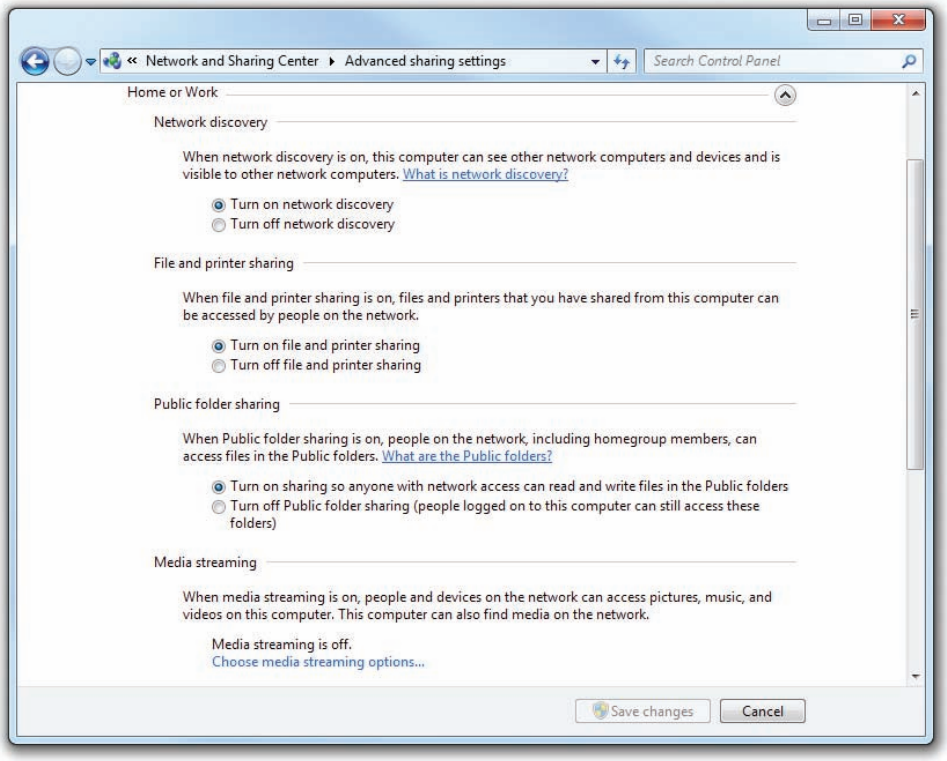
You can easily turn a Windows 7 PC into a media streaming server by selecting that option in the Control Panel. Open the Network and Sharing Center, select the *Change advanced sharing settings* link from the left Task menu, and then click the *Home or Work* option to get to the Advanced sharing settings screen (see Figure 31.9).

Halfway down the screen you'll find a link to *Choose media streaming options*. Click it. Figure 31.10 shows the Media streaming options screen. By default, Windows wants to share everything, though you can customize what's shared in case you have young children and don't want them to have access to inappropriate content.

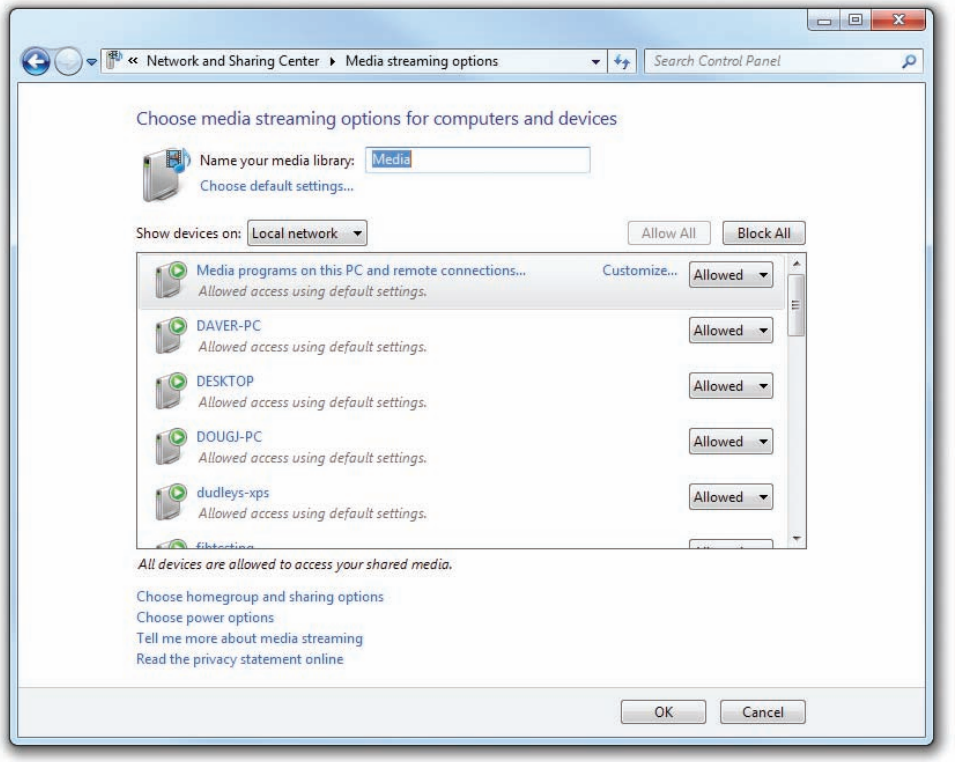
Finally, both Windows Media Player and iTunes have a feature to share media files on a local network. Figure 31.11 shows iTunes sharing via the Bonjour protocol.

