CHAPTER 17

Maintaining and Troubleshooting Windows

In this chapter, you will learn how to

- Maintain Windows
- Optimize Windows
- Troubleshoot Windows

Every computer running a Windows operating system requires occasional optimization to keep the system running snappily, ongoing maintenance to make sure nothing goes wrong, and troubleshooting when the system doesn't work correctly. Not that long ago, Windows had a bad rap as being difficult to maintain and challenging when troubleshooting problems. That's no longer true. Microsoft used its decades of experience with operating systems to search for ways to make the tasks of maintaining and troubleshooting less onerous. They've done such a good job with the latest versions of Windows that, out of the box, they are easy to optimize and maintain, although troubleshooting—and all operating systems share this—is still a bit of a challenge.

The chapter starts with maintenance and optimization, so let's make sure you know what these two terms mean. *Maintenance* means jobs you do from time to time to keep Windows running well, such as running hard drive utilities. CompTIA sees *optimization* as jobs you do to your Windows system to make it better—a good example is adding RAM. This chapter covers the standard maintenance and optimization activities performed on Windows and the tools techs use to perform them.

The last part of this chapter dives into *troubleshooting* Windows, examining steps you can take to bring a system back from the brink of disaster. You'll learn techniques for recovering a PC that won't boot and a PC that almost boots into Windows but fails.

Essentials

Maintaining Windows

Maintaining Windows can be compared to maintaining a new automobile. Of course, a new automobile comes with a warranty, so most of us just take it to the dealer to get work done. In this case, *you* are the mechanic, so you need to think as an auto mechanic would think. First, an auto mechanic needs to apply recalls when the automaker finds a serious problem. For a PC tech, that means keeping the system patches announced by Microsoft up to date. You also need to check on the parts that wear down over time. On a car that might mean changing the oil or rotating the tires. In a Windows system that includes keeping the hard drive and Registry organized and uncluttered.

Patches, Updates, and Service Packs

Updating Windows has been an important, but often neglected, task for computer users. Typically, Microsoft finds and corrects problems with its software and releases patches on the second Tuesday of every month. Sadly, because earlier versions of Windows let users decide when, if ever, to update their computers, the net result could be disastrous. The Blaster worm hammered computers all over the world in the summer of 2003, causing thousands of computers to start rebooting spontaneously—no small feat for a tiny piece of programming! Blaster exploited a flaw in Windows 2000/XP and spread like wildfire, but Microsoft had *already corrected* the flaw with a security update weeks earlier. If users had simply updated their computers, the virus would not have caused such widespread damage.

EXAM TIP You might be asked about installing service packs and patches on the CompTIA A+ 220-701 and 220-702 exams. Pay attention to the steps listed here.

The Internet has enabled Microsoft to make updates available, and *Windows Update* can grab those updates and patch user systems easily and automatically. Even if you don't want to allow Windows Update to patch your computer automatically, it'll nag you about updates until you patch your system. Microsoft provides the Windows Update service for all versions of Windows.

Once Microsoft released Service Pack 2 for Windows XP, it began pushing for wholesale acceptance of automatic updates from Windows Update. You can also start Windows Update manually. When your computer is connected to the Internet, start the utility in Windows 2000 by selecting Start | Windows Update. In Windows XP/Vista/7 you will find it at Start | All Programs | Windows Update. When you run Windows Update manually, the software connects to the Microsoft Web site and scans your computer to determine what updates you may need. Within a few seconds or minutes, depending on your connection speed, you'll get a straightforward screen like the one shown in Figure 17-1.

You have several choices here, although two are most obvious. If you click the Express button, Windows Update will grab any high-priority updates—these are security

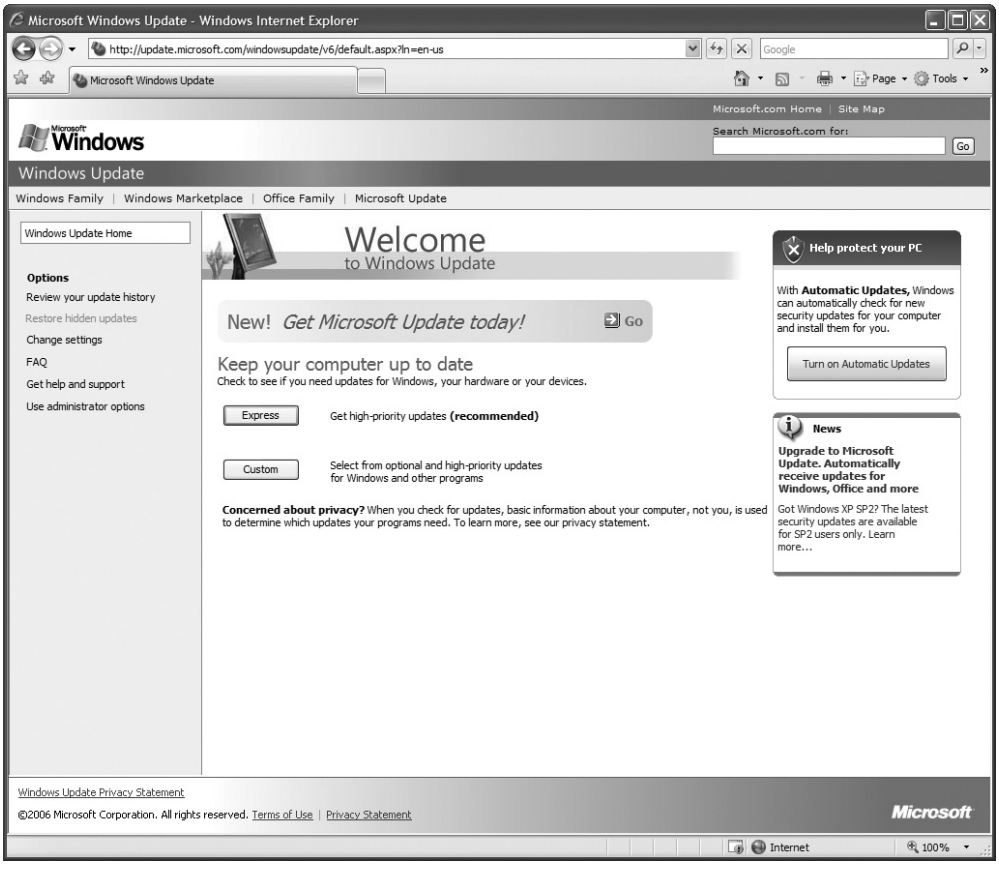


Figure 17-1 Microsoft Windows Update page

patches—and install them on your computer. If you click the Custom button, you can select from a list of optional updates.

Figure 17-2 shows the updater with a list of patches and security updates. You can scroll through the list and review the description of each update. You can deselect the checkbox next to a patch or update, and Windows Update will not download or install it. If you click the Clear All button, as you might suspect, all the updates will be removed from the list. When you click Install Updates, all the updates remaining in the list will be installed.

Automatic Updates

Updates are so important that Microsoft gives you the option to update Windows automatically through the *Automatic Updates* feature. Actually, it nags you about it! Soon after installing Windows (a day or two, in my experience), a message balloon will pop up from the taskbar suggesting that you automate updates. If you click this balloon, the Automatic Updates Setup Wizard runs, with which you can configure the update program.

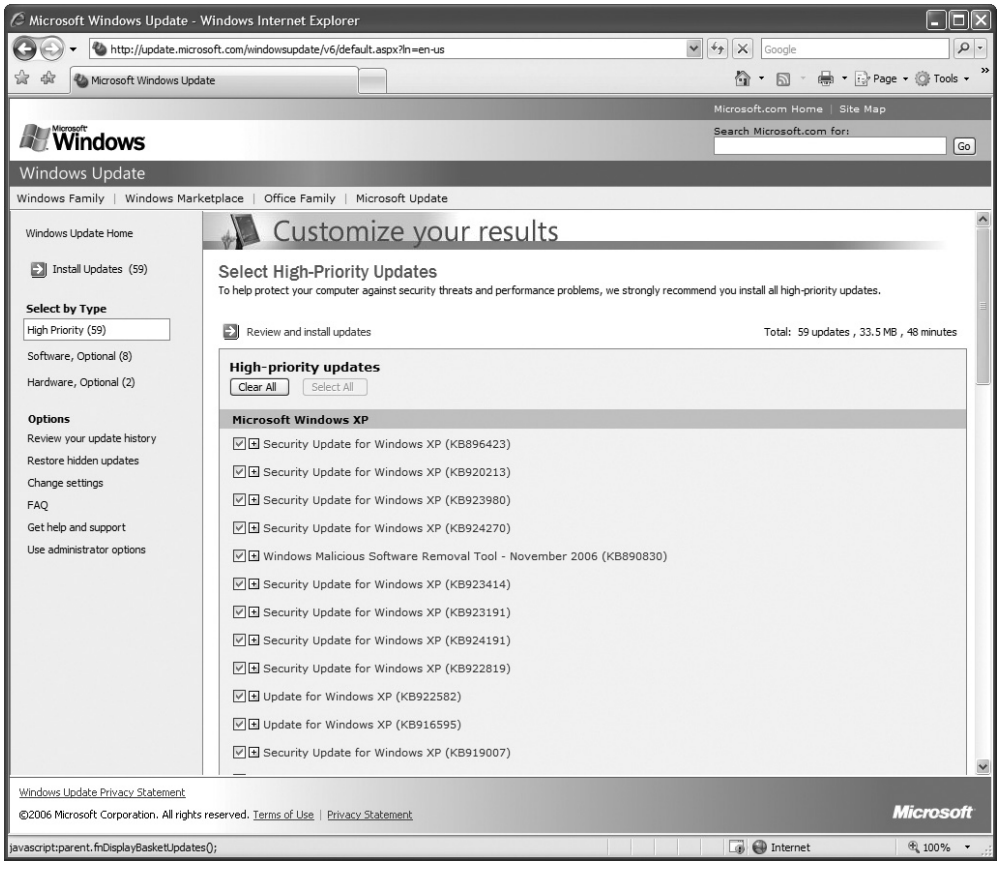


Figure 17-2 Choose updates to be installed

You say you've never seen this message balloon but would like to automate the update process? No problem. In Windows 2000 and XP, simply right-click My Computer (on the Start menu), select Properties, click the Automatic Updates tab, and select Automatic Update options. Or, open the Control Panel and double-click the Automatic Updates icon. In Windows Vista, go to Start | Windows Update to open the Windows Update dialog box. Click the Change settings menu item on the left for options. Whenever your computer connects to the Web, it checks the Windows Update page. What happens next depends on the setting you choose. You have four choices:

- **Automatic (recommended)** or **Install updates automatically (recommended)** Windows Update will simply keep your computer patched up and ready to go. This is the best option for most users, although not necessarily good for users of portable computers. Nobody wants to log into a slow hotel dial-up connection and have most of your bandwidth sucked away by Automatic Update downloading hot fixes!

- **Download updates…** Windows Update downloads all patches in the background and then, when complete, tells you about them. You have the option at that point to install or not install.
- **Notify me…** or **Check for updates…** Windows Update simply flashes a dialog box that tells you updates are available but does not download anything until you say go. This is the best option for users of portable computers. You can download files when it's convenient for you, such as when you're home rather than traveling on business.
- **Turn off Automatic Updates** or **Never check for updates (not recommended)** This does precisely what is advertised. You get neither automatic patches nor notification that patches are available. Only use this option on a system that does not or cannot connect to the Internet. If you're online, your computer needs to be patched!

When Windows Update works the way Microsoft wants it to work, it scans the Microsoft Web site periodically, downloads important patches as they appear, and then installs them on your computer. If you opted for the download-but-don't-install option, Windows Update simply notifies you when updates are downloaded and ready to install (Figure 17-3).

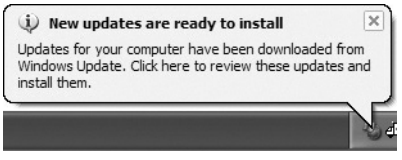


Figure 17-3 Windows Update balloon message

Windows Vista gives you the option—enabled by default—to have Windows Update include recommended updates along with important updates when it downloads or notifies you about their availability. If you've got a decent Internet connection, this can be a useful tool for keeping your drivers and such updated.

NOTE Microsoft offers the Microsoft Update tool (Windows XP) and the System Update Readiness Tool (Vista, 7) to help you determine if your system is ready to update to a newer version of Windows. You can obtain this tool from the Microsoft Web site.

Temporary File Management with Disk Cleanup

You should run the *Disk Cleanup* utility regularly to make sure you've cleared out the junk files that accumulate from daily use. All that late-night Web surfing doesn't just use up time; it also uses up disk space, leaving behind hundreds of temporary Internet files. Those, and other bits and pieces (such as those "deleted" files still hanging around in your Recycle Bin) can add up to a lot of wasted disk space if you don't periodically clean them out.

