PC Maintenance and Troubleshooting Strategies

In this chapter, you will learn:

- About operational procedures to keep you, other people, the equipment, and the environment safe
- How to develop a preventive maintenance plan and what to include in it
- How to approach and solve a PC problem

In the last several chapters, you have learned much about the hardware components of a system, including features and characteristics of the power supply, motherboard, processor, RAM, hard drive, I/O devices, and multimedia devices. You've learned how to select, install, and configure each device. And you've also learned steps you can take to troubleshoot problems with these devices. In this chapter, you can take a step back from all the details of supporting hardware devices and think about strategy. When supporting personal computers and their users, having a strategy in mind when faced with day-to-day tasks and challenges can make all the difference between feeling overwhelmed and feeling in charge. A strategy gives you direction, purpose, and a plan. This chapter is about having a plan so you know where you're going and you have a strategy to get there.

Staying safe and protecting equipment are essential to your strategy as a professional support technician. And the best support technicians are good at preventing a problem from happening in the first place, so in this chapter, you'll learn how to develop a preventive maintenance plan and use it. Finally in this chapter, you'll learn a strategy to solve any computer problems. You can apply this strategy to all the troubleshooting skills you've learned so far in this book. You can then build on this strategy in future troubleshooting situations to become an expert problem solver, confident that you can face any computer problem.

> 💡 **A+ Exam Tip** This chapter has three major sections. All the sections cover objectives on the A+ 220–701 Essentials exam that apply to operational procedures, preventive maintenance techniques, and troubleshooting theory.

OPERATIONAL PROCEDURES WHEN SUPPORTING PERSONAL COMPUTERS

A+
220-701
6.1

In this part of the chapter, you'll learn about the physical dangers of supporting personal computers and how to protect yourself and others. Then you'll learn about what can happen to damage a computer or other equipment while you are working on it and what to do to prevent that damage. You'll also learn how to dispose of used equipment and move computer equipment. And finally, you'll learn about the software copyright law that you need to be aware of when installing and supporting software.

STAY SAFE AND KEEP OTHERS SAFE

Recall from Chapter 4 that you need to immediately unplug electrical equipment that has been damaged physically or exposed to water, moisture, or electrical shorts. In addition, some printer components such as the drum on a laser printer will get so hot they will burn you. Other dangers to watch out for are chemical burns, cables that can cause people to trip, and heavy equipment that can hurt your back. You also need to be careful when working with computer cases because some have sharp edges that can cut you.

Now let's look at safety precautions to take when using cleaning pads and solutions, managing cables that might be trip hazards, and lifting heavy objects.

PROPER USE OF CLEANING PADS AND SOLUTIONS

As a PC technician, you'll find yourself collecting different cleaning solutions and cleaning pads to clean a variety of devices, including the mouse and keyboard, CDs, DVDs, Blu-ray discs and their drives, tapes and tape drives, and CRT and LCD monitors. Figure 11-1

Figure 11-1   Cleaning solutions and pads
Courtesy: Course Technology/Cengage Learning

shows a few of these products. The contact cleaner in the figure is used to clean the contacts on expansion cards, which might solve a problem with a faulty connection.

Most of these cleaning solutions contain flammable and poisonous materials. Take care when using them so that they don't get on your skin or in your eyes. To find out what to do if you are accidentally exposed to a dangerous solution, look on the instructions printed on the can or check out the material safety data sheet (see Figure 11-2). A **Material Safety Data Sheet (MSDS)** explains how to properly handle substances such as chemical solvents.

Figure 11-2 Each chemical you use should have available a material safety data sheet
Courtesy: Course Technology/Cengage Learning

An MSDS includes information such as physical data, toxicity, health effects, first aid, storage, shipping, disposal, and spill procedures. It comes packaged with the chemical, you can order one from the manufacturer, or you can find one on the Internet (see *www.ilpi.com/msds*).

If you have an accident with these or other dangerous products, your company or organization might require you to report the accident to your company and/or fill out an accident report. Check with your organization to find out how to handle reporting these types of incidents.

MANAGING CABLES

People can trip over cables or cords left on the floor, so be careful that cables are in a safe place. If you must run a cable across a path or where someone sits, use a cable or cord cover that can be nailed or screwed to the floor. Don't leave loose cables or cords in a traffic area where people can trip over them (called a **trip hazard**).

LIFTING HEAVY OBJECTS

Back injury, caused by lifting heavy objects, is one of the most common injuries that happen at work. Whenever possible, put heavy objects, such as a large laser printer, on a cart to

move them. If you do need to lift a heavy object, follow these guidelines to keep from injuring your back:

1. Looking at the object, decide which side of the object to face so that the load is the most balanced.

2. Stand close to the object with your feet apart.

3. Keeping your back straight, bend your knees and grip the load.

4. Lift with your legs, arms, and shoulders, and not with your back or stomach.

5. Keep the load close to your body and avoid twisting your body while you're holding it.

6. To put the object down, keep your back as straight as you can and lower the object by bending your knees.

Don't try to lift an object that is too heavy for you. Don't be afraid to ask for help.

PHYSICALLY PROTECT YOUR EQUIPMENT

There are some things you can do to physically protect your computer equipment. Here is my list of dos and don'ts (you can probably add your own tips to the list):

- ▲ *Don't move or jar your computer when it's turned on.* Before you move the computer case even an inch or so, power it down. Don't put the computer case under your desk where it might get bumped or kicked. Although modern hard drives are tougher than earlier models, it's still possible to crash a drive by banging into it while it's reading or writing data.

- ▲ *Don't smoke around your computer.* Tar from cigarettes can accumulate on fans, causing them to jam, which in turn will cause the system to overheat. For older hard drives that are not adequately sealed, smoke particles can get inside and crash a drive.

- ▲ *Don't leave the PC turned off for weeks or months at a time.* Once my daughter left her PC turned off for an entire summer. At the beginning of the new school term, the PC would not boot. We discovered that the boot record at the beginning of the hard drive had become corrupted. PCs, like old cars, can give you problems after long spans of inactivity.

- ▲ *Don't block air vents on the front and rear of the computer case or on the monitor.* Proper air circulation is essential to keeping a system cool. Also, for optimum air flow, put covers on expansion slot openings on the rear of the case and put face-plates over empty bays on the front of the case (see Figure 11-3). Don't set a tower case directly on thick carpet because the air vent on the bottom front of the case can be blocked.

- ▲ *Use keyboard covers in dirty environments.* You can purchase plastic keyboard covers to protect the keyboard in a dirty or extremely dusty environment.

- ▲ *High humidity can be dangerous for hard drives.* I once worked in a basement with PCs, and hard drives failed much too often. After we installed dehumidifiers, the hard drives became more reliable.

- ▲ *In BIOS setup, disable the ability to write to the boot sector of the hard drive.* This alone can keep boot viruses at bay. However, before you upgrade your OS, such as when you upgrade Windows XP to Windows Vista, be sure to enable writing to the boot sector, which the OS setup will want to do.
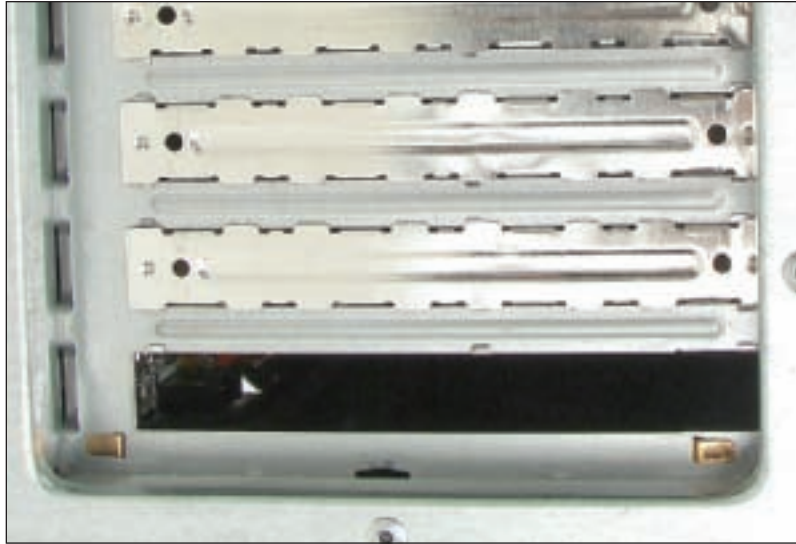
Figure 11-3 For optimum airflow, don't leave empty expansion slots and bays uncovered
Courtesy: Course Technology/Cengage Learning

▲ *If your data is really private, keep it under lock and key.* You can use all kinds of
security methods to encrypt, password protect, and hide data, but if it really is that
important, one obvious thing you can do is store the data on a removable storage
device such as a USB flash drive or external hard drive, and, when you're not using the
data, put the device in a fireproof safe. And, of course, keep at least two copies.
Sounds simple, but it works. You'll learn much more about securing computers and
their data in Chapter 19.