Hardware

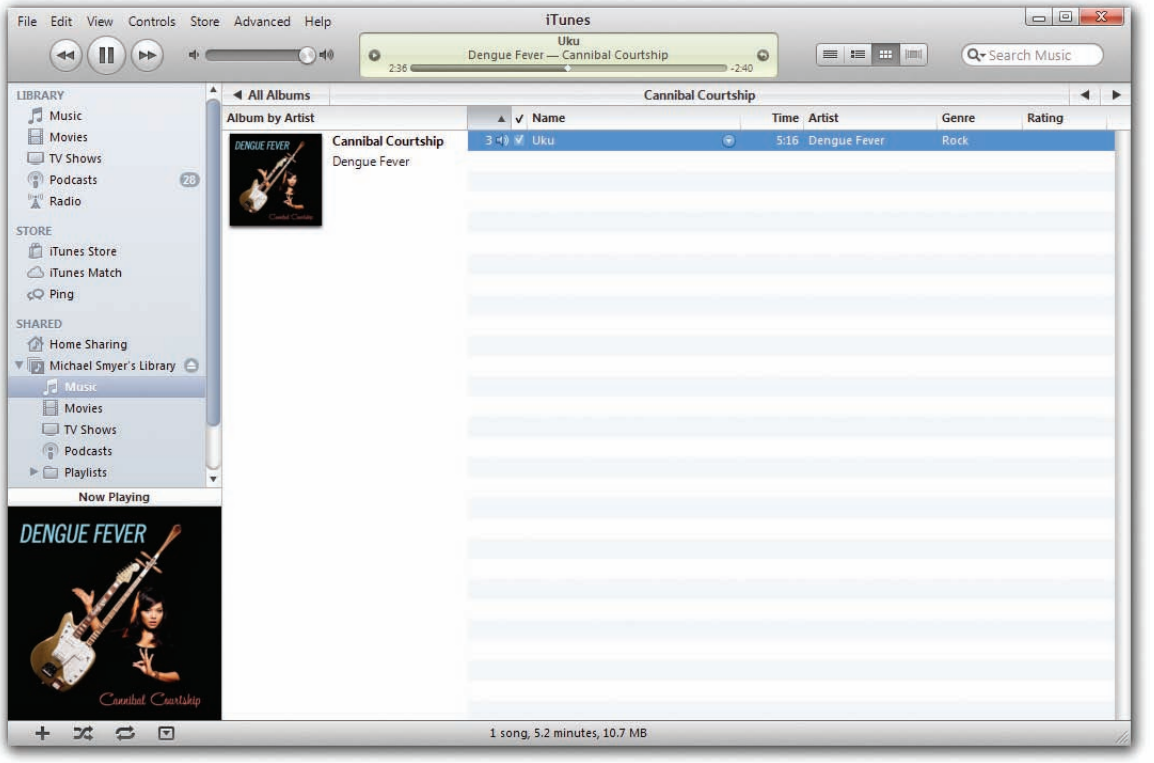
Hardware needs on a home server apply primarily to the network speed and hard drive capacity, at least according the CompTIA objectives. If you have a very active server, you should also pay attention to the amount of RAM it has and the speed of the CPU. Beefing both up above the standard thick client can help if you start getting some lag.



• **Figure 31.9** Advanced sharing settings



• **Figure 31.10** Media streaming options



• **Figure 31.11** Streaming with iTunes

You don't need to care at all about the video card in a server PC. Anything will do because you're not going to play anything directly on the server.

The CompTIA 801 objectives list "Ethernet" as a connection type for storage devices. While you won't find stand-alone external hard drives that support Ethernet connections, home servers and NAS devices can provide your PC with storage attached via Ethernet.

For the network, a wired Gigabit Ethernet NIC should be standard issue. Although it sounds cool to go wireless, you should limit the use of wireless to the single connection between the WAP and the client. The home server should connect via Ethernet to minimize any lag or dropped frames.

A file server's hard drives do the heavy and sustained lifting for the PC, so you should not stint on them. At a minimum, get two drives of identical size that have as much capacity as you can afford. No one *reduces* the amount of media in his or her collection over time, after all, especially if it's stored electronically. Plus, because you need fault tolerance on the data, you simply must use a RAID 1 configuration at a minimum (and thus the need to get two identical drives). If your budget can afford it and your motherboard supports it, get three identical drives and run in RAID 5.

Alternatives

Instead of building a custom home server box (the fun method), you can also purchase preconfigured devices that contain multiple hard drives and attach them to your network. Referred to as **network attached storage (NAS)**, these devices usually connect via Ethernet. Instead of connecting to the hard drive(s) on a server PC on the network, you connect to the NAS's hard drives. It plays the same role as a home server without all the fuss.

Cross Check

RAID Levels

You learned about RAID way back in Chapter 12, so check your memory now. Why use RAID 1 or RAID 5 for a server? Why not use RAID 0? How many drives do you need for RAID 0+1 or RAID 10?

Setting Up a Home Theater PC

You can certainly build a functional and very good home theater without the stereo receiver. My home theater doesn't use a stereo, for example, and isn't hooked up to a cable box either, yet it's great for watching movies and surfing the Internet.

A home theater system enables you to play music and watch movies and television. If done well, the experience can rival that of watching a movie at a fine movie house. When coupled with a home theater PC, the home theater system enables the full computing experience as well.

An optimal home theater has five components:

- A monitor, television, or projector
- Surround sound speakers
- A stereo receiver
- A home theater PC
- Network connectivity (such as a cable box or Ethernet)

This section looks at the specific components and issues involved with creating a home theater PC and connecting it to other components.

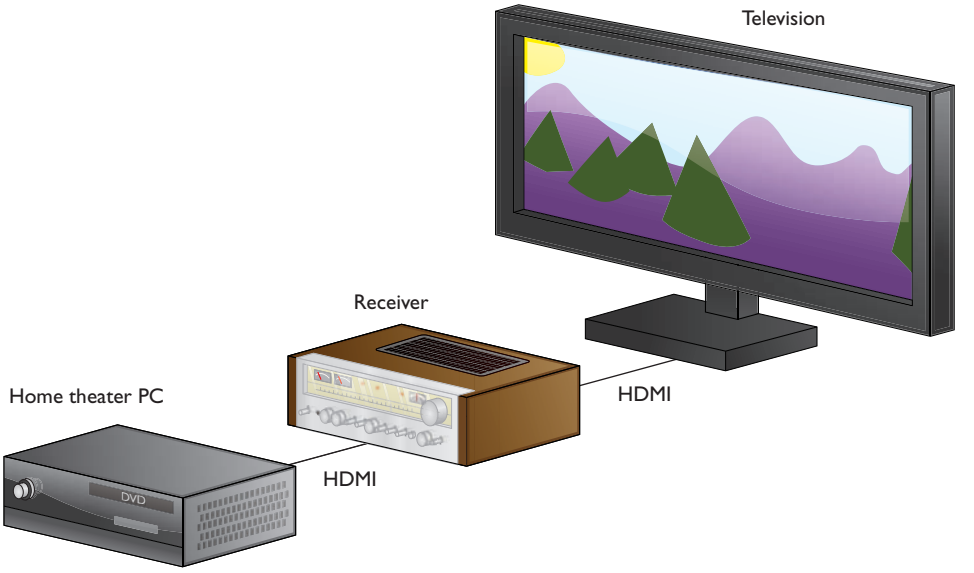
• **Figure 31.12** HDMI output on video card

Output Killer Video

A home theater PC must provide support for large monitors at high resolution, a requirement that usually involves an HDMI connector on the video card (see Figure 31.12). The HDMI cable connects the home theater box to the stereo receiver, which then pushes

the signal to the television. Figure 31.13 shows the basic home theater schematic.