You can reach this tool through the Start menu (Start | All Programs | Accessories | System Tools), or you can open My Computer or Computer, right-click the drive you

want to clean up, and select Properties. Right there in the middle of the General tab, you'll find the Disk Cleanup button.

When you click the Disk Cleanup button, the application firsts calculates the space you can free up and then displays the Disk Cleanup dialog box, which tells you how much disk space it can free up—the total amount possible as well as the amount you'll get from each category of files it checks. Vista adds an extra feature when you click the Disk Cleanup button, asking if you wish to clean up all the files on the computer or just your files. In Figure 17-4, the list of files to delete only has a few categories checked, and the actual amount of disk space to be gained by allowing Disk Cleanup to delete these files is much smaller than the estimate. As you select and deselect choices, watch this value change.

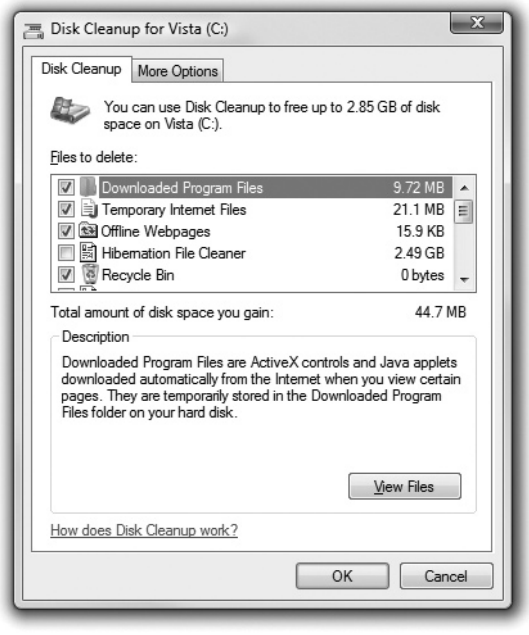


Figure 17-4 Disk Cleanup dialog box

If you scroll down through the list, you will see a choice to compress old files. What do you know, Disk Cleanup does more than just delete files? In fact, this file compression trick is where Disk Cleanup really, uh, cleans up. This is one of the few choices where you will gain the most space. The other big heavyweight category is Temporary Internet Files, which Disk Cleanup will delete. Try Disk Cleanup on a computer that gets hours of Internet use every day and you'll be pleased with the results.

Registry Maintenance

Your Registry is a huge database that Windows updates every time you add a new application or hardware or make changes to existing applications or hardware. As a result, the Registry tends to be clogged with entries that are no longer valid. These usually

don't cause any problems directly, but they can slow down your system. Interestingly, Microsoft does not provide a utility to clean up the Registry. To clean your Registry, you need to turn to a third-party utility. Quite a few Registry cleaner programs are out there, but my favorite is the freeware CCleaner by Piriform. You can download the latest copy at www.ccleaner.com/.

Before you start cleaning your Registry with wild abandon, keep in mind that all Registry cleaners are risky in that it may delete something you want in the Registry. Because Microsoft makes changes to the Registry for every version of Windows, make sure your utility supports the Windows version you're running. This is especially true for any 64-bit version of Windows! I've used CCleaner for a while and it has worked well for me—your experience may differ.

NOTE CCleaner also helps clean all of the most common Web browser and a number of popular applications.

Security: Spyware/Antivirus/Firewall

You simply cannot run a computer today without a large number of security programs to protect you from malicious attacks from spyware, malware, viruses, and hacking. In fact, the installation, monitoring, and updating of these programs (and possibly even hardware) is so important that they get their own chapter. Head to Chapter 26, "Securing Computers," for a complete discussion of how to keep your computer safe!

Error-Checking and Disk Defragmentation

Keeping drives healthy and happy is a key task for every tech. Error-checking and Disk Defragmenter, discussed way back in Chapter 12, "Implementing Hard Drives," are the key Windows maintenance tools used to accomplish this task.

When you can't find a software reason (and there are many possible ones) for a problem such as a system freezing on shutdown, the problem might be the actual physical hard drive. The tool to investigate that is Error-checking. You can perform Error-checking by using the CHKDSK command from a command line, from the Start | Run dialog box, or by using Start | Start Search. You can also access the tool through the GUI by opening My Computer or Computer, right-clicking on the drive you want to check, selecting Properties, and then clicking the Tools tab. Click Check Now to have Error-checking scan the drive for bad sectors, lost clusters, and similar problems, and repair them if possible.

Run the Disk Defragmenter (Figure 17-5) on a regular basis to keep your system from slowing down due to files being scattered in pieces on your hard drive. Before you click the Defragment button, click the Analyze button to have Windows analyze the disk and determine if defragmentation is actually necessary. If you use Vista/7, your system is defragged automatically.

Error-checking and Disk Defragmenter are such critical maintenance features that you really should have them run automatically. Take a moment to see how to schedule these and other critical jobs.

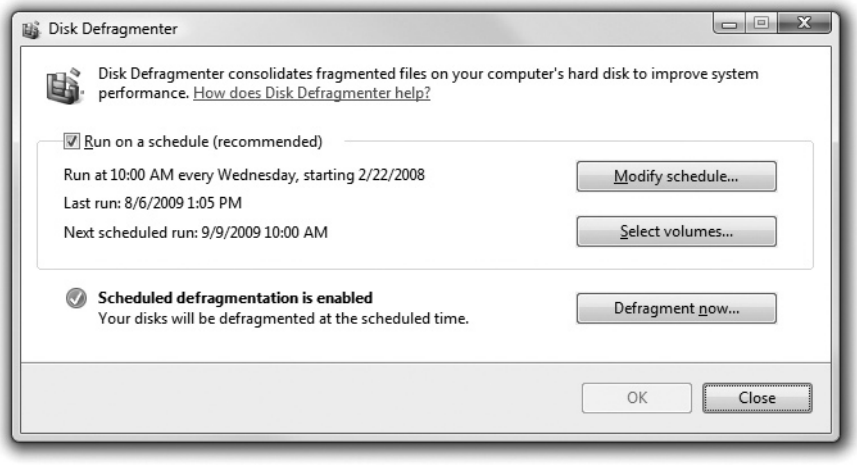


Figure 17-5 Vista Disk Defragmenter

Scheduling Maintenance

Maintenance only works properly when you do it at regular intervals. Depending on the version of Windows installed, you can schedule maintenance jobs to run automatically. The CompTIA exam objectives define three areas for you to consider for scheduled maintenance: Defragmentation, Scandisk/Check Disk, and Startup programs. For the most part, we use the Task Scheduler, although this depends on the task and the version of Windows.

Task Scheduler/Scheduled Tasks

Two versions of Task Scheduler are available: Windows 2000 and XP run Version 1.0, and Vista/7 run Version 2.0. Microsoft called it Scheduled Tasks in Windows 2000/XP, but reverted to Task Scheduler in Windows Vista. In both versions you can choose an executable program and define when you want that program to run. Figures 17.6 and 17.7 show Scheduled Tasks running a backup at a certain time of day.

Version 2.0 is much more powerful and flexible, dividing tasks into triggers, actions, and conditions. *Triggers* are actions or schedules that start a program. *Actions* are steps that define both the program to run and how it is to run. *Conditions* are extra criteria that must be met for the program to run. (Is the system idle? Is it connected to the Internet?) Figure 17-8 shows the Conditions tab for a sample task.

To open Task Scheduler, go to Start | All Programs or Programs | Accessories | System Tools | Task Scheduler or Scheduled Tasks. Note the variation in the name of the utility in the Start menu options.

The key to running scheduled maintenance is to know the names of the executable programs and any special switches you may need to enter. As we go through each of these I'll show you the names.

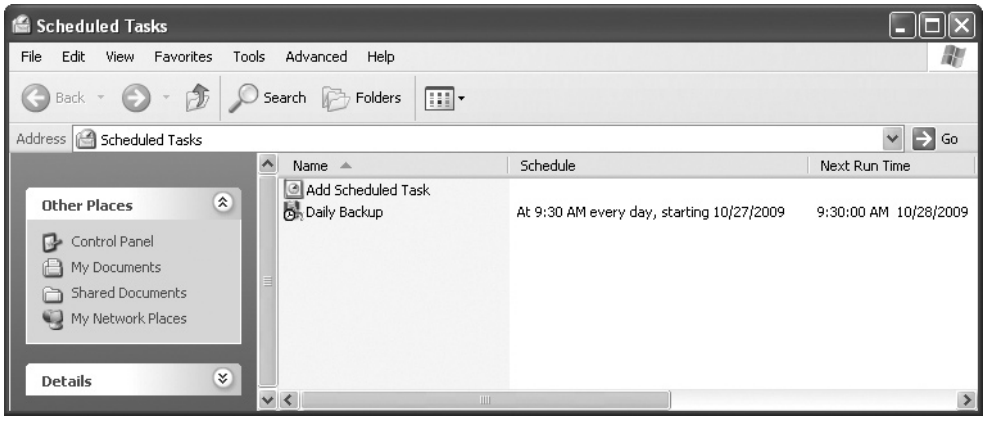
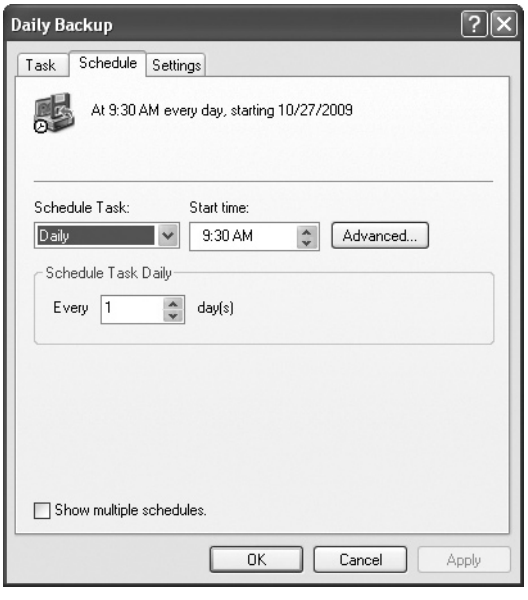


Figure 17-6 Windows XP Scheduled Tasks (Version 1.0)

Figure 17-7 Daily Backup Schedule in Windows XP



EXAM TIP The CompTIA A+ exams may use either name for the utility for scheduling maintenance in Windows. Remember that Windows 2000 and Windows XP label the tool *Scheduled Tasks*; Windows Vista (and Windows 7) label it *Task Scheduler*.

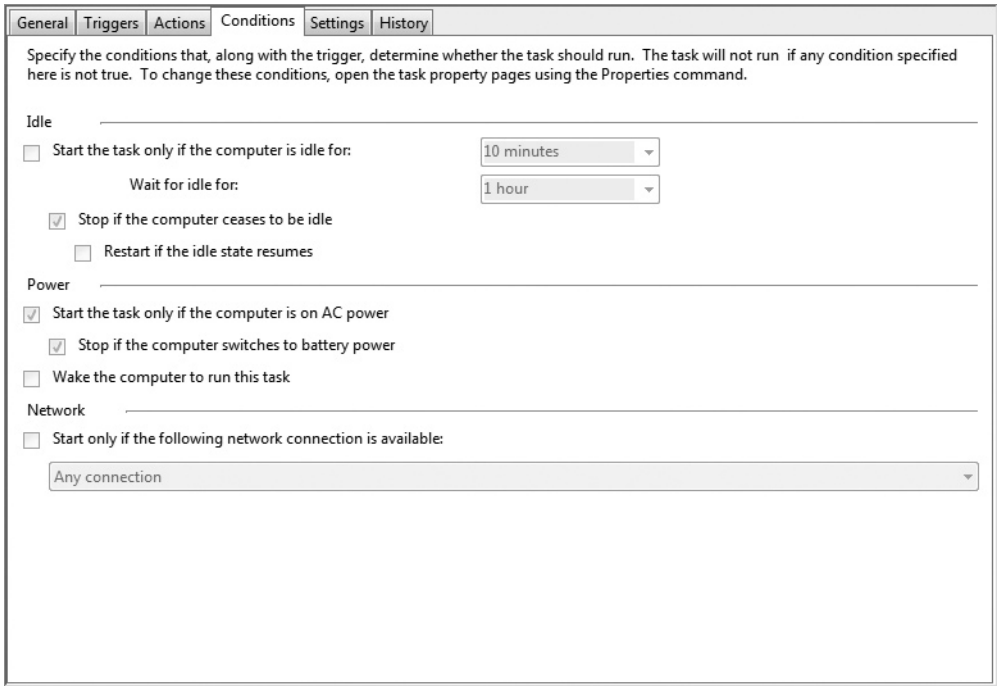


Figure 17-8 Conditions tab in the Windows Vista Task Scheduler (Version 2.0)

Defragmentation

To defragment, you need to run Disk Defragmenter (as you know), so you'll look for the executable file called defrag.exe. In Windows 2000 and XP, open Scheduled Tasks, browse for defrag.exe, and then add the drive you want to defragment, as shown in Figure 17-9.