▲ *Protect your CDs, DVDs, BDs, and other storage media.* To protect discs, keep
them away from direct sunlight, heat, and extreme cold. Don't allow a disc to be
scratched.

▲ *Keep magnets away from your computer place.* Don't work inside the computer case
with magnetized screwdrivers and or sit strong magnets on top of the computer case.

▲ *Protect electrical equipment from power surges.* Lightning and other electrical power
surges can destroy computers and other electrical equipment. If the house or office
building does not have surge protection equipment installed at the breaker box, be
sure to install a protective device at each computer. The least expensive device is a
power strip that is also a surge protector, although you might want to use a line condi-
tioner or UPS for added protection.

▲ *Don't unpack and turn on a computer that has just come in from the cold.* If your
new laptop has just arrived and sat on your doorstep in freezing weather, don't
bring it in and immediately unpack it and turn it on. Wait until a computer has had
time to reach room temperature to prevent damage from condensation and static
electricity. In addition, when unpacking hardware or software, to help protect
against static electricity, remove the packing tape and cellophane from the work area
as soon as possible.

💡 **A+ Exam Tip**   The A+ 220–701 Essentials exam expects you to know how to keep computers
and monitors well ventilated and clean and to use protective covers for input devices such as the
keyboard.

HOW TO DISPOSE OF USED EQUIPMENT

As a PC technician, it will often be your responsibility to dispose of used equipment and consumables, including batteries, printer toner cartridges, hard drives, and monitors. Table 11-1 lists such items and how to dispose of them. Manufacturer documentation and local environmental regulators can also provide disposal instructions or guidance.

Part	How to Dispose
Alkaline batteries, including AAA, AA, A, C, D, and 9-volt	Dispose of these batteries in the regular trash. First check to see if there are recycling facilities in your area.
Button batteries used in digital cameras and other small equipment; battery packs used in notebooks	These batteries can contain silver oxide, mercury, lithium, or cadmium and are considered hazardous waste. Dispose of them by returning them to the original dealer or by taking them to a recycling center. To recycle, pack them separately from other items. If you don't have a recycling center nearby, contact your county for local regulations for disposal.
Laser printer toner cartridges	Return these to the manufacturer or dealer to be recycled.
Ink-jet printer cartridges Computer cases, power supplies, and other computer parts Monitors Chemical solvents and containers	Check with local county or environmental officials for laws and regulations in your area for proper disposal of these items. The county might have a recycling center that will receive them. Discharge a monitor before disposing of it. See the MSDS documents for chemicals to know how to dispose of them.
Storage media such as hard drives, CDs, DVDs, and BDs	Do physical damage to the device so it is not possible for sensitive data to be stolen. Then the device can be put in the trash. To meet legal requirements to destroy data, consider using a data-destruction service.

Table 11-1   Computer parts and how to dispose of them

Monitors and power supplies can contain a charge even after the devices are unplugged. Most CRT monitors today are designed to discharge after sitting unplugged for 60 minutes. To manually discharge a monitor, a high-voltage probe is used with the monitor case opened. Ask a technician trained to fix monitors to do this for you.

Don't throw out a hard drive, CD, DVD, tape, or other media that might have personal or corporate data on it unless you know the data can't be stolen off the device. You need to do physical damage to the device. For example, you can assure yourself that ordinary attempts by a thief to access the data on a hard drive will fail if you take a hammer and nail and punch the drive housing, forcing the nail straight through to the other side so that all drive disks are damaged. You can also break CDs and DVDs in half and do similar physical damage to flash drives or tapes.

However, if the data is extra sensitive and *really* important, know that a skilled thief can recover some data from a hard drive or other device that has been damaged in this way. To completely destroy the data, consider a secure data-destruction service. In fact, many government and corporate organizations are required by law to completely destroy data before disposing of media. For example, a hospital is required by law to protect patient data in this way. If you work for such an organization, using a data-destruction service is your safest option. To find a service, search the Internet using the search string "secure data destruction." However, don't use a service unless you have thoroughly checked its references and guarantees of legal compliance that you need to meet.

> 💡 **A+ Exam Tip** The A+ 220–701 Essentials exam expects you to know how to follow environmental guidelines to dispose of batteries, CRTs, chemical solvents, and containers. If you're not certain how to dispose of a product, see its MSDS document.

HOW TO MOVE COMPUTER EQUIPMENT

If you are shipping a computer, be aware that rough handling can cause damage, as can exposure to water, heat, and cold. The computer can also be misplaced, lost, or stolen. If you are preparing a computer for shipping, you would also want to do the following:

- Back up all important data on the computer. How to make backups is covered in Chapter 13. Make sure that the tapes or disks holding the backup data are secured and protected during transit. Consider shipping them separately.
- Coil all external cords and secure them with plastic ties or rubber bands.
- Pack the computer, monitor, and all devices in their original shipping cartons or similar boxes with enough packing material to protect them. Each device needs to be wrapped or secured separately so devices will not bump against each other.
- Purchase insurance on the shipment. Postal insurance is not expensive, and can save you a lot of money if materials are damaged in transit.

Now let's look at your responsibility under the law to protect software copyrights.

PROTECTING SOFTWARE COPYRIGHTS

As a computer support technician, you will be faced with the legal issues and practices surrounding the distribution of software. When someone purchases software from a software vendor, that person has only purchased a license for the software, which is the right to use it. The buyer does not legally *own* the software and, therefore, does not have the right to distribute it. The right to copy the work, called a copyright, belongs to the creator of the work or others to whom the creator transfers this right. Copyrights are intended to legally protect the intellectual property rights of organizations or individuals to creative works, which include books, images, and software.

As a PC technician, you will be called upon to install, upgrade, and customize software. You need to know your responsibilities in upholding the law, especially as it applies to software copyrights.

> 📝 **Notes** While the originator of a creative work is the original owner of a copyright, the copyright can be transferred from one entity to another.

FEDERAL COPYRIGHT ACT OF 1976

The Federal Copyright Act of 1976 was designed in part to protect software copyrights by requiring that only legally obtained copies of software be used; the law also allows for one backup copy (also called an archive copy) of software to be made. Making unauthorized copies of original software violates the Federal Copyright Act of 1976 and is called software piracy or, more officially, software copyright infringement. Some software companies have taken the position that the one archive copy of the software is not allowed.

Making a copy of software and then selling it or giving it away is a violation of the law. Because it is so easy to do, and because so many people do it, many people don't realize that it's illegal. Normally, only the employee who violated the copyright law is liable for

infringement; however, in some cases, an employer or supervisor is also held responsible, even when the copies were made without the employer's knowledge. The Business Software Alliance has estimated that 38 percent of software in the world is obtained illegally.