Both DVI and DisplayPort can support 1080p HDTV resolution, as you'll recall from Chapter 21. Many televisions today have a DVI port, so this is a viable solution, especially if you don't have a stereo receiver (see the following section).

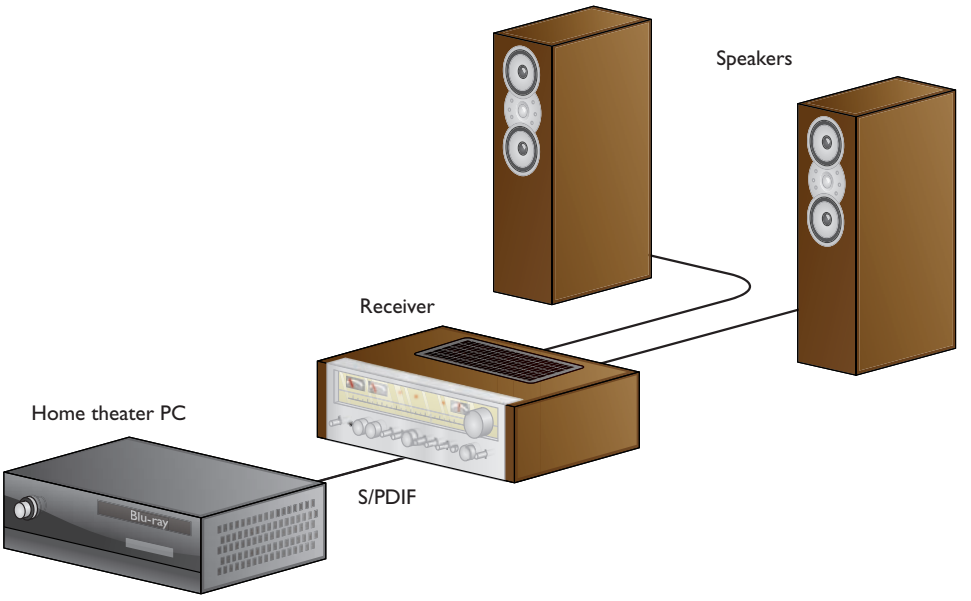


• **Figure 31.13** Television, receiver, home theater PC

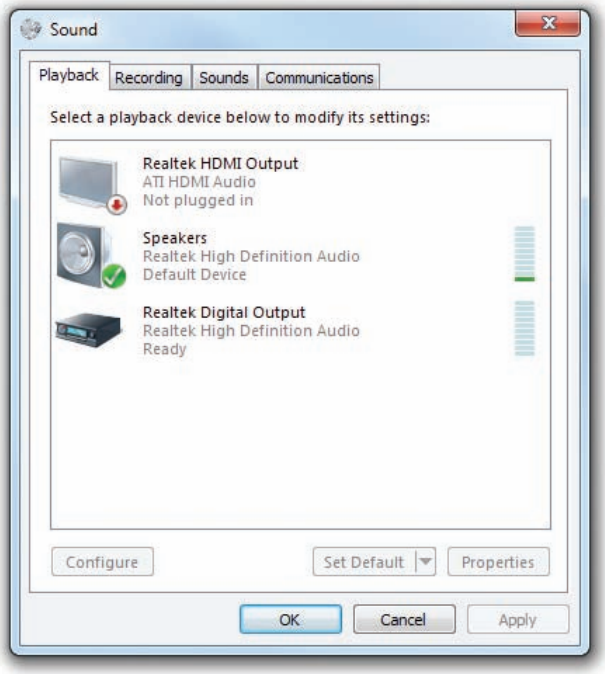
Play It Loudly

A great home theater system simply must have surround sound and a thumping subwoofer, so the home theater PC needs a sound card or built-in sound processor that supports 5.1 or 7.1 stereo. For the best output, the sound card connects to the stereo receiver via S/PDIF, through either the optical connector or coaxial connector. The speakers then connect to the receiver. Figure 31.14 shows the schematic with speakers added.

HDMI carries both the video signal and the surround sound audio signal, so if you plug it into the television directly from the PC, the rig will use the television's speakers by default. If you have the surround sound speakers plugged into the computer rather than a receiver, you need to go into the Sound applet in the Control Panel to select the playback device you prefer (see Figure 31.15).



• **Figure 31.14** PC, receiver, speakers



• **Figure 31.15** Sound applet for choosing playback device

Look Cool in the Process

Home theater components look like traditional stacking stereo components, such as a receiver, equalizer, DVD player, and so on. It simply won't do to put a beige office computer case alongside your sleek, black-clad components (see Figure 31.16).

You can get a case for a PC that stacks nicely with other home theater components (see Figure 31.17). CompTIA calls this style of case an **HTPC**, although that's not an industry-standard form factor. I assume the letters stand for *home theater PC*.

Access the Media—Streaming and TV

The home theater PC needs access to content, usually through Gigabit Ethernet to get streaming media through the home server PC you created in the previous section of the chapter. The home theater could use Wi-Fi (802.11n or better), though wired is best, especially for HD content.

The home theater PC wouldn't normally have anything to do with a signal from the cable company or from a dedicated optical disc player, like a Blu-ray Disc box. Those signals go from the applicable box to the stereo receiver directly.

• **Figure 31.16** This is not right!