If you use Windows Vista/7 and want to change when Disk Defragmenter runs (or turn it off completely), open the Start menu, type **defrag,** and press ENTER (Figure 17-10). You can start defragging right away or modify/disable the task on the Disk Defragmenter: Modify Schedule dialog box.

It's best to run Disk Defragmenter every evening if possible. If you're using Vista, take advantage of the "only run when idle" condition to keep Disk Defragmenter from interrupting possibly more important tasks.

EXAM TIP The CompTIA exams call the Disk Defragmenter program "Defrag," the common tech slang term for it.

Error-checking (Scandisk and Check Disk)

The tool you know and love as Error-checking appears on the CompTIA A+ competencies as *Scandisk* and *Check Disk*. (Neither tool exists on modern versions of Windows.)

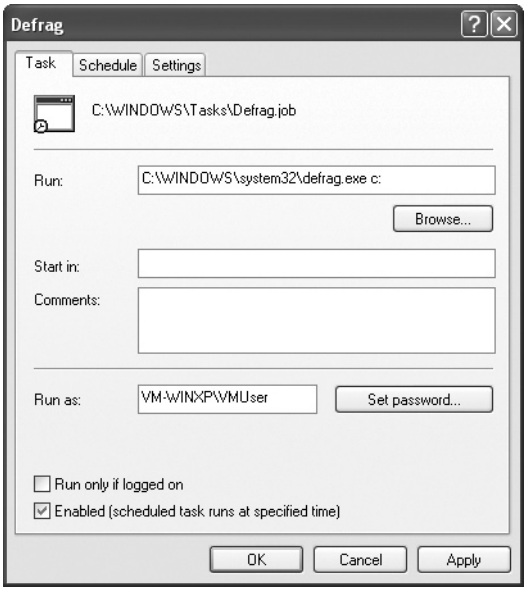


Figure 17-9 Scheduling a disk defragmentation in Windows XP

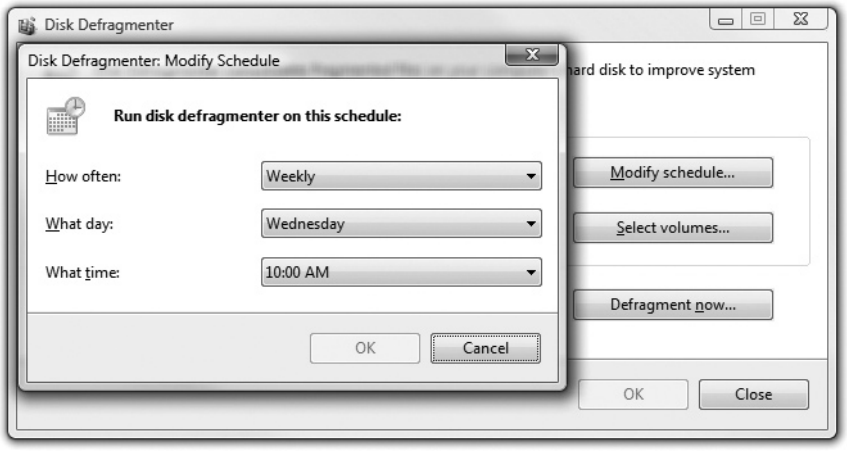


Figure 17-10 Vista's Disk Defragmenter Schedule

Regardless of what you call Error-checking, setting up Task Scheduler to run it automatically is a good thing.

NOTE No versions of Windows run Error-checking automatically, so you'll need to set up a task on the computer if you wish to do so.

Using the technique you just learned to set up a scheduled task with Disk Defragmenter, create another scheduled task to run Error-checking. Its executable is called chkdsk.exe (Figure 17-11). There are two switches you should use: /F to repair sectors and /R to tell Error-checking to attempt to recover data on known bad sectors.

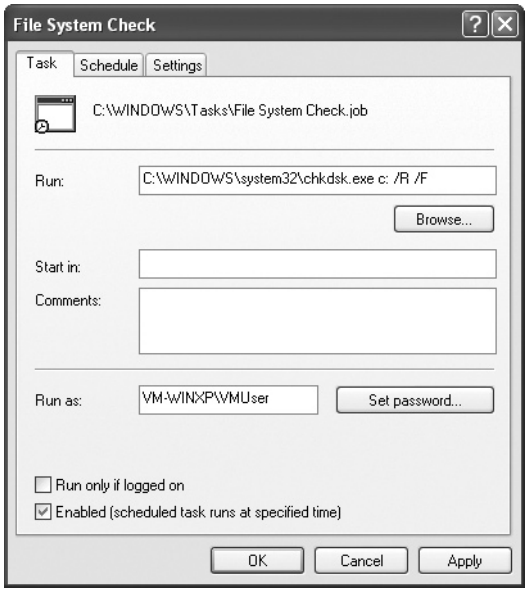


Figure 17-11 Scheduling Error-checking in Windows XP

Opinions vary on how often you should run Error-checking as a scheduled task. For the CompTIA exams, a monthly check is a good idea. For the real world, you should run Error-checking when you suspect a problem with your drives.

Startup Programs

Techs use the *System Configuration utility* to edit and troubleshoot operating system and program startup processes and services. It has been available in all Windows operating systems except Windows 95 and Windows 2000. Prior to Windows Vista, the System Configuration utility offered quick access to troubleshoot and edit the boot.ini file. It still offers some of these features in Vista, such as the capability to disable or enable troublesome or unwanted services and startup items. The BCD data store is used in place of the boot.ini in Windows Vista, however, so you obviously cannot use the System Configuration utility to edit the boot.ini in Vista.

To start the System Configuration utility, go to Start | Run or Start | Start Search, enter **msconfig**, and click OK or press ENTER (Figure 17-12). The program will run automatically in Windows XP; in Vista you may need to provide the necessary credentials or response, depending on the User Account Control (UAC) setup.

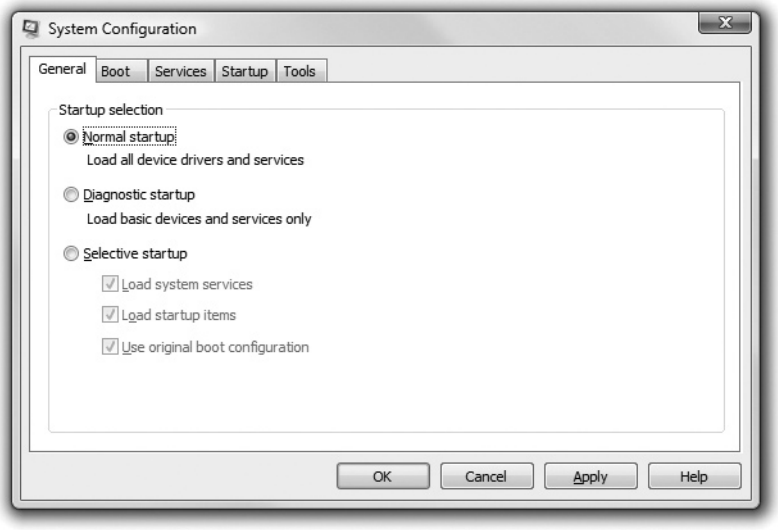


Figure 17-12 The Windows Vista System Configuration utility

EXAM TIP You should remember that you can configure the System Configuration utility with startup selections for troubleshooting. After using the System Configuration utility to change your startup programs, you can choose Normal startup to load all drivers and services. A Diagnostic startup loads basic services only, and a Selective startup enables you to select which system services and startup items to load on startup.

Optimizing Windows

Maintenance is about keeping Windows' performance from degrading with time and use. Of course, you don't just want to keep trouble at bay—you want to make your systems better, stronger, faster! Anything you do that makes Windows better than it was before, such as adding a piece of software or hardware to make something run better, is an optimization.

Installing and Removing Software

Probably the most common optimization performed on any PC is adding and removing applications. Installing and removing software is part of the normal life of any PC. Each time you add or remove software, you are making changes and decisions that can affect the system beyond whatever the program does, so it pays to know how to do it right.

System Information

Windows comes with a handy built-in utility known as the *System Information tool* (Figure 17-13) that collects information about hardware resources, components, and the software environment. When it finishes doing that, it provides a nice and tidy little report,

enabling you to troubleshoot and diagnose any issues and conflicts. As with many other tools you can access from the Start | Run or Start | Start Search dialog box, the CompTIA A+ exams refer to System Information by its executable, *MSINFO32*.

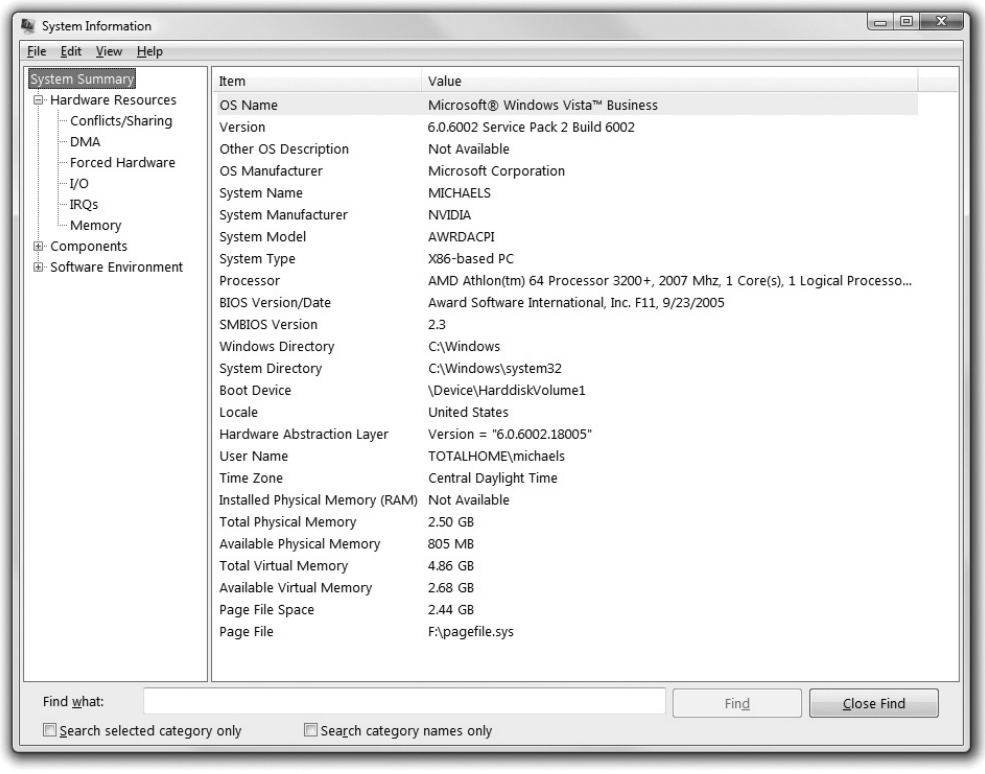


Figure 17-13 System Information

You can start System Information in one of the following ways:

- Choose Start | Programs or All Programs | Accessories | System Tools | System Information.
- In Windows XP, click Start, click Run, and then type **msinfo32** and click OK. In Windows Vista, open the Start Search box, type **msinfo32**, and press ENTER.

It is also important to note that you can use System Information to gather information about remote computers by selecting View | Remote Computer and then entering the remote computer's network machine name. Under Tools, you even get quick access to System Restore and the DirectX Diagnostic Tool, a tool for checking your video card that Chapter 19, "Video," discusses.

Installing Software

Most application programs are distributed on optical discs (although this is slowly changing). Windows supports *Autorun*, a feature that enables the operating system to look for and read a special file called—wait for it—autorun.inf. Immediately after a removable media device (optical disc or thumb drive) is inserted into your computer, whatever program is listed in autorun.inf runs automatically. Most application programs distributed on removable media have an autorun file that calls up the installation program.

Sometimes, however, you need to institute the installation sequence yourself. Perhaps the installation disc lacks an Autorun installation program, or perhaps Windows is configured so that you must start programs on optical discs manually. In some cases, a disc may contain more than one program, and you must choose which of them to install. Regardless of the reason, beginning the installation manually is a simple and straightforward process of using the *Add or Remove Programs* applet in the Control Panel in Windows XP. Windows 2000 calls the applet Add/Remove Programs. Click the Add New Programs button (Figure 17-14), follow the prompts, and provide the media or location of the files. In Windows Vista and 7, Microsoft has replaced the Add or Remove Programs applet with *Programs and Features*, which does not have the Add New Programs feature.