By purchasing a site license, a company can obtain the right to use multiple copies of software, which is a popular way for companies to provide software to employees. With this type of license, companies can distribute software to PCs from network servers or execute software directly off the server. Read the licensing agreement of any software to determine the terms of distribution. When you install software, this end-user licensing agreement (EULA) is usually displayed during installation and requires that you agree to it before continuing with the installation (see Figure 11-4).
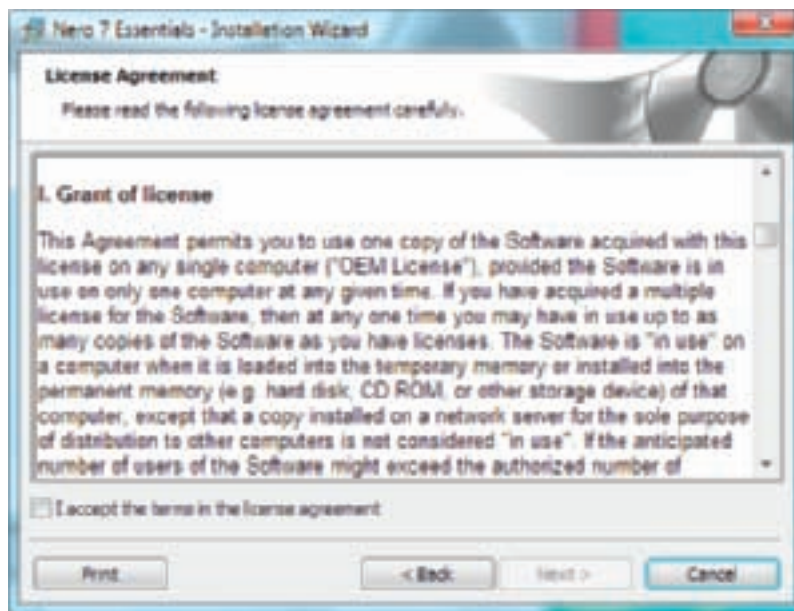

Figure 11-4   Agree to the EULA before the installation continues
Courtesy: Course Technology/Cengage Learning

INDUSTRY ASSOCIATIONS

One of two associations committed to the prevention of software piracy is the Software & Information Industry Association (*www.siia.net*), a nonprofit organization that educates the public and enforces copyright laws. The other organization, the Business Software Alliance (*www.bsa.org*), manages the BSA Anti-Piracy Hotline at 1-888-NOPIRACY. These associations are made up of hundreds of software manufacturers and publishers in North and Latin America, Europe, and Asia. They promote software raids on large and small companies; in the United States, they receive the cooperation of the U.S. government to prosecute offenders.

Vendors might sometimes sell counterfeit software by installing unauthorized software on computers for sale. This practice is called hard-disk loading. Vendors have even been known to counterfeit disk labels and Certificates of Authenticity. Warning signs that software purchased from vendors is pirated include:

- ◢ No end-user license is included.
- ◢ There is no mail-in product registration card.
- ◢ Software is installed on a new PC, but documentation and original discs are not included in the package.
- ◢ Documentation is photocopied, or discs have handwritten labels.

WHAT ARE YOUR RESPONSIBILITIES UNDER THE LAW?

Recall that according to the Federal Copyright Act of 1976, the legal users of software have the right to make one backup copy. Other rights are based on what the copyright holder allows. In 1990, the U.S. Congress passed the Software Rental Amendment Act, which prevents renting, leasing, lending, or sharing software without the express written permission of the copyright holder. In 1992, Congress instituted criminal penalties for software copyright infringement, which include imprisonment for up to five years and/or fines up to $250,000 for the unlawful reproduction or distribution of 10 or more copies of software.

As an employee of a company that has a site license to use multiple copies of the software, your responsibility is to comply with the site license agreement. It is also your responsibility to purchase only legitimate software. Purchasers of counterfeit or copied software face the risk of corrupted files, virus-infected discs, inadequate documentation, and lack of technical support and upgrades as well as the legal penalties for using pirated software.

When the software budget is very low, instead of purchasing or pirating commercial software, you might consider using open source software. Open source software is developed by volunteers, and the software is free to use, copy, and even distribute as long as you agree to the terms of the license as defined by the group making the software available. Examples of open source software are the Linux OS, Apache HTTP Server (a Web server), and Mozilla Firefox (a Web browser).

Now we're ready to look at ways to set up an effective preventive maintenance plan for personal computers.

PERSONAL COMPUTER PREVENTIVE MAINTENANCE

**A+
220-701
2.5**

Preventive maintenance can prevent certain computer problems from occurring in the first place. The more preventive maintenance work you do initially, the fewer problems you are likely to have later, and the less troubleshooting and repair you will have to do.

If you are responsible for the PCs in an organization, make and implement a preventive maintenance plan to help prevent failures and reduce repair costs and downtime. In addition, you need a disaster recovery plan to manage failures when they occur. PC failures are caused by many different environmental and human factors, including heat, dust, magnetism, power supply problems, static electricity, human error (such as spilled liquids or an accidental change of setup and software configurations), and viruses. The goals of preventive maintenance are to reduce the likelihood that the events that cause PC failures will occur and to lessen the damage if they do.

This section focuses on what to do when a computer becomes your permanent responsibility and how to create a preventive maintenance plan. This chapter contains the complete lists of tasks; some of the tasks are discussed in detail in other chapters.

SET UP A METHOD OF DOCUMENTATION

When you first set up a new computer, start a record book about this computer, using either a file on disk or a notebook dedicated to this machine. In this notebook or file, record any changes in setup data as well as any problems you experience or maintenance that you do on this computer. Be diligent in keeping this notebook up to date, because it will be invaluable in diagnosing problems and upgrading equipment. Keep a printed or handwritten record of all changes to BIOS setup data and jumpers on the motherboard, and store the record with the hardware and software documentation.

If you are not the primary user of the computer, you might want to keep the hardware documentation separate from the computer itself. Label the documentation so that you can easily identify that it belongs to this computer. Keep this hardware documentation and your notes in a safe place. Some support people tape a large envelope inside the computer case; the envelope contains important documentation and records specific to that computer. On the other hand, if you're also responsible for software reference manuals, know that these manuals need to be kept in a location that is convenient for users.

> 📝 **Notes** If you are not using call-tracking software, you might want to keep a record of all troubleshooting you do on a computer in a word-processing document that lists all the problems you have encountered and the solutions you used. This will help save time when troubleshooting problems you have encountered before. Store the document file on a CD-RW, flash drive, or floppy disk that you keep with the computer's documentation. You might want to make a new printout each time the document changes. Don't store the document on the hard drive of the computer it applies to because it will not be available if the hard drive fails.

CREATE A PREVENTIVE MAINTENANCE PLAN

It is important to develop an overall preventive maintenance plan. If your company has established written guidelines for PC preventive maintenance, read them and follow the procedures necessary to make them work. If your company has no established plan, make your own.

A preventive maintenance plan tends to evolve from a history or pattern of malfunctions within an organization. For example, dusty environments can mean more maintenance, whereas a clean environment can mean less maintenance. Table 11-2 lists some guidelines for developing a preventive maintenance plan that might work for you.

> 💡 **A+ Exam Tip** The A+ 220–701 Essentials exam expects you to know how to clean internal and external components and use appropriate cleaning materials as part of a regular preventive maintenance plan.

Component	Maintenance
Computer	Physically inspect the computer by doing the following: ◢ Make sure the computer is in a proper environment. Problems to look for are listed earlier in the chapter. ◢ Check that air vents on the computer case or monitor are not blocked by papers, books, drapes, or other obstructions. ◢ Make sure the inside of the computer case is free from dust. Use an antistatic vacuum, blower, or can of compressed air to blow the dust out of the case and clean vents, power supply, and fans. ◢ Verify that chips and expansion cards are firmly seated. ◢ Check cables and cords for wear and tear. Look for trip hazards and correct them if necessary.
Keyboard	◢ Clean the keyboard. Unplug the keyboard and then blow or vacuum it out. To dislodge debris, turn the keyboard upside down and bump it. Use cleaning wipes to clean the surface.
Mouse	◢ Clean the mouse. To clean a wheel mouse, remove the cover of the mouse ball from the bottom of the mouse. The cover usually comes off