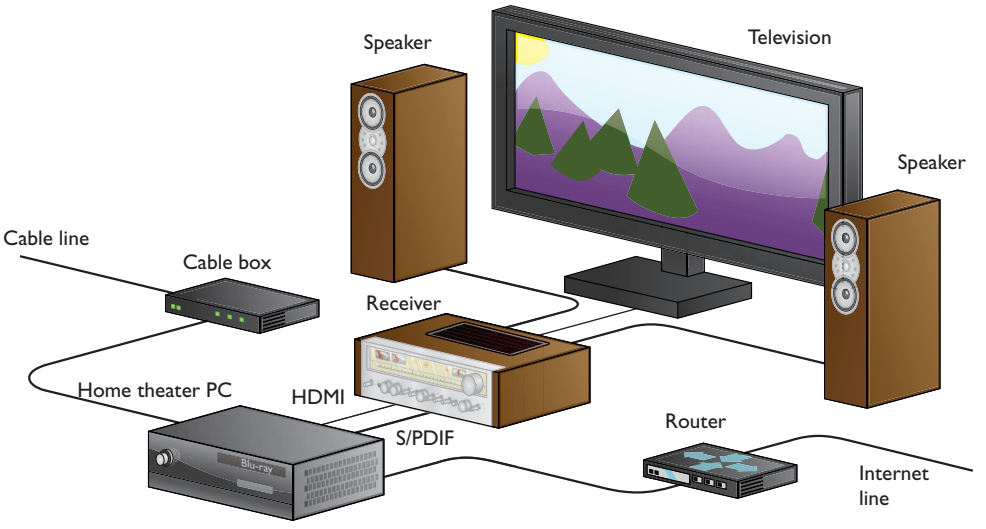
• **Figure 31.17** HTPC case

The only time the home theater PC should receive a television signal directly is through broadcast over the air. For this signal, the PC needs a television tuner, like you learned about in Chapter 25. You would use this to catch local news or sports programs.

Figure 31.18 shows the home theater schematic with all the media access methods included.

DLNA

Before we leave the hardware to look at software, I want to mention one topic that's outside the scope of the CompTIA A+ exams, but that you might run into in the field.



• **Figure 31.18** Final home theater

Digital Living Network Alliance (DLNA) certified devices connect to your home network, discover each other, and share media. In theory, DLNA devices should work with minimal setup or fuss, even if sourced from different manufacturers. If you share media files on a Windows PC, for example, a DLNA-equipped television, PlayStation 3, or other home theater device should be able to view those files. Look for the DLNA logo on devices as diverse as digital cameras, Blu-ray Disc players, network storage boxes, printers, and more.

Software Tools for Playback

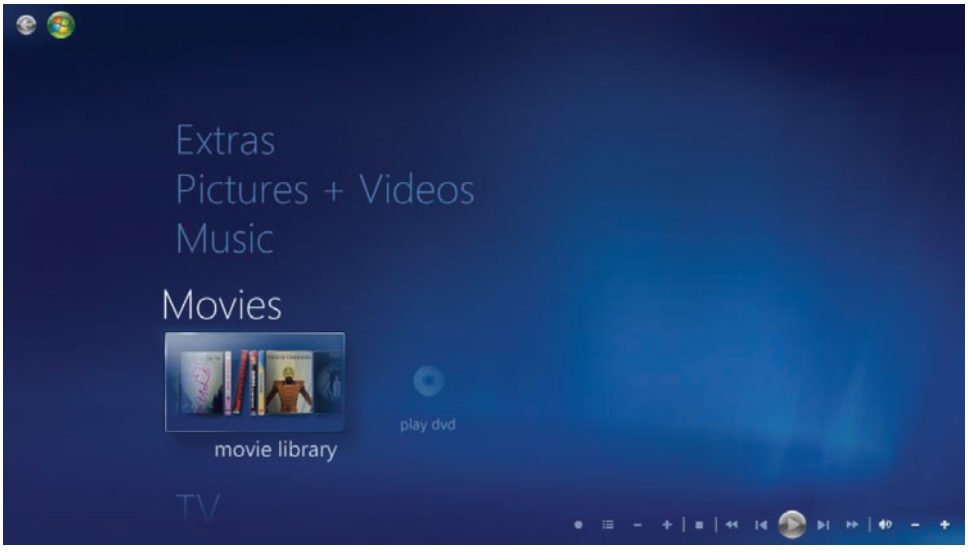
Once you have the media center hardware set up properly, you need software to access streaming media. Microsoft includes Windows Media Center in some editions of Windows. If you don't have one of those editions (see Table 31.1), then you need to use a third-party tool, such as the excellent XBMC or Plex.

Table 31.1 Versions of Windows That Include Media Center

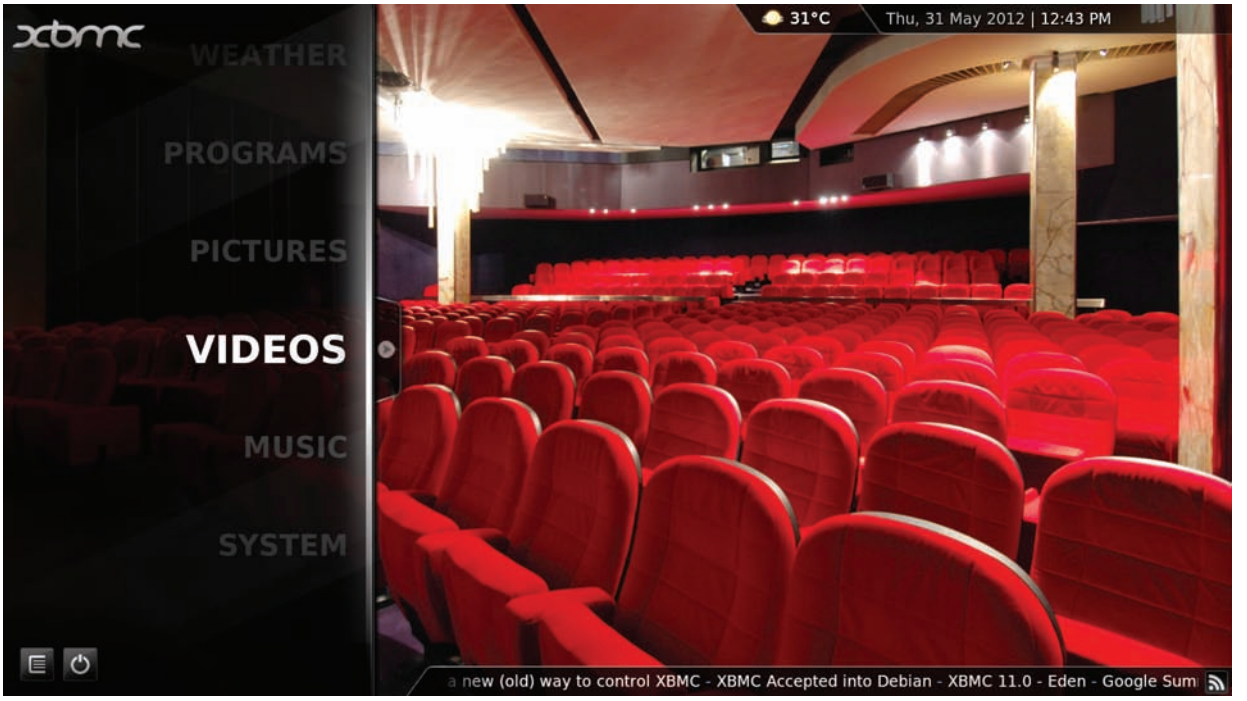
Windows XP	Windows Vista	Windows 7
Media Center	Home Premium	Home Premium
	Ultimate	Professional
		Ultimate

Windows Media Center enables you to stream content from a home server and watch content stored locally. You can even access some television shows broadcast over the Internet (see Figure 31.19). Most of the setup happens via wizards that run when you select an option. If you want to add content from networked computers, you'll need to add it to the appropriate library (in Windows 7) or connect to the shared folder(s) in Windows XP or Windows Vista.