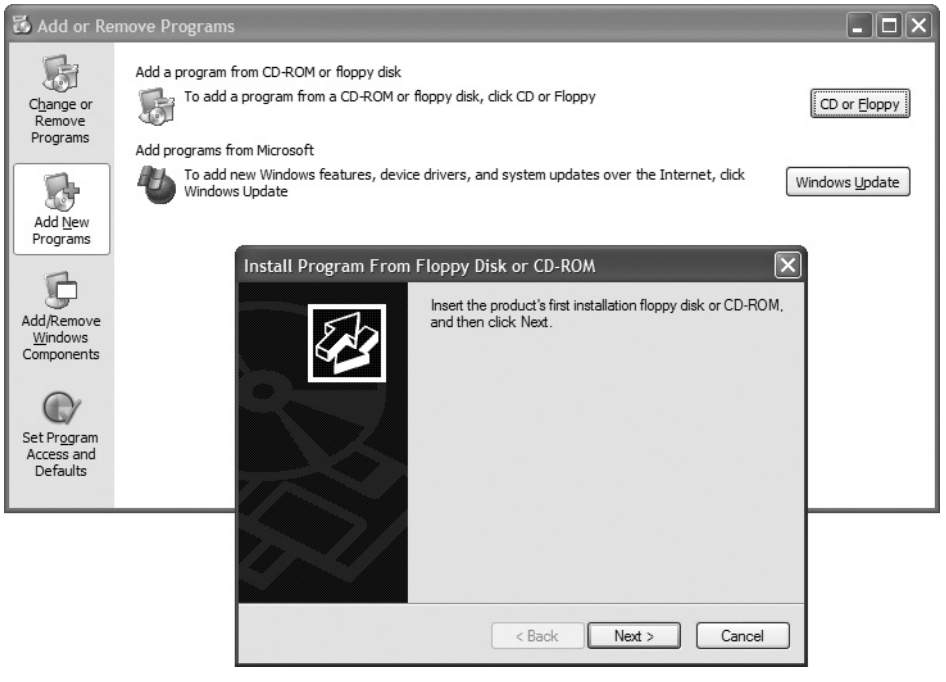


Figure 17-14 Add New Programs

If you have sufficient permissions to install an application—your account is a member of the Administrators group in Windows 2000, for example, or is an Administrator Account in Windows XP and up—the application will begin its installation routine. If you don't have sufficient permissions to install an application, Windows will stop the installation.

With Windows Vista/7, UAC complicates the installation process a bit. You will most likely be prompted by UAC when installing an application to give you time to review what is happening to your system in case you did not approve of the program being installed. If you are using an administrator account, you can simply click Continue and finish the installation. Should you be logged in with a less privileged account, you will need to enter a user name and password of an account with administrative privileges. Some installers have trouble letting UAC know that they need more privileges and simply fail no matter what account you are logged in with. In those cases it is best to right-click the installer icon and select Run as Administrator to give the installer the access it expects from the start.

Assuming all is well, you typically first must accept the terms of a software license before you can install an application. These steps are not optional; the installation simply won't proceed until you accept all terms the software manufacturer requires and, in many cases, enter a correct code. You may also be asked to make several decisions during the installation process. For example, you may be asked where you would like to install the program and if you would like certain optional components installed. Generally speaking, it is best to accept the suggested settings unless you have a very specific reason for changing the defaults.

Removing Software

Each installed application program takes up space on your computer's hard drive, and programs that you no longer need simply waste space that could be used for other purposes. Removing unnecessary programs can be an important piece of optimization.

You remove a program from a Windows PC in much the same manner as you install it. That is, you use the application's own uninstall program, when possible. You normally find the uninstall program listed under the application's icon on the Start Menu, as shown in Figure 17-15.

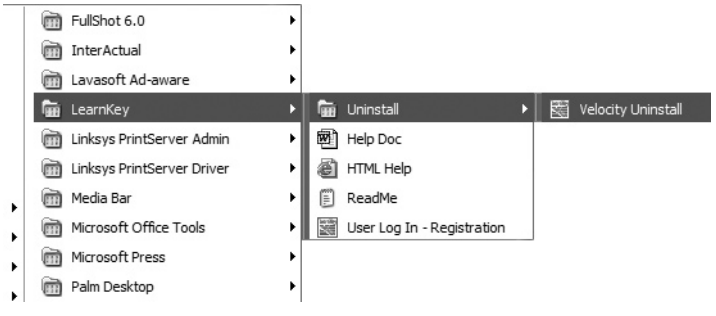


Figure 17-15 Uninstall me!

If an uninstall program is not available, use the appropriate Windows Control Panel applet to remove the software. Figure 17-16 shows this applet in Windows Vista. You select the program you want to remove and click the Uninstall/Change button or Change/Remove button. Windows displays a message warning you that the program will be permanently removed from your PC. If you're certain you want to continue, click Yes.

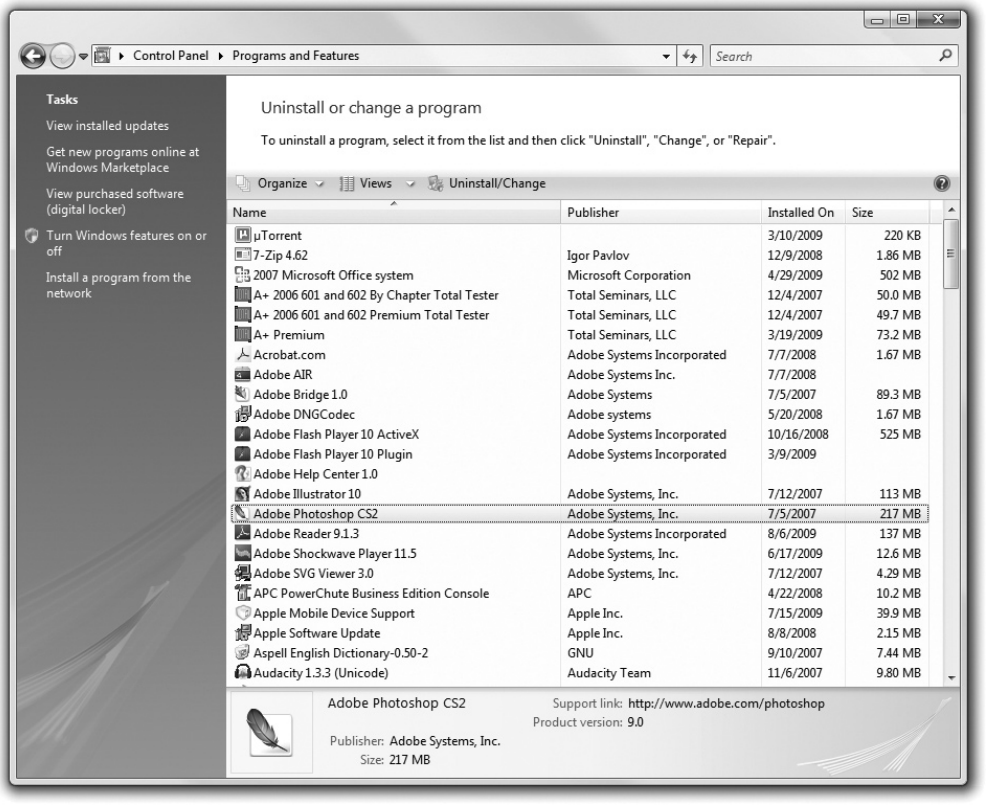


Figure 17-16 Programs and Features applet

You may then see a message telling you that a shared file that appears to no longer be in use is about to be deleted, and asking your approval. Generally speaking, it's safe to delete such files. If you do not delete them, they will likely be orphaned and remain unused on your hard disk forever. In some cases, clicking the Uninstall/Change or Change/Remove button starts the application's install program (the one you couldn't find before) so you can modify the installed features. This is a function of the program you're attempting to remove. The end result should be the removal of the application and all of its pieces and parts, including files and Registry entries.

Adding or Removing Windows Components/Features

When you installed Windows, it tried to guess which optional Windows components you would need. It installed Notepad, modem support, and games on your computer. You can remove these Windows components from your system if you like, and add other components as well. If you're adding components, you'll need a copy of your Windows CD/DVD, or another location where the Windows source files are stored. This task really hasn't changed from previous versions of Windows.

To add or remove a Windows component in Windows 2000/XP, open the Add/Remove Programs or Add or Remove Programs applet in the Control Panel. From here, select Add/Remove Windows Components, which opens the Windows Components Wizard (Figure 17-17). You can select an installed program here. You can see how frequently it is used, how much disk space it uses, and (sometimes) the last time it was used.

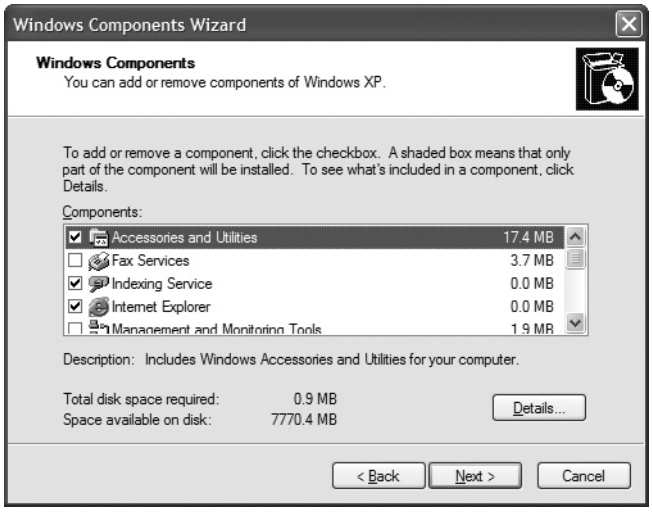


Figure 17-17 Windows Components Wizard

In Windows Vista/7, open the Programs and Features applet in the Control Panel, and then click the *Turn Windows features on or off* option on the Tasks list. Click Continue if prompted by UAC and you will be presented with the Windows Features dialog box (Figure 17-18). To toggle a feature on or off, simply click its checkbox. Unlike previous versions of Windows, you no longer need to have the installation disc to turn on features.

Installing/Optimizing a Device

The processes for optimizing hardware in Windows are absolutely identical, even down to the troubleshooting utilities, and are very similar to the steps for installing a new device. The installation process is covered in every chapter of this book that deals with

Figure 17-18 Windows Features dialog in Vista

one type of device or another, so this section concentrates on the issues that fit best under optimization.

EXAM TIP Both CompTIA A+ exams test you on installing and optimizing devices.

Driver Updates

Device manufacturers occasionally update their drivers. Most of these updates take place to fix problems, but many updates incorporate new features. Whatever the case, when one of your devices gets an updated driver, it's your job to install it. Windows/Microsoft Update provides an easy method to update drivers from manufacturers that take advantage of the service. If you are using Windows 2000 or XP, you usually need to select the Custom option to see these updates because the Express option only installs high-priority updates. When you click on the Custom option, look under Hardware, Optional (on the left) to see if Windows has any driver updates (Figure 17-19).

If you are using Vista/7, you will need to click *View available updates* to see if any drivers are available for your system. No matter what version of Windows you have, take some time to read what these updates do—sometimes you may choose not to install a driver update because it's not necessary or useful to your system.

If Windows does not put a driver update in the Windows Update tool, how do you know a device needs updating? The trick is to know your devices. Video card manufacturers update drivers quite often. Get in the habit of registering your video card with the manufacturer to stay up to date. Any very new device is also a good candidate for an update. When you buy that new cool toy for your system, make a point to head over to the manufacturer's Web site and see if any updates have come out since it was packaged for sale. That happens more often than you might think!