Table 11-2 Guidelines for developing a PC preventive maintenance plan

Component	Maintenance
	with a simple press and shift or turn motion. Clean the rollers with a cotton swab dipped in a very small amount of liquid soap. The sticky side of duct tape works well to clean the mouse ball.
Monitor	▲ Clean the screen with a lint-free cloth. You can also use special monitor wipes that are safe for CRT and LCD monitors.
Printers	▲ Using compressed air or a vacuum, clean out the dust and bits of paper. Small pieces of paper can be removed with tweezers, preferably insulated ones. ▲ Clean the paper path with a soft, lint-free cloth. ▲ Don't re-ink ribbons or use recharged toner cartridges. ▲ If the printer uses an ozone filter, replace it as recommended by the manufacturer. ▲ Replace other components as recommended by the manufacturer. You can purchase maintenance kits from the printer manufacturer, which include a scheduled maintenance plan for the printer. How to perform these scheduled maintenances is covered in Chapter 22.
UPS or surge protector	▲ Verify the system is protected against electrical surges by using a UPS or surge protector. ▲ Run a weak battery test on the UPS. ▲ Run a diagnostic test on the UPS as appropriate.
Backup of data	▲ If the computer is used to hold important data, verify data is being backed up on a regular basis and backup media is being kept in an offsite location. How to schedule backups is covered in Chapter 13.
Hard drive	▲ Rearrange noncontiguous parts of files (called defragmenting the drive), delete unneeded files, and check the drive for errors. How to do all this is covered in Chapter 13.
Clean up the start routine	▲ To keep Windows from starting slowly, reduce Windows startup programs to a minimum (covered in Chapters 13 and 14). ▲ Delete temporary files and check the hard drive for errors (covered in Chapter 13).
Drivers and firmware updates	▲ Update firmware or device drivers only if the device is giving problems (covered in Chapter 5).
Security	▲ Verify Windows has all updates and patches installed and that Windows is set to automatically download and install updates (covered in Chapter 12). ▲ Verify that antivirus software is installed, running, and updated (covered in Chapter 20). ▲ Verify that a personal firewall is configured and running on the computer (covered in Chapter 19).
Software	▲ If directed by your employer, check that only authorized software is present.
Written records	▲ Keep a record of all software, including version numbers and the OS installed on the PC. ▲ Keep a record of all hardware components installed, including hardware settings. ▲ Record when and what preventive maintenance is performed. ▲ Record any repairs done to the PC.

Table 11-2 Guidelines for developing a PC preventive maintenance plan (continued)

📝 **Notes** In most situations, you don't need to back up installed applications. If the application gets corrupted, you can install it again using the setup CDs. It's extremely important that you have the original setup CDs handy when a hard drive fails—without these CDs, you won't be able to reinstall the software. Users that you support also need to understand that you cannot reinstall software installed on their systems if the software has been pirated and the CDs or DVDs are no longer available.

HOW TO TROUBLESHOOT A PC PROBLEM

When a computer doesn't work and you're responsible for fixing it, you should generally approach the problem first as an investigator and discoverer, always being careful not to compound the problem through your own actions. If the problem seems difficult, see it as an opportunity to learn something new. Ask questions until you understand the source of the problem. Once you understand it, you're almost done, because most likely the solution will be evident. If you take the attitude that you can understand the problem and solve it, no matter how deeply you have to dig, you probably *will* solve it.

One systematic method to solve a problem used by most expert troubleshooters is the six steps diagramed in Figure 11-5. These steps are:

1. Interview the user and back up data before you make any changes to the system.

2. Examine the system, analyze the problem, and make an initial determination of what is the source of the problem.

3. Test your theory. If the theory is not confirmed, form another theory or escalate.

4. After you know the source of the problem, plan what to do to fix the problem and then fix it.

5. Verify the problem is fixed and that the system works. Take any preventive measures to make sure the problem doesn't happen again.

6. Document activities, outcomes, and what you learned.

Now let's examine the process step by step. As you learn about these six steps, you'll also learn about 15 rules useful when troubleshooting that are interspersed among the steps. Here's the first rule.

Rule 1: Approach the Problem Systematically

When trying to solve the problem, start at the beginning and walk through the situation in a thorough, careful way. This one rule is invaluable. Remember it and apply it every time. If you don't find the explanation to the problem after one systematic walkthrough, then repeat the entire process. Check and double-check to find the step you overlooked the first time. Most problems with computers are simple, such as a loose cable or circuit board. Computers are logical through and through. Whatever the problem is, it's also very logical. Also, if you are faced with more than one problem on the same computer, work on only one problem at a time. To try to solve multiple problems at the same time can get too confusing.

💡 **A+ Exam Tip** The A+ 220–701 Essentials exam expects you to know about all the aspects of troubleshooting theory and strategy and how to apply the troubleshooting procedures and techniques described in this section. At the front of the book, read over the A+ 220–701 Objective 2.1 and compare it to Figure 11-5.
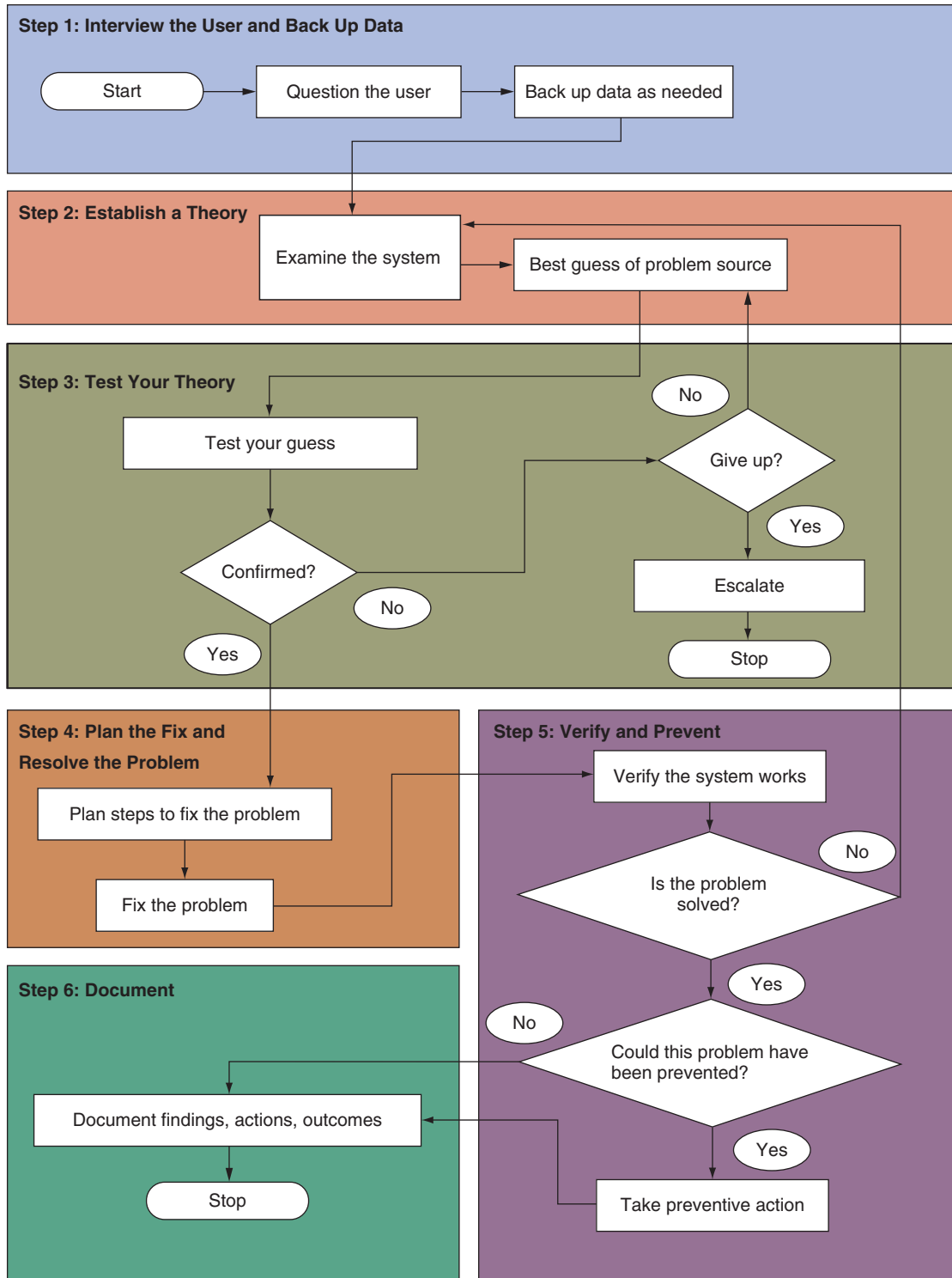
Step 1: Interview the User and Back Up Data

Start → Question the user → Back up data as needed

Step 2: Establish a Theory

Examine the system → Best guess of problem source

Step 3: Test Your Theory

Test your guess

Give up?
No
Yes

Confirmed?
No
Yes

Escalate

Stop

Step 4: Plan the Fix and Resolve the Problem

Plan steps to fix the problem

Fix the problem

Step 5: Verify and Prevent

Verify the system works

Is the problem solved?
No
Yes

Could this problem have been prevented?
No
Yes

Take preventive action

Step 6: Document

Document findings, actions, outcomes

Stop

Figure 11-5   General approach to problem solving
Courtesy: Course Technology/Cengage Learning

11

A+ 220-701

STEP 1: INTERVIEW THE USER AND BACK UP DATA

Every troubleshooting situation begins with interviewing the user if he or she is available. Sometimes you might be presented with a PC to fix when all you have is a written description of the problem and you don't have the opportunity to talk with the user. However, if you can

speak with the user, ask questions to help you identify the problem, how to reproduce it, and possible sources of the problem. Also ask about any data on the PC that is not backed up.