As cool as Windows Media Center is, you can find absolutely beautiful and functional third-party software for free, such as XBMC and Plex. XBMC in particular enables you to customize the look and feel of the interface, and many people have made awesome skins available too. Figure 31.20 shows the default skin for XBMC; Figure 31.21 shows the same content but displayed with a completely different skin. Plex is not flashy, but it's totally functional. There are versions of XBMC and Plex available for Windows, Mac OS X, and Linux. You can download XBMC from xbmc.org. Get Plex at www.plexapp.com.



• **Figure 31.19** Windows Media Center



• **Figure 31.20** Default XBMC

• **Figure 31.21** XBMC sporting the Aeon skin

Gaming PC

And now for the grand finale, the PC you've been waiting for, the system you've always wanted to build. As an aspiring PC tech, you probably took your first apprehensive steps into the dark underbelly of PCs with a game: *Doom*, *Quake*, *Myst*, *The Sims*, *World of Warcraft* . . . you've played at least one of them. While casual gamers can get by with a standard desktop PC (like the thick client you read about earlier), those who take their gaming seriously want a powerful PC ready to pump out the latest graphics. A gamer goes through a game's graphics settings and sets everything to the max. And since games aren't all about how good they look, you'll also want a good sound card and headphones. (Okay—you also need a good game, but one thing at a time.)

First, I'm going to tell you about the optimal gaming PC—the best bang-for-your-buck gaming PC that will play every game out there without breaking your wallet. (It's cheaper than you think! You can get a lot for about $1000.) Then I'll show you how you can take PC gaming from a hobby to a lifestyle—your only lifestyle—with beyond-bleeding-edge components that you don't need but should buy anyway.

A Gaming PC That Won't Break Your Wallet

A gaming PC isn't that different from your run-of-the-mill thick client: all of the components are the same, but taken to the next level. The Windows recommended system requirements no longer cut it. Instead, you might turn your attention to the system requirements in a favorite PC game. Find a game that came out in the last year or two and see what it needs from your PC. You'll find that most games actually have pretty low system requirements.

A lot of modern PC games are *ports* or copies of console games (originally created for the Xbox 360 or PlayStation 3, for example). Because the consoles were launched so long ago—before Windows Vista!—their old hardware makes it easy for modern PCs to run ported games. Games designed specifically for PCs, however, can take advantage of every core and gigabyte you give them. Take a PC game's system requirements and bump them up a notch or two to keep your gaming PC future-proof. **Future-proofing** means building a PC in a way that keeps it relevant for a few years. You don't want your PC to be out of date a week after you build it. Going beyond the current requirements for a game will make it ready for new games that come out a year or two from now.

The Internals Most of the big improvements over a standard thick client will happen inside the case. Every game is coded differently—just like any other application—so each game will take advantage of your hardware to varying degrees. Some games, for example, are designed to use quad-core CPUs and others are not. If a game can only use one core, those three other cores in a quad-core CPU can't play along. But you want a quad-core CPU anyway. Why? Future-proofing and price. Why limit yourself now when more and more games can take advantage of multiple cores? And these days, the price is right. Find a quad-core Intel processor with a speed of 3 GHz or more. If you have a tighter budget, get the AMD equivalent.

Make sure you get a motherboard and CPU that are compatible with one another. I'll talk more about gaming motherboards later in this section.

For a budget-minded gaming PC, the processor is the first place you want to splurge a little bit. You don't need a special case or motherboard.

You don't need more than 4 GB of RAM, and you only need enough hard drive space to store all your games. You don't need an extra monitor. Powering games revolves around two elements, so you'll spend the most money on these parts. I already told you about CPUs, so now let's talk about the biggest-ticket item, the graphics card.

A powerful graphics card (combined with a quality CPU) enables you to do two things: turn up the graphics quality and increase the performance (see Figure 31.22). The graphics-quality of the game depends as much on the graphics card as it does on the designers of the game. A good graphics card can't make an ugly game look pretty, but it can make a pretty game look gorgeous. At higher settings, all sorts of smoothing and filtering happens that would make weaker systems choke. At the same time, you also want to maximize performance. In games, we measure performance by the number of frames per second (FPS) displayed. Most games are designed to run at about 30 FPS, though the sky's the limit on the top end. If you're getting fewer than 20 FPS (everything will look very choppy and it will be difficult to play the game), you'll probably need to turn down the graphics settings in the game, and no one wants to do that!

• **Figure 31.22** An NVIDIA 680 graphics card (photo courtesy of NVIDIA)

So what should you look for in a graphics card? This can be a very "you get what you pay for" proposition, but NVIDIA and AMD—the two dominant graphics processing unit (GPU) manufacturers—have helpfully divided their products by number to show you at a glance how powerful they are. Yes, there are buses, cores, shaders, bandwidths, and so on, but it's all encapsulated into a (slightly random) number. The NVIDIA and AMD numbering systems, however, are entirely different, a little confusing, and sometimes loop back around to the beginning. I owned an NVIDIA GeForce4 MX 460 back in 2002. This is, of course, not the same as the NVIDIA GeForce GTX 460 released in 2010. And the NVIDIA GeForce GTX 460 is more powerful than an AMD Radeon 4850, even though AMD's number is bigger. Use each GPU manufacturer's Web site to learn about the latest available graphics processors. When it comes time to buy, look for the third- or fourth-best card available in the latest generation's lineup. If the best card available is the "690," look for the "650" or "670" model. You can usually save hundreds of dollars and still get the best graphics and performance with modern games.

Graphics card model numbers are organized by generations. As of 2012, NVIDIA cards were divided between the 500 and 600 generations, while AMD cards used the 6000 and 7000 series. Within each generation, a lower number means less power (and lower price), while a higher number means more power (and a higher price). The top NVIDIA card, for example, might be the 690 model, while the low-end model would use the 620 name. For the latest model information, check out the NVIDIA and AMD Web sites.