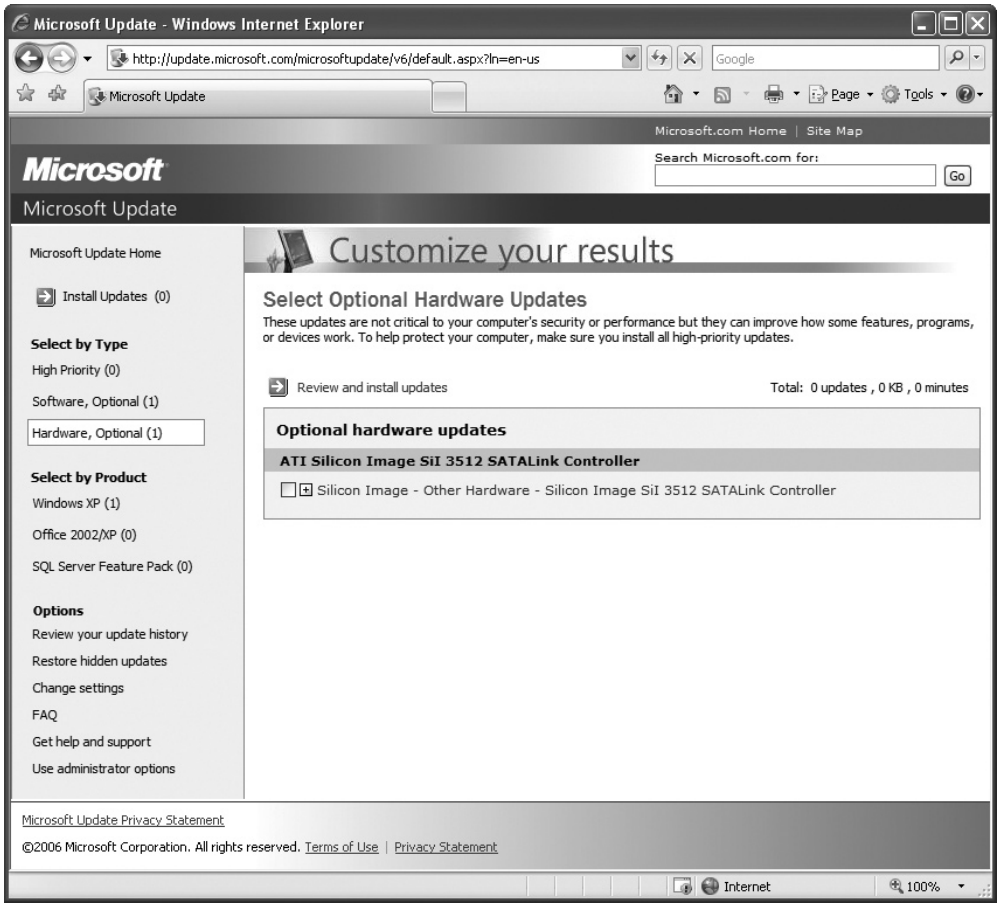


Figure 17-19 Optional Hardware updates

Driver Signing

Device drivers become part of the operating system and thus have the potential to cause lots of problems if they're written poorly. To protect Windows systems from bad device drivers, Microsoft uses *driver signing*, which means that each driver has a digital signature. Any drivers included on the Windows installation media or at the Windows Update Web site are digitally signed. Once you have installed a driver, you can look at its Properties to confirm that it was digitally signed. Figure 17-20 shows a digitally signed network card driver.

When an unsigned driver is detected during hardware installation, you'll see the message in Figure 17-21 offering you the choice to stop or continue the installation. Signed drivers are more or less a sure thing, but that doesn't mean unsigned ones are a problem—just consider the source of the driver and ensure that your device works properly after installation.

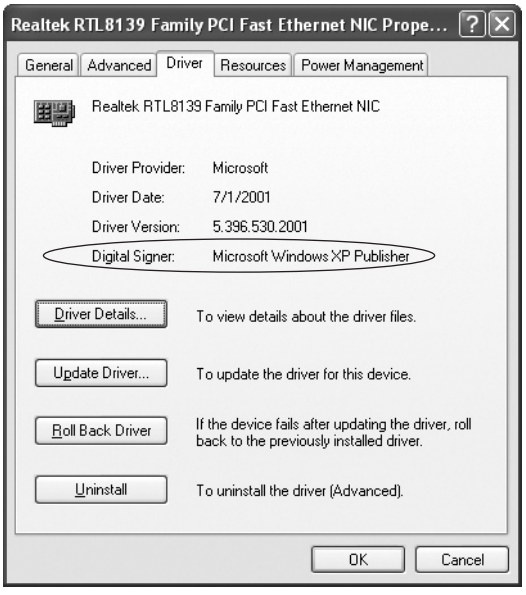


Figure 17-20
A digitally signed driver

Figure 17-21
Stop or continue installation of an unsigned driver

You can control how Windows behaves when drivers are being installed. Click the Driver Signing button on the Hardware tab of the System Properties dialog box to display the Driver Signing Options dialog box shown in Figure 17-22. If you select Ignore, Windows will install an unsigned driver without warning you. If you select Warn, you will be prompted when Windows detects an unsigned driver during driver installation, and you will be given the opportunity to either stop or continue the installation. Choosing Block will prevent the installation of unsigned drivers.

The default Driver Signing setting is Warn. This also is the default setting during installation, so you will always be warned when Windows detects an unsigned driver during

Figure 17-22 Driver Signing Options dialog box

Windows installation. This is no problem for a standard installation, when you are sitting at the computer, responding to all prompts—but it is a problem for automated, unattended installations. This is a good reason to check out all your device drivers before installing Windows. In 64-bit versions of Windows, all drivers must be signed. No exceptions. Microsoft wants to keep tight controls on the drivers to improve stability.

Device Manager

You've worked with *Device Manager* in other chapters when installing and troubleshooting devices; it's also the tool to use when optimizing device drivers. Right-click on a device in Device Manager to display the context menu. From here you can update or uninstall the driver, disable the device, scan for hardware changes, or display the Properties dialog box. When you open the Properties dialog box, you'll see several tabs that vary according to the specific device. Most have General, Driver, Details, and Resources. The tab that matters most for optimization is the Driver tab.

The Driver tab has buttons labeled Driver Details, Update Driver, Roll Back Driver, and Uninstall. Driver Details lists the driver files and their locations on disk. Update Driver opens the Hardware Update Wizard—not very useful given that the installation programs for almost all drivers do this automatically. The Roll Back Driver option is a different story. It enables you to remove an updated driver, thus rolling back to the previous driver version. Roll Back Driver (Figure 17-23) is a lifesaver when you install a new driver and suddenly discover it's worse than the driver it replaced! Uninstall removes the driver.

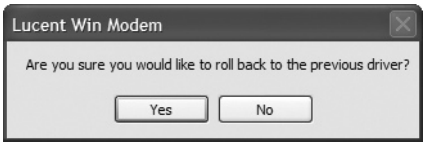


Figure 17-23 Rolling back to the previous driver

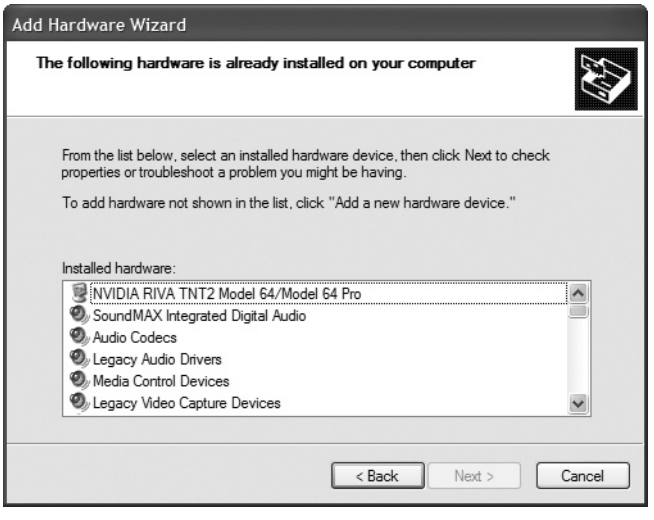
Adding a New Device

Windows should automatically detect any new device you install in your system. If Windows does not detect a newly connected device, use the Add Hardware Wizard or Add Hardware to get the device recognized and drivers installed (Figure 17-24). You'll find it on the Hardware tab of the System Properties dialog box.

Figure 17-24
Add Hardware Wizard

Click Next on the Welcome screen, and the wizard searches for hardware that has been connected but does not yet have a driver installed. If it detects the device, select it, and the wizard installs the driver. You may have to point to the source location for the driver files. If it does not detect the device, which is very likely, it will ask you if the hardware is connected. When you answer yes and click Next, it gives you a list of installed hardware, similar to Figure 17-25.

Figure 17-25
List of installed hardware



If the device is in the list, select it and click Next. If not, scroll to the bottom and select *Add a new hardware device*, and then click Next. If the device is a printer, network card, or modem, select *Search for and install the hardware automatically* and click Next. In that case, once the wizard detects the device and installs the driver, you're finished. If you do see your device on the list, your best hope is to select *Install the hardware that I manually select from a list*. In the subsequent screens, select the appropriate device category, select the device manufacturer and the correct model, and respond to the prompts from the Add Hardware Wizard to complete the installation.

Performance Options

One optimization you can perform on all Windows versions is setting Performance Options. *Performance Options* are used to configure CPU, RAM, and virtual memory (page file) settings. To access these options in Windows 2000/XP, right-click My Computer and select Properties, click the Advanced tab, and click the Options button (Windows 2000) or Settings button (Windows XP) in the Performance section of that tab. In Windows Vista/7, right-click Computer and select Properties; then click the Advanced system settings option in the Tasks list. If you are prompted for an administrator password or confirmation, type the password or confirmation. Click on the Advanced tab and click the Settings button in the Performance section of that tab. Once you get to the Performance Options dialog box, its behavior differs between Windows 2000 and Windows XP/Vista (one of the few places where Vista acts the same as XP!).

In Windows 2000, the Performance Options dialog box shows a pair of radio buttons called Applications and Background Services. These radio buttons set how processor time is divided between the foreground application and all other background tasks. Set this to Applications if you run applications that need more processor time. Set it to Background Services to give all running programs the same processor usage. You can also adjust the size of the page file in this dialog box, but in most cases I don't mess with these settings and instead leave control of the page file to Windows.

The Windows XP/Vista Performance Options dialog box has three tabs: Visual Effects, Advanced, and Data Execution Prevention (Figure 17-26). The Visual Effects tab enables you to adjust visual effects that impact performance. Try clicking the top three choices in turn and watch the list of settings. Notice the tiny difference between the first two choices. The third choice, *Adjust for best performance*, turns off all visual effects, and the fourth option is an invitation to make your own adjustments. If you're on a computer that barely supports Windows XP, turning off visual effects can make a huge difference in the responsiveness of the computer. For the most part, though, just leave these settings alone.

The Advanced tab in Windows XP, shown in Figure 17-27, has three sections: Processor scheduling, Memory usage, and Virtual memory. Under the Processor scheduling section, you can choose to adjust for best performance of either Programs or Background services. The Memory usage settings enable you to allocate a greater share of memory to programs or to the system cache. The Virtual memory section of this tab enables you to modify the size and location of the page file. Microsoft dropped the Memory usage settings option in Windows Vista.

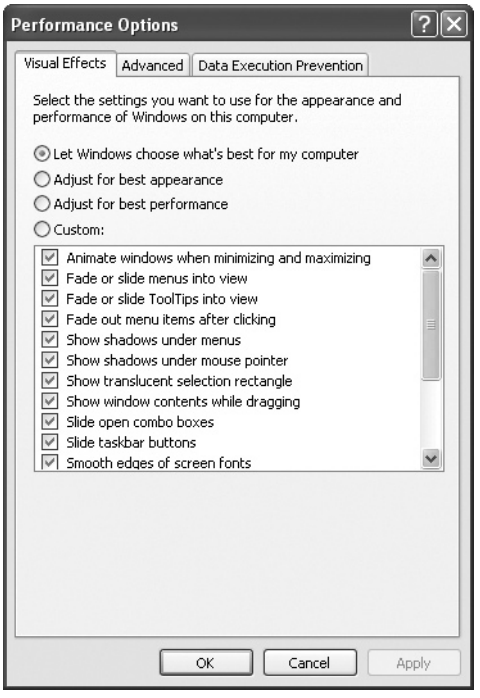


Figure 17-26 Windows XP Performance Options dialog box

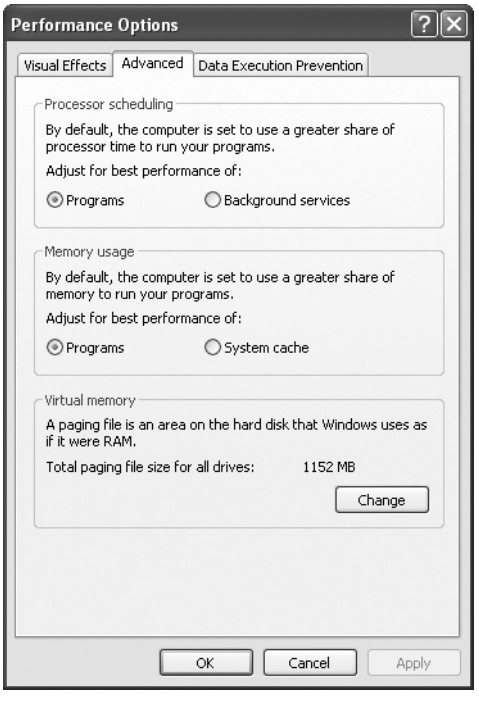


Figure 17-27 Advanced tab of Performance Options dialog box

Microsoft introduced *Data Execution Prevention* (*DEP*) with Windows XP Service Pack 2. DEP works in the background to stop viruses and other malware from taking over programs loaded in system memory. It doesn't prevent viruses from being installed on your computer, but makes them less effective. By default, DEP monitors only critical operating system files in RAM, but the Data Execution Prevention tab enables you to have DEP monitor all running programs. It works, but you'll take a performance hit. Like other options in the Performance Options dialog box, leaving the DEP settings as default is the best option most of the time.