> 💡 **A+ Exam Tip** The A+ 220–701 Essentials exam expects you to know how to interact with a user and know what questions to ask, given a troubleshooting scenario.

Chapter 3 lists several sample questions to ask a user. Here are the four most important ones:

1. Can you please describe the problem, including error messages, failures, and what you see or hear?
2. What changes have recently been made to the system?
3. Is there important data on the system that is not backed up?
4. Can you show me how to reproduce the problem?

Based on the answers you receive, ask more penetrating questions until you feel the user has given you all the information he or she knows that can help you solve the problem. As you talk with the user, don't forget to use all the communication skills that you learned about in Chapter 3. As you talk with the user, keep in mind rules 2, 3, and also 4.

Rule 2: Establish Your Priorities

This rule can help make for a satisfied customer. Decide what your first priority is. For example, it might be to recover lost data, or to get the PC back up and running as soon as possible. Ask the user or customer for advice when practical.

Rule 3: Beware of User Error

Remember that many problems stem from user error. If you suspect this is the case, ask the user to show you the problem and carefully watch what the user is doing.

Rule 4: Keep Your Cool and Don't Rush

In some situations, you might be tempted to act too quickly and to be drawn into the user's sense of emergency. But keep your cool and don't rush. For example, when a computer stops working, if unsaved data is still in memory or if data or software on the hard drive has not been backed up, look and think carefully before you leap! A wrong move can be costly. The best advice is not to hurry. Carefully plan your moves. Read the documentation if you're not sure what to do, and don't hesitate to ask for help. Don't simply try something, hoping it will work, unless you've run out of more intelligent alternatives!

After you have talked with the user, be sure to back up any important data that is not currently backed up before you begin work on the PC. If the PC is working well enough to boot to the Windows desktop, you can use Windows Explorer to copy data to a flash drive, another computer on the network, or other storage media.

> 💡 **A+ Exam Tip** The A+ 220–701 Essentials exam expects you to know the importance of making backups before you make changes to a system.

If the computer is not healthy enough to use Windows Explorer, don't do anything to jeopardize the data. If you must take a risk with the data, let it be the user's decision to do

so, not yours. Try to boot the system. If the system will not boot to the Windows desktop, recall from Chapter 8 that you can remove the hard drive from the system and use a PATA to USB converter or a SATA to USB converter to connect the drive to a USB port on another computer. You can then copy the data to the other computer. Next, return the hard drive to the original computer so you can begin troubleshooting the problem.

If possible, have the user verify that all important data is safely backed up before you continue to the next troubleshooting step. If you're new to troubleshooting and don't want the user looking over your shoulder while you work, you might want to let him or her know you'd prefer to work alone. You can say something like, "Okay, I think I have everything I need to get started. I'll let you know if I have another question."

STEP 2: EXAMINE THE SYSTEM AND MAKE YOUR BEST GUESS

You're now ready to start solving the problem. Rules 5 and 6 can help.

Rule 5: Make No Assumptions

This rule is the hardest to follow, because there is a tendency to trust anything in writing and assume that people are telling you exactly what happened. But documentation is sometimes wrong, and people don't always describe events as they occurred, so do your own investigating. For example, if the user tells you that the system boots up with no error messages, but that the software still doesn't work, boot for yourself. You never know what the user might have overlooked.

Rule 6: Try the Simple Things First

Most problems are so simple that we overlook them because we expect the problem to be difficult. Don't let the complexity of computers fool you. Most problems are easy to fix. Really, they are! To save time, check the simple things first, such as whether a power switch is not turned on or a cable is loose. Generally, it's easy to check for a hardware problem before you check for a software problem. For example, if a USB drive is not working, verify the drive works on another computer before verifying the drivers are installed correctly.

Follow these steps to form your best guess (best theory) and test it:

1. *Reproduce the problem and observe for yourself what the user has described*. For example, if the user tells you the system is totally dead, find out for yourself. Plug in the power and turn on the system. Listen for fans and look for lights and error messages. As another example, suppose the user tells you that Internet Explorer will not open. Try opening it yourself to see what error messages might appear. As you investigate the system, refrain from making changes until you've come up with your theory as to what the source of the problem is. Can you duplicate the problem? Intermittent problems are generally more difficult to solve than problems that occur consistently.

2. *Decide if the problem is hardware or software related*. Sometimes you might not be sure, but make your best guess. For example, if the system fails before Windows starts to load, chances are the problem is a hardware problem. If the user tells you the system has not worked since the lightning storm the night before, chances are the problem is electrical. If the problem is that Windows Explorer will not open even though the Windows desktop loads, you can assume the problem is software related. In another example, suppose a user complains that his Word documents are getting corrupted. Possible sources of the problem might be that the user does not know how to

save documents properly, the software or the OS might be corrupted, the PC might have a virus, or the hard drive might be intermittently failing. Investigate for yourself and then decide if the problem is caused by software, hardware, or the user.

3. *Make your best guess as to the source of the problem.* Here are some practical examples of what a best guess might be, keeping in mind the rule to check the simple things first:

▲ The video does not work. Your best guess is the monitor cables are loose or the monitor is not turned on.

▲ Spreadsheets are getting corrupted. Your best guess is the user is not saving the documents correctly.

▲ The DVD drive is not reading a DVD. Your best guess is the DVD is scratched.

▲ The system refuses to boot and gives the error that the hard drive is not found. Your best guess is internal cables to the drive are loose.

If you're having a problem deciding what might be the source of the problem, try searching these resources for ideas and tips:

▲ User manuals and installation manuals for a device or software often list symptoms of problems with possible solutions and troubleshooting tips.

▲ Use a search engine to search the Internet for help. Use, in your search string, an error message, symptom, hardware device, or description of the problem. For the most reliable information about a hardware device or application, see the Web site of the manufacturer (see Figure 11-6). These sites might offer troubleshooting and support pages,
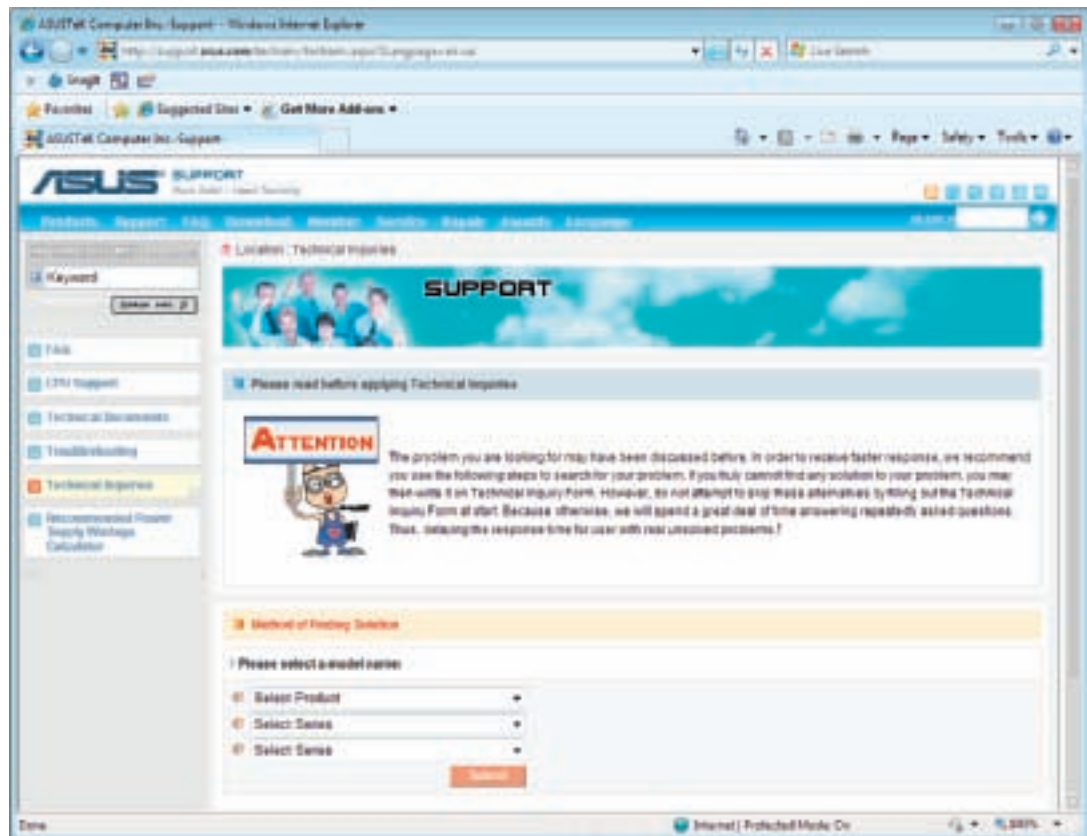

Figure 11-6 Search manufacturer Web sites for help with a hardware or software product
Courtesy: Course Technology/Cengage Learning

help forums, chat sessions, and e-mail support. For Windows problems, the best Web sites to search are *technet.microsoft.com* or *support.microsoft.com*.