While the CPU and GPU will satisfy your eyes, don't forget about your ears. More and more games can take advantage of high-end sound cards that produce true surround sound rivaling blockbuster movies. Hear the squeal of your tires, the noise of your jet engine, and the fiery power of a wizard's spell in 5.1 surround sound! You'll need to spend a bit of money (almost as much as that graphics card you just found) to hear the difference, but if you're an audio geek, it's worth it. Look for sound cards that support extra channels (7.1), more bits (24-bit), and higher sample rates (192 KHz).

All of this power inside your case means it needs to handle a lot of extra heat. A more powerful CPU and GPU will put out more heat, and you'll need a cooling system that can handle it (see Figure 31.23). For a budget setup, you don't need to jump straight to liquid cooling (though it's always an option). Most cases have a few extra spots for fans that you can buy

The key components of a great gaming PC include: a high-end processor, a powerful video card, a good sound card, and enough cooling (fans, heat sinks, liquid cooling) to keep all those parts from melting your machine.

• **Figure 31.23** Powerful CPU fan and heat sink

Like keyboards and mice, cases are a very personal choice. Some people like wild colors. Other people want lights and windows showing off their internal devices. Personally, I prefer a plain black case. No lights. No windows. No distractions.

separately. Get some 120-mm fans and go to town. Your case cannot be too cool (and neither can you).

The Externals For a budget gaming PC, there's not much to improve outside of your case. One monitor will work fine, but make sure it has a resolution of at least 1920 × 1080 and is 24 inches diagonally. That will enable you to easily watch 1080p HD video content and play console ports at or above their intended resolution. Likewise, a basic 2.1 or 5.1 speaker setup will work just fine with your nice sound card. Don't use cheap headphones, though. Invest in something nice (with a microphone, if you like to voice chat while gaming) that is comfortable and produces sounds that aren't tinny or hollow (see Figure 31.24).

• **Figure 31.24** Sennheiser HD 598

Many gamers like to buy fancy keyboards and mice, covered in extra buttons that can be customized to launch your wizard's fireball with a single click. Some keyboards even add little LCD screens that show you exactly how your keys have been customized and enable you to adjust your custom keyboard layout on the fly (see Figure 31.25). Keyboards and

mice are very personal—get whatever best helps you game.

• **Figure 31.25** A nice keyboard with built-in LCD screen

A Gaming PC That Will Set Your Wallet on Fire

If money is no object, go buy a yacht, and on that yacht, set up your dream gaming PC. Here, no price is too high, no technology too frivolous, and no monitor too big. If it exists, you should have it, even if you'll never use it. Some of this will sound extreme, and that's the point. I'll point out the best places to spend too much money and transform your budget box into the ultimate gaming PC.

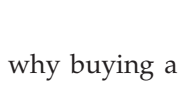
The Internals With the budget box, I told you why buying a quad-core processor was a good investment for future games that will take advantage of the technology. Now, quad-core isn't nearly enough. As of 2012, six-core processors like the Intel Core i7 Extreme Edition sit at the top of the CPU heap and will future-proof your PC for years to come. No game needs it, but at $1000, you can't afford not to get it.

If that wasn't extreme enough, get ready for your graphics card purchase, or should I say graphics *cards*? That's right: you'll need more than one high-end graphics card if you want the best of the best PC gaming experience. (And forget about not getting the very best card available—just look for the highest model number available and hand over your credit card.)

NVIDIA and AMD have both developed their own technology for linking multiple graphics cards. NVIDIA calls their technology **Scalable Link Interface (SLI)**, while AMD calls theirs **CrossFire**. Using a special cable (that looks sort of like a ribbon cable), the graphics cards can combine their power to increase graphical quality and performance (see Figure 31.26). With either technology, you can link up to four video cards together for more power than any current PC game could use. (But that's not the point.) Gamers will argue how effective these multicard setups really are—in fact, some games are so poorly optimized that they will run worse with more than one graphics cards. Read up on how each game you play works with multiple graphics cards and proceed accordingly.

While you're at it, you might as well get a bunch of extra RAM (16 GB sounds comfy). A solid-state drive (or two) will help load game levels into RAM that much faster. When you need a break from gaming, a Blu-ray Disc optical drive enables you to watch HD movies. Add to that a 7.1 sound card and Gigabit networking card for high-speed connections to other gamers, and you have the start of an unmatched gaming-performance machine.

The Externals If you have multiple video cards, why not buy multiple monitors? You learned about multiple monitor setups when you read about audio/video workstations earlier in this chapter, and many games can take



Installing multiple graphics cards requires a motherboard that can handle two or more PCIe cards, a power supply that produces enough wattage, a case it will all fit in, and a cooling system powerful enough to keep your PC from overheating (a liquid-cooling setup sounds nice right about now). Keep these things in mind when upgrading or building your PC.

• **Figure 31.26** An SLI cable

For the ultimate graphics card/monitor combination, NVIDIA supports four graphics cards connected together via SLI, attached to three side-by-side 3-D monitors. I've never seen it in person, but I imagine it's as close as you can get to standing inside a video game world. (AMD CrossFireX also supports multiple video cards, but not connected to three monitors.)

If you skipped the other custom PC sections because this is the coolest kind of PC to build, don't forget to go back and read anything you missed. Who knows? You might decide to become a filmmaker instead of play games all day. (Yeah, right!)

advantage of this feature. Picture, if you will, three monitors, side by side: the nose of your race car speeds down the track on the center monitor while the crowd whips by on the left and right monitors. With multiple monitors, your field of view doubles, triples, or more!

Instead of expanding your view left and right, you can also improve your display forward and backward with 3-D technology. More and more PC games are including support for 3-D displays. You'll need the slightly silly glasses to make it work, but for gaming, the effect is amazing. Lots of action games require a good sense of (virtual) depth perception to play. You can't hit the enemy warlock with your fireball if you can't aim it properly. With 3-D displays, distant enemies will *look and feel* distant. Everything becomes much more natural with 3-D technology. To use it, you'll need a display and video card that supports the technology.

For sound, why stop at puny PC speakers? Jump to big home theater surround sound speakers (see Figure 31.27). Get a gamepad, too (for the PC games that support it). While you're at it, buy a nice chair with good back support and padding. When you game for hours on end in a good chair, your neck, back, and bottom will thank you.