Resource Tracking

One big issue with optimization is knowing when something needs optimization. Let's say your Windows computer seems to be running more slowly. Resource tracking is very important for identifying the performance problem. Task Manager and the Performance console are tools you can use to figure out what (if anything) has become a bottleneck.

Task Manager

The *Task Manager* has many uses. Most users are only aware of the Applications tab, used to shut down a troublesome program. For optimization purposes, Task Manager is a great tool for investigating how hard your RAM and CPU are working at any given moment and why. The quick way to open the Task Manager is to press CTRL-SHIFT-ESC. Click the Performance tab to reveal a handy screen with the most commonly used information: CPU usage, available physical memory, size of the disk cache, commit charge (memory for programs), and kernel memory (memory used by Windows). Figure 17-28 shows a system with a dual-core processor, which is why you see two screens under CPU Usage History. A system with a single-core processor would have a single screen.

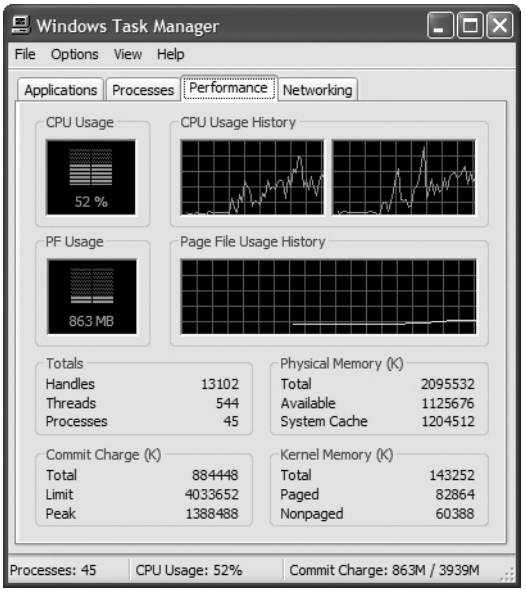


Figure 17-28 Task Manager

Not only does Task Manager tell you how much CPU and RAM usage is taking place, it also tells you what program is using those resources. Let's say your system is running slowly. You open up Task Manager and see that your CPU usage is at 100 percent. You then click on the Processes tab to see all the processes running on your system. Click on the CPU column heading to sort all processes by CPU usage to see who's hogging the CPU (Figure 17-29)! To shut off a process, just right-click the process and select End Process. Many times a single process opens many other processes. If you want to be thorough, click End Process Tree to turn off not only the one process but also any other processes it started.

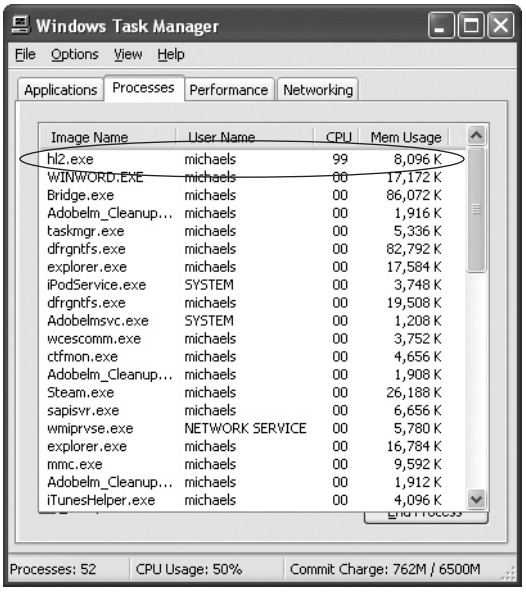


Figure 17-29
CPU usage

NOTE Every program that runs on your system is composed of one or more processes.

Task Manager is also a great tool for turning off processes that are hogging memory. Let's say you're experiencing a slowdown, but this time you also notice your hard drive light is flickering nonstop—a clear sign that you've run out of memory and the page file is now in use. You go into Task Manager and see no available system memory—now you *know* the page file is in use! To make the PC run faster, you have to start unloading programs—but which ones? By going into the Processes tab in Task Manager, you can see exactly which processes are using the most memory. Just be careful not to shut down processes you don't recognize; they might be something the computer needs.

Performance Console

Task Manager is good for identifying current problems, but what about problems that happen when you're not around? What if your system is always running at a CPU utilization of 20 percent—is that good or bad? Windows 2000 and XP provide a tool called the *Performance console* that logs resource usage so you can track items such as CPU and RAM usage over time. Performance is an MMC console file, PERFMON.MSC, so you call it from Start | Run or through the Performance icon in Administrative Tools. Use either method to open the Performance console (Figure 17-30). As you can see, there are two nodes, System Monitor and Performance Logs and Alerts.

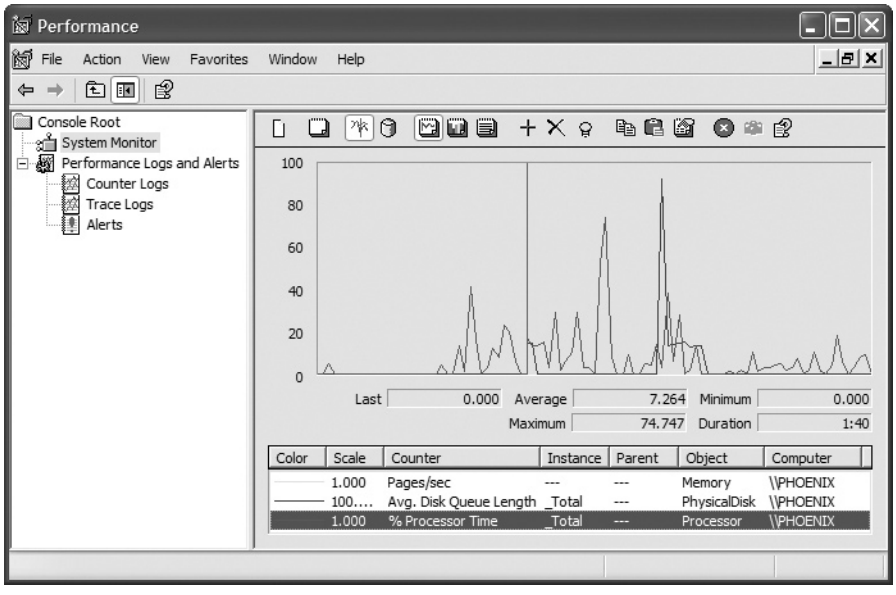


Figure 17-30 Performance console

Objects and Counters To begin working with the Performance console, you need to understand two terms: object and counter. An *object* is a system component that is given a set of characteristics and can be managed by the operating system as a single entity. A *counter* tracks specific information about an object. For example, the Processor object has a counter, %Processor Time, that tracks the percentage of elapsed time the processor uses to execute a non-idle thread. Many counters can be associated with an object.

System Monitor *System Monitor* gathers real-time data on objects such as memory, physical disk, processor, and network, and displays this data as a graph (line graph), histogram (bar graph), or simple report. Think of System Monitor as a more detailed, customizable Task Manager. When you first open the Performance console, the System

Monitor shows data in graph form. The data displayed is from the set of three counters listed below the chart. If you want to add counters, click the Add button (the one that looks like a plus sign) or press CTRL-I to open the Add Counters dialog box. Click the Performance object drop-down list and select one of the many different objects you can monitor. The Add Counters dialog box includes a helpful feature: you can select a counter and click the Explain button to learn about the counter, as in Figure 17-31. Try that now.

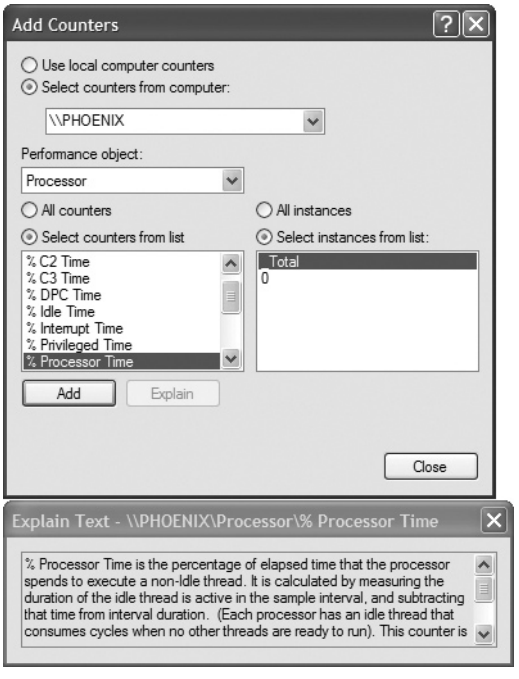


Figure 17-31 Add Counters dialog box

Even with just three counters selected, the graph can get a little busy. That's where one of my favorite System Monitor features shines. If you want the line of charted data from just one counter to stand out, select the counter in the list below the graph and then press CTRL-H. See how this trick makes the %Processor Time line stand out in Figure 17-32? Imagine how useful that is when you are monitoring a dozen counters.

Performance Logs and Alerts The *Performance Logs and Alerts* snap-in enables Windows to create a written record of just about anything that happens on your system. Do you want to know if someone is trying to log on to your system when you're not around? The following procedure is specific to Windows XP, but the steps are nearly identical in Windows 2000.

To create the new event log, right-click Counter Logs and select New Log Settings. Give the new log a name—in this example, "Unauthorized Accesses." Click OK, and a properties box for the new log appears, similar to that in Figure 17-33.

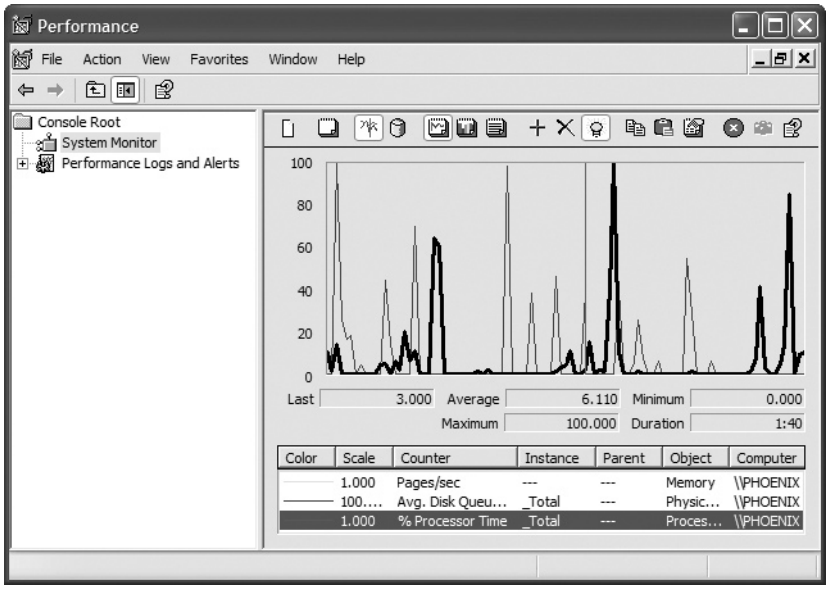
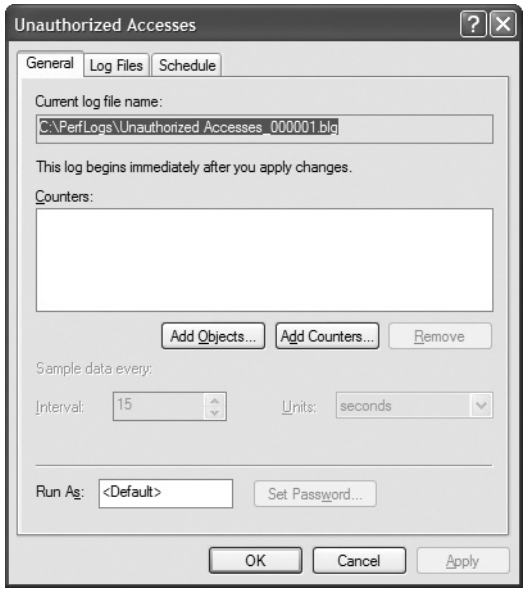


Figure 17-32 CTRL-H makes one set of data stand out

Figure 17-33 Creating a new performance log



To select counters for the log, click Add Counters and then select the *Use local computer counters* radio button. Select Server from the Performance object pull-down menu and then select Errors Logon from the list of counters; click Add and then click Close.