▲ Training materials, technical books, reference manuals, and textbooks like this one can all be good sources of help.

📄 **Notes** To limit your search to a particular site when using *www.google.com*, use the site parameter in the search box. For example, to search only the Microsoft site for information about the defrag command, enter this search string: **defrag site:microsoft.com**.

APPLYING **CONCEPTS** Possibly the most powerful strategy in this entire chapter for troubleshooting is to use a search engine to find insights and solutions on the Internet. The chances are always good that someone has had exactly the same problem, presented the problem on some forum on the Internet, and someone else has presented a step-by-step solution. All you have to do is find it! As you practice this type of Web research, you'll get better and better at knowing how to form a search string and which Web sites are trustworthy and present the best information. If your first searches don't work, please don't give up! It might take patient searching for 15 or 20 minutes to find the solution you need. As you search, most likely you will learn more and more about the problem. But sometimes too much information can overwhelm you. Here are a few tips to narrow down an Internet search and zero in on the solution:

1. Go to *www.google.com* and click **Advanced Search**. In the Advanced Search window, shown in Figure 11-7, click **Date, usage rights, numeric range, and more**. Under Date, select past 24 hours, past week, past month, or past year.

2. To limit your search to only one site, include the site parameter in your Google search string. For example, to limit your search to the ASUS site when searching for Vista drivers for your P5AD2 motherboard, use this search string: **asus P5AD2 Vista drivers site:asus.com**. It's best to not include the www in the site name so that addresses such as support.asus.com will be used.

3. Limit your search results by adding more detail to your search string. For example, instead of searching on "driver Asus motherboard" search on "Vista audio driver Asus P5AD2 motherboard."

4. Speaking of drivers for a motherboard, consider the audio drivers might not come from ASUS, the board manufacturer. Don't forget to check the Web site of the chipset manufacturer (Intel at *www.intel.com*) or the audio controller manufacturer (C-Media at *www.cmedia.com.tw*). If you don't know who these manufacturers are, you can find that information on the Internet. For example, a search on "audio controller Asus P5AD2" will tell you that the audio controller for this board was built by C-Media.

So now let's practice. Suppose you have used Disk Management in Windows XP to configure a hard drive as a dynamic disk. But now you need to upgrade to Windows Vista Home Premium, which does not support dynamic disks. Is there a way to convert a dynamic disk to a basic disk without losing all the data on the disk? Search the Internet for the step-by-step solution to do this. What was the search string you used that led you to the solution? On what Web site did you find the solution?
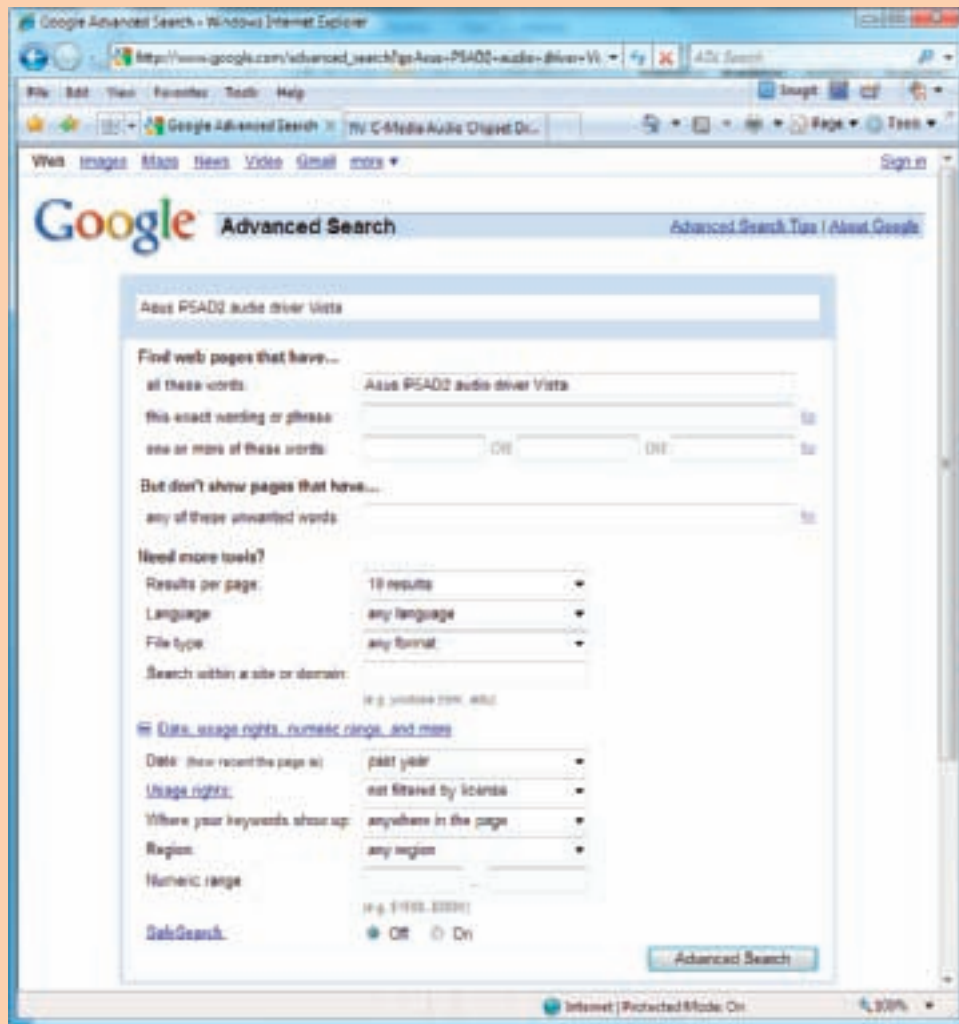
Figure 11-7   Use Google Advanced Search features to narrow down the number of hits
Courtesy: Course Technology/Cengage Learning

STEP 3: TEST YOUR THEORY

For simple problems, you can zip right through Steps 3, 4, and 5 in Figure 11-5 quickly. Here are two examples where Steps 3, 4, and 5 go very fast:

▴ The video does not work and you suspect loose cables or the monitor is not turned on. You check the video cable connection (Step 3) and discover it's loose. As you connect it (Step 4), the video display works. Problem solved. So now you take the time to screw the video cable to the connection (Step 5) so the problem won't happen again.

▴ Spreadsheets are getting corrupted. As you watch the user save a file, you discover he is saving files in a wrong format that other software in the office cannot read (Step 3). You step the user through saving the file correctly and

then verify that others can open the file (Step 4). You explain to the user which format to use (Step 5). The problem then is solved, and it's not likely to happen again.

Here are two examples of Step 3 which include testing a guess that is not correct:

▲ The CD drive won't read a CD and you suspect the CD is scratched. When you check the disc, it looks fine. Your next guess is the CD drive is not recognized by Windows. You check Device Manager, and it reports errors with the drive. Your next guess is that drivers are corrupted.

▲ The system refuses to boot and gives the error message that the hard drive is not found. Internal cable connections are solid. Your next guess is the power supply is not supplying power to the drive.