That's it! Who knew it was so easy to spend $10,000 on a gaming PC? While most gamers will stick with something closer to the budget box, keep in mind that there is so much more power available—more than most games can handle. Whether you spend $100, $1000, or $10,000, don't forget to look for what *you* want out of your gaming PC. What games do you play? What do they require? What do you want? When you answer those questions, finding the parts you need becomes easy. Finding the right game, however, is an entirely different challenge.

• **Figure 31.27** 5.1 surround sound speakers (photo courtesy of Klipsch Group, Inc.)

Chapter 31 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about building your own PC.

Research and build a standard thick client

- Before you build your first PC, you need to do some research on the parts you are going to use. Read reviews online, written by both industry experts and users. Learn everything you can about the part. Check with the manufacturer and retailer for warranties and return policies. Compare the device you like with others that are available—which is better? Visit a local brick-and-mortar store so you can play with the parts and see them in person.
- Thick clients are general-purpose devices. They don't use the best components or the worst components. Thick clients should be able to handle the majority of home and office tasks.
- Start your search for thick client components by reading the Windows recommended system requirements. Then forget about those and make sure your thick client has at least a 2-GHz, dual-core CPU, 4 GB of RAM, a hard drive with 500-GB capacity, and a DirectX 11 video card. Use a mid-tower case to ensure you have room for expansion later.
- Pick the CPU and motherboard first. Make sure you use a current socket that you can use with newer CPUs a few years down the road. Find a middle-of-the-road processor from either AMD or Intel. Make sure the motherboard you pick supports the same features as the CPU. The motherboard should have plenty of expansion slots so you can add more components to your thick client later.
- Depending on your needs, you can either use the onboard video device built into your motherboard or add a dedicated PCIe video card. Avoid noisy video cards. You should find a 20-inch widescreen monitor with an LED backlight.
- Get a hard drive with a capacity of 1 TB. You probably don't need a RAID array, but make sure you can make backups.
- Download a Web browser or two and some office-suite applications like Microsoft Office.

Customize a professional PC

- A thin client is similar to a thick client, except it is designed with the most limited of hardware in mind. These devices usually have a single purpose, such as operating as a point-of-sale device.
- Virtualization workstations enable a user to install a second virtual machine onto their local system. You can run an entirely separate OS inside your original OS. For good performance, you'll need lots of RAM and a powerful 64-bit CPU.
- Photographers and graphic designers need high-performance monitors so they can properly and accurately see their work. Monitors should be calibrated to display the correct colors. You'll want a 64-bit CPU and lots of RAM. If you work with CAD/CAM applications, you may want to add a professional-level graphics card, such as one of the NVIDIA Quadro cards. Graphic designers also often use digitizer tablets to draw directly into the computer.
- Audio workstations have similar requirements to graphics workstations: lots of RAM and a fast, multicore CPU. You'll want a large monitor for more workspace and big hard drives to store all of your files. Audio professionals also need an audio interface box that enables them to connect microphones and other instruments. Audio workstations can include control surfaces, which mimic the look and feel of analog mixing consoles.
- A video workstation combines the requirements of an audio and graphics workstation. Video professionals need multiple color-calibrated monitors to view their work. The workstation needs a powerful CPU paired with as much RAM as possible. High-speed, high-capacity hard drives will enable you to store more video files. A professional-level graphics card will also help the video software run more smoothly. Like audio and graphics workstations, special control surfaces are available for video editing. You can also purchase custom keyboards with special labeling that matches the controls for popular video editing software.

Build a specialized consumer PC

- With so many computing devices floating around your home, having a central storage space can make accessing your files and media a lot easier. Home server PCs supply media streaming, file sharing, and print sharing. Media streaming can use special software, though Windows has built-in sharing capabilities.
- The home server PC should have a fast network connection and gobs of storage. The storage should also be fault tolerant in a RAID array. If you have a more active server, pay attention to the amount of RAM and speed of your CPU.
- Instead of building a custom home server PC, you can also use a network attached storage (NAS) device that replicates many of the duties of a home server PC in a prebuilt box. The NAS attaches to your network via Ethernet and serves files stored on its hard drives.
- A home theater should include a display, surround sound speakers, stereo receiver, home theater PC, and network connectivity.
- Most home theater setups use HDMI to send audio and video between devices. If you are connecting directly from your home theater PC to your TV or other display, you can also use DVI or DisplayPort.
- Your sound setup should include 5.1 or 7.1 surround sound speakers, connected to a receiver. The receiver controls the speakers, unless you plug the speakers directly into the PC.
- To match the rest of your home theater components, make sure your home theater PC uses an HTPC form factor.
- Home theater PCs receive content over Gigabit Ethernet, perhaps streamed from a home server PC. Wired connections are best for streaming HD content.
- DLNA enables you to easily share media on your computer with devices that support the standard. Using a DLNA device, you can browse the shared drives and folders on your PC and play back various media formats.
- To access your media on your home theater PC, you can either use the Windows Media Center or download third-party applications such as XMBC and Plex.
- A gaming PC isn't that different from a standard thick client. The components are the same, but taken to the next level. Upgrade to a quad-core processor with a speed of at least 3 GHz. You should find the latest generation of video cards and find a model one or two steps below the most powerful version. Use NVIDIA's and AMD's model numbers to help you sort out which cards are high-end and which cards are low-end. The video card and CPU will be where you spend the most money on your gaming PC.
- The power of the graphics card determines how high you can push the game's graphic details and how well it will perform. The performance of a PC game is measured in frames per second (FPS).
- Make sure you have at least 4 GB of RAM. You need enough hard drive space to hold your PC games.
- To improve the sound quality, purchase a dedicated sound card. If you are an audiophile, you'll definitely hear the difference.
- Because of all these advanced components, you'll need to upgrade your cooling setup. You'll need a large CPU fan and heat sink. You can also consider water-cooling your system.
- Get a nice 24-inch monitor with a resolution of at least 1920 × 1080. A basic 2.1 or 5.1 speaker setup should also suffice for most games. Optionally, you can get a nice set of headphones with an attached microphone for voice chatting with your friends while you game.
- Gaming keyboards and mice are available that include extra buttons and fancy LCD screens. These components are entirely a personal choice.
- Advanced (and expensive) gaming machines can use advanced technology to increase the performance and visual fidelity. These include connecting multiple graphics cards via SLI and CrossFire, connecting multiple monitors, and purchasing 3-D monitors.
- Other components can be upgraded, too: you can upgrade your CPU to more than four cores, quadruple your RAM, and add solid-state drives. You can also get better speakers and gamepads and joysticks.