Back in the Properties box for your new log, click the Schedule tab and set up when you want this thing to start running—probably at the end of the workday today. Then select when it should stop logging—probably tomorrow morning when you start work. Click the Log Files tab to see where the log file will be saved—probably C:\PerfLogs—and make a note of the filename. The filename will consist of the name you gave the log and a number. In this example I named the new performance log "Unauthorized Accesses," so the filename is Unauthorized Accesses_000001.blg.

When you come back in the morning, open the Performance console, select Performance Logs and Alerts, and then select Counter Logs. Your log should be listed on the right. The icon by the log name will be green if the log is still running or red if it has stopped. If it has not stopped, select it and click the Stop button (the one with the black square, circled in Figure 17-34).

Figure 17-34 Stopping the performance log

To view the log, open the Performance console, select System Monitor, change to Report view, and load the file as a new source by using the Properties box.

Reliability and Performance Monitor Windows Vista improves on the old Performance console dramatically with the Reliability and Performance Monitor. The Reliability and Performance Monitor still has a complete Performance console with all the objects and counters you see in Windows 2000 and XP, but it adds an excellent Resource Overview, a Reliability Monitor and a much more flexible way to use counters with Data Collector Set and Reports.

NOTE A complete discussion of the Reliability and Performance Monitor is outside the scope of the CompTIA A+ objectives, but it's an amazing tool!

You can open Reliability and Performance Monitor in Windows Vista by starting the Performance Information and Tools in the Administrative Tools Control Panel applet to get the Resource Overview dialog box (Figure 17-35). You can also open the tool by going to Start | Start Searching, typing **perfmon.msc**, and pressing ENTER.

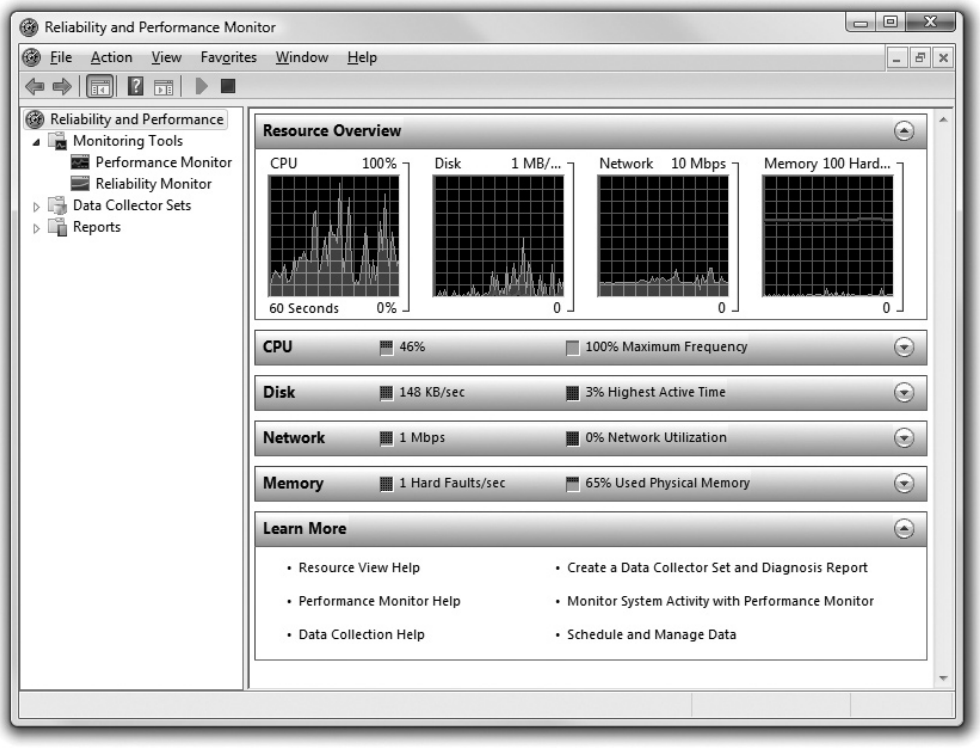


Figure 17-35 Resource Overview in Vista

Think of the Resource Overview as an advanced Task Manager, giving details on CPU, hard drive, network, and memory usage. When you click on one of the four bars, you get details on exactly which processes are using those resources—a powerful tool when you suspect a program might be hogging something! Figure 17-36 shows the Network bar opened to reveal the processes using the network and how much data each is sending.

The Reliability and Performance Monitor option you can select under the Monitoring Tools is simply a re-creation of the Performance console and works as described earlier for Windows 2000 and XP (Figure 17-37). This is a great tool for quick checks on specific counters.

Microsoft included Data Collector Sets in the Reliability and Performance Monitor, groupings of counters you can use to make reports. You can make you own Data Collector Sets (User Defined) or you can just grab one of the predefined system sets. Once you start a Data Collector Set, you can use the Reports option to see the results (Figure 17-38). Data Collector Sets not only enable you to choose counter objects to track, but they also enable you to schedule when you want them to run.

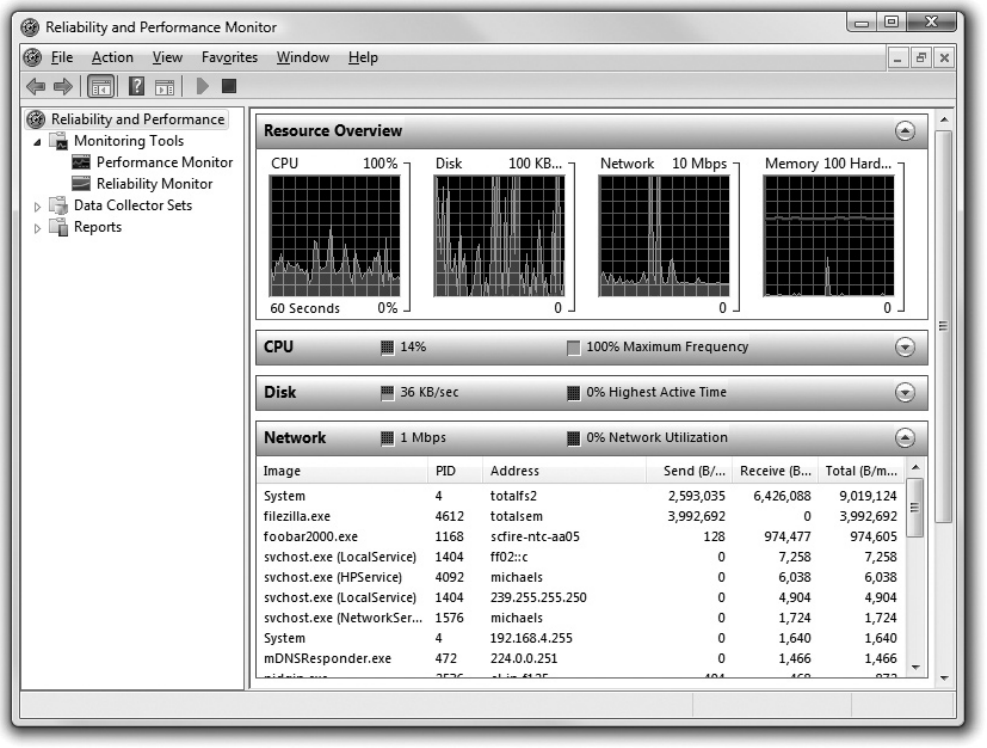


Figure 17-36 Network Bar in Reliability and Resource Monitor

EXAM TIP The CompTIA A+ exams aren't going to ask too many detailed questions on either Performance Monitor or Reliability and Performance Monitor. That doesn't mean you can ignore these amazing tools! Make sure you understand that these tools give you the power to inspect anything happening on your system to help you diagnose problems.

Preparing for Problems

As part of optimizing Windows, techs need to prepare for problems. You must have critical system files and data backed up and tools in place for the inevitable glitches. Different versions of Windows enable you to prepare for problems differently. Microsoft seems to break backups into certain areas: backing up personal data, backing up local copies of critical system state information, backing up a small amount of very critical system information on some form of removable media, and providing some way to use backups if your system won't boot. Let's see all of these.

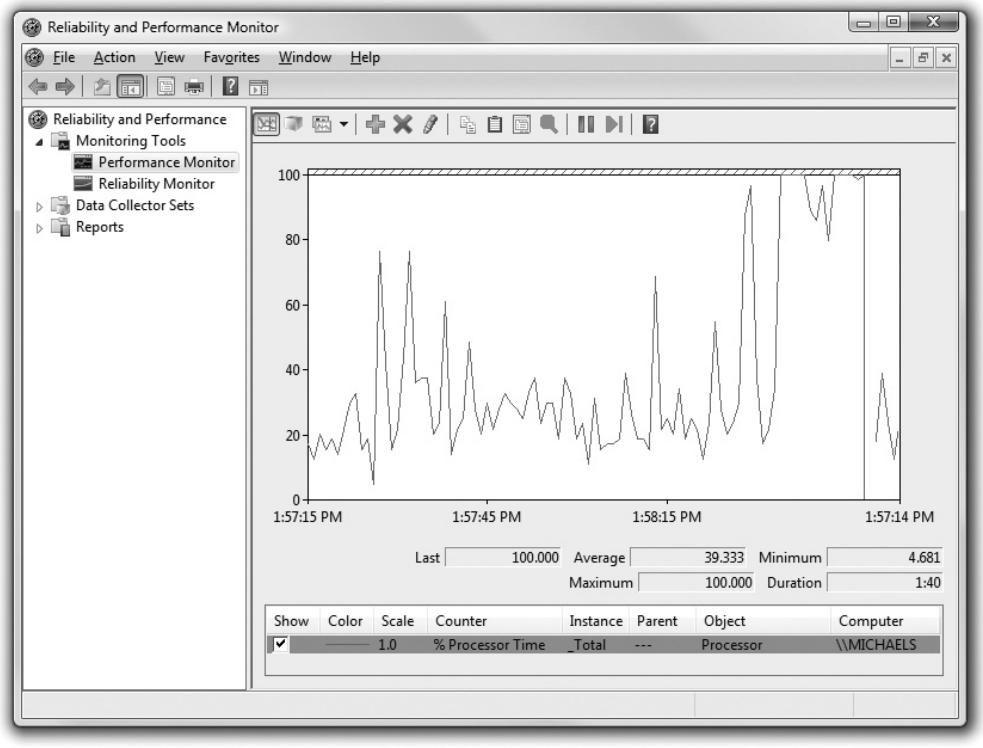


Figure 17-37 Reliability and Performance Monitor

Back Up Personal Data

The most important data on your computer is the personal data: your documents, e-mail messages and contacts, Web favorites, photographs, and other files. To handle backing up personal data, every version of Windows comes with some form of backup utility. There are big differences between the backup that comes with Windows 2000 and XP compared to the one that comes with Vista (and the one that comes with Windows 7 is different still), so let's break up the idea of backing up personal data between Windows 2000/XP and Vista.

Backup Utility for Windows 2000 and XP (NTBackup)

Windows 2000 Backup/Windows XP *Backup Utility* (different names, but the same program under the hood, *NTBackup*) provides almost all the tools you need to back up files and folders. It has come a long way from its origins in Windows NT. NTBackup supports a greater variety of devices, enabling you to back up to network drives, logical drives, tape, and removable disks (but not optical discs). Most folks, however, still turn to third-party utilities to create system, e-mail, browser, and personal data backups.