Here are two examples of Step 3 where your guess is correct and then you move on toward Step 4 to plan a solution:

▲ Word files are getting corrupted. After eliminating several simple causes, you guess that the hard drive is going bad. You check Event Viewer, a Windows utility that reports errors with hardware devices, and discover Windows has recorded write errors to the drive multiple times (Step 3). Your theory is confirmed that the drive is bad and needs replacing (Step 4).

▲ Video does not work. You check cables and power and verify monitor settings controlled by buttons on the front of the monitor are all okay, but still no video. You guess the video cable might be bad and exchange it with one you know is good, but still no video. Therefore, you guess that the monitor is bad. You move the monitor to a working PC and it still does not work. You try a good monitor on the first PC and it works fine. Your guess that the monitor is bad has been confirmed (Step 3). Next, you plan how to purchase a new monitor (Step 4).

As you test your guesses, keep in mind rules 7 through 13.

Rule 7: Trade Known Good for Suspected Bad

When diagnosing hardware problems, this method works well if you can draw from a group of parts that you know work correctly. Suppose, for example, video does not work. The parts of the video subsystem are the video card, the power cord to the monitor, the cord from the monitor to the PC case, and the monitor itself. Also, don't forget that the video card is inserted into an expansion slot on the motherboard, and the monitor depends on electrical power. As you suspect each of these five components to be bad, you can try them one at a time beginning with the easiest one to replace: the monitor. Trade the monitor for one that you know works. If this theory fails, trade the power cord, trade the cord to the PC video port, move the video card to a new slot, and trade the video card.

When you're trading a good component for a suspected bad one, work methodically by eliminating one component at a time. Don't trade the video card and the monitor and then turn on the PC to determine if they work. It's possible that both the card and the monitor are bad, but assume that only one component is bad before you consider whether multiple components need trading.

In this situation, suppose you keep trading components in the video subsystem until you have no more variations. Next, take the entire subsystem—video card, cords, and monitor—to a PC that you know works, and plug each of them in. If they work, you have isolated the problem to the PC, not the video. Now turn your attention back to the PC: the motherboard, the software settings within the OS, the video driver, and other devices. Knowing that the video subsystem works on the good PC gives you a valuable tool. Compare the video driver on the good PC to the one on the bad PC. Make certain the BIOS settings, software settings, and other settings are the same.

Rule 8: Trade Suspected Bad for Known Good

An alternate approach works well in certain situations. If you have a working PC that is configured similarly to the one you are troubleshooting (a common situation in many corporate or educational environments), rather than trading good for suspected bad, you can trade suspected bad for good. Take each component that you suspect is bad and install it in the working PC. If the component works on the good PC, then you have eliminated it as a suspect. If the working PC breaks down, then you have probably identified the bad component.

Rule 9: Divide and Conquer

This rule is the most powerful. Isolate the problem. In the overall system, remove one hardware or software component after another, until the problem is isolated to a small part of the whole system. As you divide a large problem into smaller components, you can analyze each component separately. You can use one or more of the following to help you divide and conquer on your own system:

- ▲ In Windows, stop all nonessential services running in the background to eliminate them as the problem.
- ▲ Boot from a bootable CD or DVD to eliminate the OS and startup files on the hard drive as the problem.

Remove any unnecessary hardware devices, such as a scanner card, internal modem, CD drive, and even the hard drive. Once down to the essentials, start exchanging components you know are good for those you suspect are bad, until the problem goes away. You don't need to physically remove the CD drive or hard drive from the bays inside the case. Simply disconnect the data cable and the power cable. Remember that the problem might be a resource conflict. If the network card worked well until the CD drive was reconnected and now neither works, try the CD drive without the network card. If the CD drive works, you most likely have a resource conflict.

Rule 10: Become a Researcher

Following this rule is the most fun. When a computer problem arises that you can't easily solve, be as tenacious as a bulldog. Search the Internet, ask questions, then read more, make some phone calls, and ask more questions. Take advantage of every available resource, including online help, the Internet, documentation, technical support, and books such as this one. Learn to perform advanced searches using a good search engine on the Web, such as *www.google.com*. What you learn will be yours to take to the next problem. This is the real joy of computer troubleshooting. If you're good at it, you're always learning something new.

Rule 11: Write Things Down

Keep good notes as you're working. They'll help you think more clearly. Draw diagrams. Make lists. Clearly and precisely write down what you're learning. If you need to leave the problem and return to it later, it's difficult to remember what you have observed and already tried. When the problem gets cold like this, your notes will be invaluable.

Rule 12: Don't Assume the Worst

When it's an emergency and your only copy of data is on a hard drive that is not working, don't assume that the data is lost. Much can be done to recover data. If you want to recover lost data on a hard drive, don't write anything to the drive; you might write on top of lost data, eliminating all chances of recovery.

Rule 13: Reboot and Start Over

This is an important rule. Fresh starts are good, and they uncover events or steps that might have been overlooked. Take a break! Get away from the problem. Begin again.

By the time you have finished Step 3, the problem will have been solved or you will know the source of the problem and will be ready to plan a solution.

STEP 4: PLAN YOUR SOLUTION AND THEN FIX THE PROBLEM

Some solutions, such as replacing a hard drive or a motherboard, are expensive and time consuming. You need to carefully consider what you will do and the order you will do it. When planning and implementing your solution, keep rules 14 and 15 in mind.

Rule 14: Use the Least Invasive Solution First

As you solve computer problems, always keep in mind that you don't want to make things worse, so you should use the least invasive solution. Keep in mind that you want to fix the problem in such a way that the system is returned to normal working condition with the least amount of effort. For example, don't format the hard drive until you've first tried to fix the problem without having to erase everything on the drive.

Rule 15: Know Your Starting Point

Find out what works and doesn't work before you take anything apart or try some possible fix. Suppose you decide the power supply is bad and exchange it. After you make the exchange, you discover the CD-ROM drive doesn't work. You don't know if you broke the drive while working on the system or it was already broken before you started. As much as possible, find out what works or what doesn't work before you attempt a fix. For example, you can reboot the computer and read a file from CD or use an application to print a file on the network.

Do the following to plan your solution and fix the problem:

1. Consider different solutions, and select the least invasive one. In other words, choose the solution that fixes the problem by making as few changes to the system as possible. Some solutions are obvious, such as replacing a bad monitor, but others might not be so obvious. For example, if Windows is corrupted and your options are to reinstall Windows or repair it, it's better to repair it so there's less work to do to restore the system to good working order and to return it to the configuration the user had before the problem occurred.

2. If hardware needs replacing, follow guidelines given in other chapters to select a replacement part that is compatible with your system.

3. Before installing the new part, as best you can, determine what works and doesn't work about the system so you know your starting point.

4. Install the new part. This might be as simple as plugging up a new monitor. Or it might be as difficult as replacing a hard drive, reinstalling Windows and applications software, and restoring data from backups.

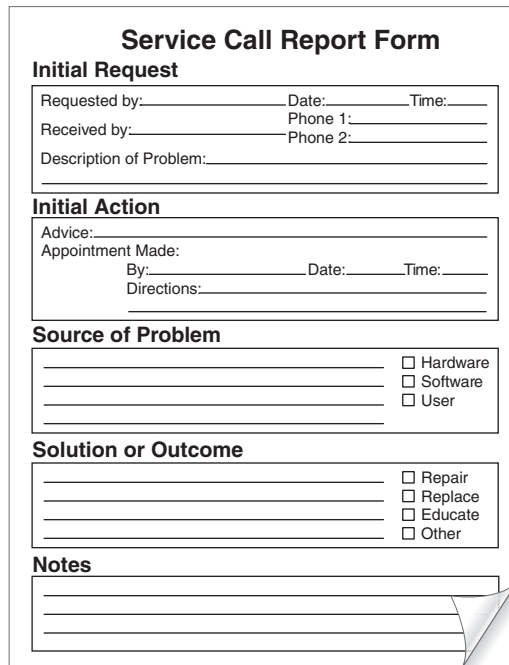## STEP 5: VERIFY THE FIX AND TAKE PREVENTIVE ACTION

After you have implemented your solution, reboot the system and verify all is well. Can you reach the Internet, use the printer, or burn a CD? If possible, have the user check everything and verify that the job is done satisfactorily. If either of you find a problem, return to Step 2 in the troubleshooting process to reexamine the system and form a new theory as to the cause of the problem.

After you and the user have verified all is working, ask yourself the question, "Could this problem have been prevented?" If so, go the extra mile to instruct the user, install a surge protector, or whatever else is appropriate to prevent future problems.