Key Terms

audio interface *(1178)*
CrossFire *(1191)*
Digital Living Network Alliance (DLNA) *(1186)*
future-proofing *(1188)*
home server PC *(1179)*
HTPC *(1184)*
network attached storage (NAS) *(1182)*
profile *(1177)*
Scalable Link Interface (SLI) *(1191)*
thick client *(1173)*
thin client *(1176)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. You can store files remotely without a home server by using a(n) _____ device.
2. A(n) _____ is a system designed to handle only very basic applications with an absolute minimum amount of hardware required by the operating system.
3. A(n) _____ is a box that you hook up to your PC with inputs that enable you to connect professional microphones and instruments.
4. CompTIA calls a general-purpose SOHO computer a(n) _____.
5. _____ cases are used to make your computer blend in with the rest of your home theater equipment.
6. Overbuilding your gaming PC to handle games that aren't out yet is called _____.
7. Connecting multiple graphics cards in your PC uses _____ technology if you're using NVIDIA cards and CrossFire technology if you're using AMD cards.
8. _____ certified devices connect to your home network, discover each other, and communicate over the Internet.
9. To ensure that the color output matches between your monitor and your printer, you can use a calibration device to create a(n) _____ both for your monitor and for your printer.
10. If you want to share files and printers over your home network, you can set up a(n) _____.

Multiple-Choice Quiz

1. What is a thin client?
   - **A.** A computer with a 32-bit-wide address bus
   - **B.** A portable computer
   - **C.** A system designed to handle only very basic applications with the minimum hardware required by the operating system
   - **D.** A computer in a narrow, small form-factor case
2. What three functions does a home server PC provide? (Select three.)
   - **A.** Media streaming
   - **B.** File sharing
   - **C.** Web hosting
   - **D.** Print sharing
3. What's a good guide to use when deciding on hardware for a basic thick client?
   - **A.** Buy whatever is on sale.
   - **B.** Always start with the most expensive hardware.
   - **C.** Check the recommended requirements for the OS you want to use.
   - **D.** Check the MSDS for the OS you want to use.
4. How can you make sure that your printouts match the colors displayed on your monitor?
   - **A.** Calibrate your GPU with a GPU calibrator.
   - **B.** Calibrate your monitor and printer to use the same profile.

C. Just buy an expensive monitor and printer; no setup is needed.

D. Use RGB ink in your LaserJet printer.

5. How do you share a printer in Windows 7?

A. Open Device Manager, right-click on the printer, select Properties, and select Share this printer.

B. You have to install special drivers for your printer.

C. Open the Devices and Printers applet in the Control Panel, right-click on the printer, select Printer properties, and then check the Share this printer checkbox on the Sharing tab.

D. You have to have Windows Home Server in order to share printers.

6. What program that comes with some versions of Windows turns your PC into a home theater PC?

A. XBMC

B. Windows Media Center

C. Plex

D. Windows Home Theater

7. What term defines building your PC to run games that aren't out yet?

A. Future-proofing

B. Next-gen proofing

C. Overbuilding

D. Prebuilding

8. What does CompTIA call a PC case built for a home theater?

A. Media center case

B. XBMC

C. HTPC

D. Stereo case

9. Bob wants to build a new gaming computer, but he doesn't want to spend a ton of money. What parts should he spend the most money on? (Select two.)

A. CPU

B. Case

C. Power supply

D. Graphics card

10. What is the most important component for building a virtualization workstation?

A. CPU

B. Power supply

C. RAM

D. Large monitor

11. What are the high-end sound output devices on audio workstations called?

A. Sound cards

B. Audio interfaces

C. Consoles

D. Calibrators

12. What three things does a video workstation benefit from? (Select three.)

A. High-end motherboard

B. Fast, multicore CPU

C. Lots of RAM

D. Professional-level GPU

13. What device can store your files remotely if you don't want to build a home server PC?

A. NAS

B. WAP

C. PCI

D. NIC

14. Your friend Susan just won the lottery! After spending a few weeks buying mansions and European sports cars, she decides that what she wants most out of her limitless fortune is to be able to play computer games all day. Not knowing anything about building PCs, she comes to you for help building the Ultimate Gaming Rig. What features would help Susan get the absolute most performance out of her games? (Select three.)

A. A quad-SLI or quad-CrossFire graphics card setup

B. A top-of-the-line CPU

C. One or more SSDs

D. A case with a window on the side

15. Which of the following editions of Windows comes with Windows Media Center?
    - **A.** Windows 7 Home Premium
    - **B.** Windows XP Professional
    - **C.** Windows Vista Home Basic
    - **D.** Windows Vista Business

Essay Quiz

1. Write an essay describing your ideal PC. If you're into music, write about an audio workstation; if you're into games, write about a gaming PC; and so on. What components are important to the type of PC you want to build? Is there anything you want on your PC that's not covered in this chapter? Do you need your PC to do more than one thing?
2. Write about your personal process for researching and purchasing PC components. Which Web sites do you visit? Do you read PC magazines? How do you comparison shop? Are there any local stores that you visit?

Lab Projects

• Lab Project 31.1

Pretend you've been saving money to build yourself a gaming PC. You've managed to scrape together $1000, and it's burning a hole in your pocket. Go on the Internet and shop for components to put together the best home theater PC you can within your budget. Remember to research any components before deciding on which to purchase, and definitely don't forget to include shipping costs in your budget. Write down in a spreadsheet each component, its price, and your reasons for purchasing it.

• Lab Project 31.2

Using your classroom PCs, download and install XBMC from www.xbmc.org. Using the resources available on the XBMC Web site, configure your copy of XBMC with custom skins and background images. Set up XBMC to play a DVD or CD when you put one in your optical drive. If you have a smartphone and you're allowed to use it in class, download and install a free XBMC remote app and set it up to control XBMC on your PC. Look through the available add-ons and try installing any that sound interesting to you. When you're finished customizing, write a short summary of what you did and how you did it.

• Lab Project 31.3

Turn one of your classroom PCs into a home server PC by setting up file and printer sharing. If you've got a printer available, plug it into the server PC and share it with the other PCs in the classroom. Download a video file of some sort (you can download a free, open source, 3-D short film at www.sintel.org/download) and stream it from the server PC to other classroom PCs. When you're finished, write a short guide to sharing media and printers in Windows.