STEP 6: DOCUMENT WHAT HAPPENED

Good documentation helps you take what you learned into the next troubleshooting situation, train others, develop effective preventive maintenance plans, and satisfy any audits or customer or employer queries about your work. Be sure to write down the initial symptoms, the source of the problem, and what you did to fix it. Figure 11-8 shows a Service Call Report Form that might be used in a small computer repair center.

Figure 11-8　Service call report form
Courtesy: Course Technology/Cengage Learning

APPLYING CONCEPTS　Intermittent problems can make troubleshooting challenging. The trick in diagnosing problems that come and go is to look for patterns or clues as to when the problems occur. If you or the user can't reproduce the problem at will, ask the user to keep a log of when the problems occur and exactly what messages appear. Tell the user that intermittent problems are the hardest to solve and might take some time, but that you won't give up. Show the user how to get a printed screen of the error messages when they appear. Here's one method to print a screen shot:

1. Press the **Print Screen** key to copy the displayed screen to the Windows Clipboard.

2. Launch the Paint software accessory program and paste the contents of the Clipboard into the document. You might need to use the Zoom Out command on the document first. You can then print the document with the displayed screen, using Paint. You can also paste the contents of the Clipboard into a document created by a word-processing application such as Word.

>> CHAPTER SUMMARY

▲ A Material Safety Data Sheet (MSDS) tells you how to deal with accidents that happen with chemicals.

▲ Avoid trip hazards by moving cables out of the way or installing protective covers over the cables.

▲ Dispose of used computer equipment, batteries, and printer cartridges according to guidelines in your county. Discharge a CRT monitor before disposing of it.

▲ Destroy storage devices such as hard drives or CDs before throwing them in the trash so that sensitive data cannot be stolen off the device.

▲ Never ship a PC when the only copy of important data is on its hard drive.

▲ The buyer of software does not legally own the software or have the right to distribute it. According to the Federal Copyright Act of 1976, you have the right to make one backup copy of software.

▲ When a PC is your permanent responsibility, keep good backups of data and system files, document all setup changes, problems, and solutions, and take precautions to protect the system against viruses and other attacks.

▲ The goals of preventive maintenance are to make PCs last longer and work better, protect data and software, and reduce repair costs.

▲ A PC preventive maintenance plan includes blowing dust from the inside of the computer case, keeping a record of setup data, backing up the hard drive, and cleaning the mouse, monitor, and keyboard.

▲ Protecting software and hardware documentation is an important preventive maintenance chore.

▲ The six steps in the troubleshooting process are as follows: 1. Interview the user and back up data, 2. Examine the system and form a theory of probable cause, 3. Test your theory, 4. Plan a solution and implement it, 5. Verify all works and take appropriate preventive measures, and 6. Document what happened and the outcome.

11

>> KEY TERMS

For explanations of key terms, see the Glossary near the end of the book.

copyright	license	site license
hard-disk loading	Material Safety Data Sheet (MSDS)	trip hazard

>> REVIEWING THE BASICS

1. If you spill a cleaning solution on your clothes and hands, what is the best way to find out how to deal with the spill?

2. What is the term used to describe a network cable lying loose in a high-traffic area?

3. When lifting a heavy object, should you bend your back over the object or stoop down to the object, keeping your back straight?

4. Why should a tower case not sit on thick carpet?

5. What can you do to protect a keyboard that is used in an extremely dusty area?

6. Why is it not a good practice to unpack computer parts immediately after they have been delivered on a cold day?

7. Why is it not a good idea to throw used batteries in the trash?

8. What is the best way to get rid of laser printer toner cartridges?

9. What should you do to a failed hard drive that was used in the Accounting Department before you put the drive in the trash?

10. When shipping a computer, why is it not a good idea to ship backups of the system in the same package with the computer?

11. Which law defines software copyright infringement?

12. What is the difference between a license to use software and a site license to use software?

13. Why is it not a good idea to buy software that is on CDs with handwritten labels?

14. What are the six steps used by troubleshooters to solve PC problems?

15. When solving a PC problem, why is it important to use the least obstructive solution first?

>> THINKING CRITICALLY

1. If computers in your office are your responsibility, what should you do when you visit a user's desk and discover a network cable running across the room?

   a. Ask the user to please not leave cables on the floor where someone can trip.

   b. Ask the user permission to move the cable.

   c. Move the cable so it is not a trip hazard.

   d. Put a sign up to tell people to watch for the cable.

2. As a help-desk technician, list some good detective questions to ask if the user calls to say, "My PC won't boot."

3. Someone calls saying he has attempted to install a new monitor, but the monitor does not work. List some questions you would ask.

>> HANDS-ON PROJECTS

PROJECT 11-1:   Safely Clean Computer Equipment

Following guidelines in the chapter, practice some preventive maintenance tasks by following these steps to clean a computer:

1. Shut down the computer and unplug it. Press the power button to drain power.

2. Clean the keyboard, monitor, and mouse. For a wheel mouse, remove the ball and clean the wheels.

3. Clean the outside of the computer case.

4. Open the case and using a ground bracelet, clean the dust from the case. Make sure all fans move freely.

5. Verify the cables are out of the way of airflow. Use cable ties as necessary.

6. Check that each expansion card and memory module is securely seated in its slot.

7. Power up the system and make sure all is working.

8. Clean up around your work area. If you left dust on the floor as you blew it out of the computer case, be sure to clean it up.

PROJECT 11-2:   Developing Help-Desk Skills

Pair up with a second person in your class or lab environment. Then, without either of you watching, have a third person in your class or lab environment create an error on a computer so that the computer does not boot properly. Now, have your partner sit at the computer and play the role of an inexperienced user who tries to start up the system and receives an error he does not know how to handle. You will sit with your back to the partner/user and you cannot see the computer. In this setup, troubleshoot the problem and talk the user through to a solution. While doing so, abide by these rules:

1. You can't turn around to look at the screen or the computer.

2. You have to practice professional mannerisms and speech.

3. As you work, you have to keep a log of the "phone call to the help desk," recording in the log the major steps toward diagnosing and correcting the problem.

When the problem is resolved, have the third person create a different problem that causes the PC not to boot correctly, and exchange roles with your partner.

PROJECT 11-3:   Researching Disposal Rules

Research the laws and regulations in your community concerning the disposal of batteries and old computer parts. Answer these questions regarding your community:

1. How do you properly dispose of a monitor?

2. How do you properly dispose of a battery pack used by a notebook computer?

3. How do you properly dispose of a large box of assorted computer parts, including hard drives, floppy drives, computer cases, and circuit boards?

PROJECT 11-4:   Researching PC Support

The Internet is an excellent resource to use when problem solving, and it's helpful to know which Web sites are trustworthy and useful. Access each of the Web sites listed in Table 11-3, and print one Web page from each site that shows information that might be useful for a support technician. If the site offers a free e-mail newsletter, consider subscribing to it.

11

Organization	Web Site
CNET, Inc.	*www.cnet.com*
Experts Exchange (subscription site)	*www.experts-exchange.com*
F-Secure Corp	*www.f-secure.com*
How Stuff Works	*www.howstuffworks.com*
Kingston Technology (information about memory)	*www.kingston.com*
Michael Karbo	*www.karbosguide.com*
Microsoft Technical Resources	*support.microsoft.com*
PC Today Online	*www.pctoday.com*
PC World	*www.pcworld.com*
Tom's Hardware Guide	*www.tomshardware.com*
WebMediaBrands	*www.webopedia.com*
ZDNet (publishes several technical magazines)	*www.zdnet.com*

Table 11-3   Web sites of technical information

>> *REAL PROBLEMS, REAL SOLUTIONS*

REAL PROBLEM 11-1: Troubleshooting PC Problems for Friends and Family

You have learned much about PC troubleshooting and repair already in this book. Now it's time to try your hand at some real-life troubleshooting. Make yourself available to family and friends to help them with their computer problems. For the first three problems you tackle, keep notes that describe the initial problem, what you did to solve it or to escalate it to others, and the outcome. Then answer the following questions:

1. List what you learned about technology from these three problems.

2. List what you learned about working with people when helping them with these three problems.

3. What one thing will you do differently when faced with similar problems?

4. What is something that you recognize you need to know, that you don't yet know, about PC troubleshooting that would have helped you with these three problems?