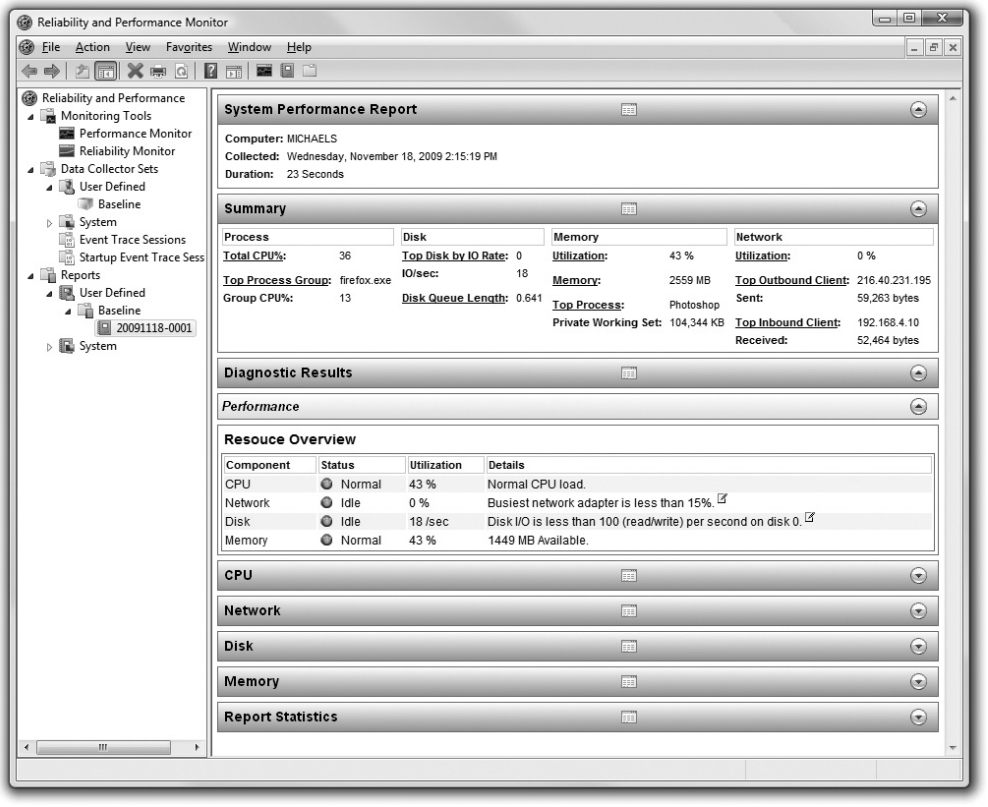


Figure 17-38 Sample Report

NOTE The Backup Utility is not included in the default installation of Windows XP Home. You must install it manually from the Windows CD-ROM.

You can start NTBackup by navigating the Start menu to Accessories | System Tools, or by clicking the Backup Now button on the Tools page of the local disk properties box. I prefer to start it from Start | Run with the command **ntbackup**. Click the Backup Wizard button to run the Backup Wizard. This technique works in both Windows 2000 and Windows XP. To use the Windows XP version in Advanced Mode, click Advanced Mode on the opening screen (Figure 17-39). To have it always open in Advanced Mode, deselect the *Always start in wizard mode* checkbox. If the program is in Advanced Mode and you want to run it as a wizard, click the Wizard Mode link to open the Backup or Restore Wizard.

Figure 17-39 Choosing to run the Backup Wizard in Advanced Mode

A Backup by Any Other Name

Microsoft has been dreadfully inconsistent on the naming of the backup programs that bundle with Windows. Here's the scoop in a nutshell. In Windows 2000, the official name of the backup program is *Microsoft Windows Backup*, but the dialog box that opens is simply called *Backup*. The wizard interface is called the *Backup Wizard*. The quick command-line command you run to get to the utility is *NTBACKUP*. Are you with me?

The backup program in Windows XP has a similar slew of names. The official name of the program is *Backup Utility for Windows*. The Advanced Mode dialog box is called *Backup Utility*, but the wizard interface differs depending on whether you run the utility in Wizard Mode or click the Backup Wizard button in the Advanced Mode dialog box. The former runs the *Backup or Restore Wizard*; the latter runs the *Backup Wizard*. These wizards offer different options, with the Backup or Restore Wizard providing the simpler, consumer-oriented interface. Both wizards are only different faces for the Backup Utility. Got it? Oh, and NTBACKUP is the command-line command to run the program in Windows XP, so Microsoft provides at least a nod at naming consistency.

Most seasoned techs call the backup programs in Windows 2000 and Windows XP *Backup* or *NTBackup*. You need to know the variety of names, though, to provide proper customer support. This is especially true in a help desk environment.

To create a backup, start the Backup Utility, click Advanced Mode, and choose the Backup tab. Check the boxes next to the drives and files you want to include in the backup.

To include your system state information, such as Registry and boot files (which you should do), click the System State checkbox. To specify where to put the backup file you're creating, either type the path and file name in the *Backup media or file name* box or click Browse, select a location, type the file name, and click Save. Click Start Backup. Choose whether you want to append this backup to a previous one or overwrite it. Click Advanced to open the Advanced Backup Options dialog box, select *Verify data after backup*, and click OK. Click Start Backup again. A dialog box shows you the utility's progress. When it finishes, click Close and then close the Backup Utility.

Both versions of NTBackup give you three choices after you click Advanced Mode: Backup Wizard (Advanced), Restore Wizard (Advanced), and a third choice that is very important. The third option in Windows 2000 is the Emergency Repair Disk. As you can see in Figure 17-40, the third option in Windows XP is the Automated System Recovery Wizard.

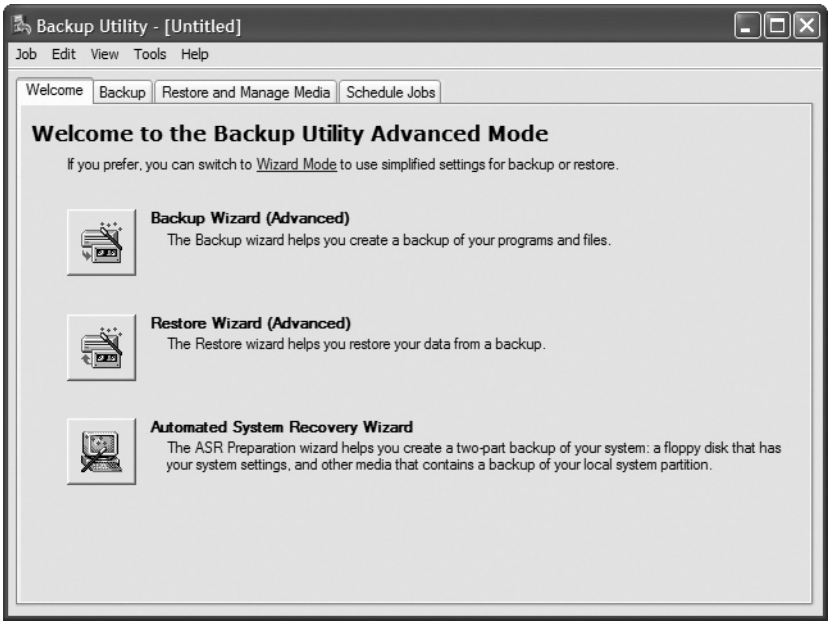


Figure 17-40 Windows XP Backup Utility options

Windows 2000 Emergency Repair Disk (ERD) The Windows 2000 *Emergency Repair Disk* (*ERD*) disk saves critical boot files and partition information and is your main tool for fixing boot problems in Windows 2000. It is not a bootable disk, nor does it store very much information; the ERD does not replace a good system backup! It works with a special folder called \WINNT\REPAIR to store a copy of your Registry. It's not perfect, but it gets you out of most startup problems. Making a new

ERD before you install a new device or program is good practice. Then the ERD is ready if you need it.

So you have this great Emergency Repair Disk that'll take care of all of your system repair problems. You just pop it in the floppy drive and go, right?

Not just yet. As I mentioned, the ERD itself is not a bootable disk. To use the ERD, you must first boot the system by using the Windows installation CD-ROM. Follow these steps to repair a system by using the ERD:

1. Boot the system, using either your set of boot diskettes or the installation CD-ROM.
2. In the Welcome to Setup dialog box, press the R key to select the option to repair a Windows 2000 installation.
3. The Windows 2000 Repair Options menu appears. You have the option of either entering the Recovery Console or using the Emergency Repair Disk.
4. Press the R key to select the option to repair Windows 2000 by using the emergency repair process.
5. The next screen offers the choice of Manual or Fast repair.

- Manual repair lets you select the following repair options: inspect the startup environment, verify the system files, and inspect the boot sector.
- Fast repair doesn't ask for any further input.

6. Follow the onscreen instructions and insert the ERD when prompted.
7. Your system will be inspected and, if possible, restored. When the process finishes, the system restarts.

Windows XP Automated System Recovery (ASR) The Windows XP *Automated System Recovery* (*ASR*) looks and acts very similar to the Windows 2000 ERD. The ASR Wizard lets you create a backup of your system. This backup includes a floppy disk and backup media (tape or CD-R) containing the system partition and disks containing operating system components (Figure 17-41).

The restore side of ASR involves a complete reinstallation of the operating system, preferably on a new partition. This is something you do when all is lost. Run Setup and press F2 when prompted during the text-mode portion of Setup. Follow the prompts on the screen, which will first ask for the floppy disk and then for the backup media.

Backup Wizard Data files are not backed up by the ERD or by the ASR. Therefore, you have to back up data files. If you run the Backup Wizard and click the Next button on the Welcome screen, you'll open the dialog box in Figure 17-42. You have three options here. The first two are fairly self-explanatory: You can back up everything or just selected drives and files.

The third option needs some explanation. The *Only back up the System State data* radio button enables you to save "other" system-critical files, but with Windows 2000/XP, it's not much more than making an ERD with the Registry backup. This option really makes sense for Windows 2000 Server and Windows Server 2003 systems because

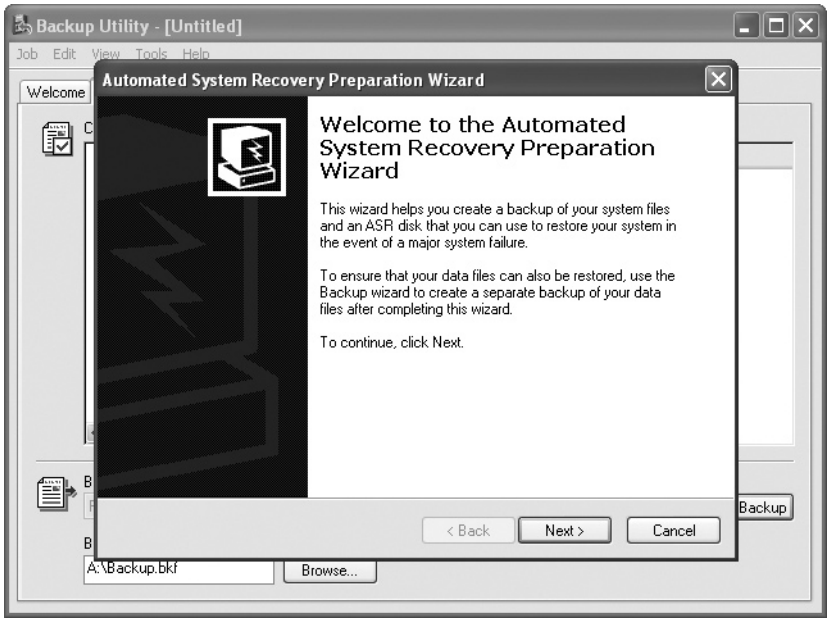
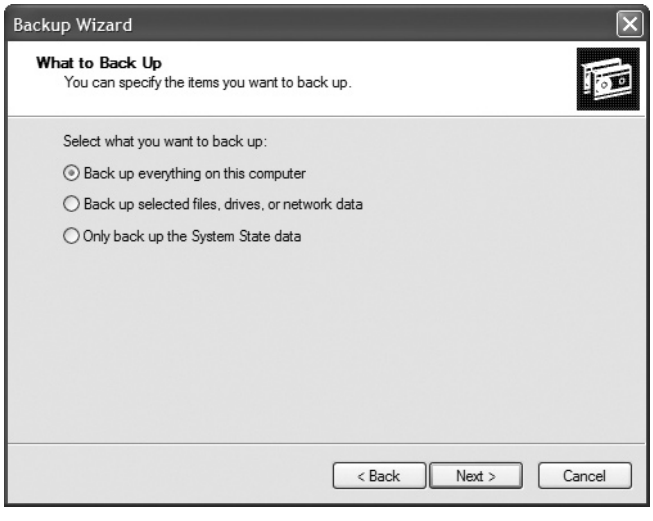


Figure 17-41 Creating an ASR backup

Figure 17-42 Backup Wizard options



it saves Active Directory information (which your Windows 2000/XP systems do not store) as well as other critical, server-specific functions. (I cover more on these topics in Chapter 23, "Local Area Networking.") But the CompTIA A+ certification exams may still expect you to know about it!

Tape Backup The odd fact that Microsoft has not updated the Backup or Restore Wizard to enable you to back up to optical discs of any sort has kept alive the practice of tape backups. Tape drives connect to the ATA or SCSI bus, just like optical drives, but rather than using a shiny CD-R or DVD+R disc, you have to back up to magnetic tape (Figure 17-43).

Figure 17-43
Backup tapes

Tape drive manufacturers have done pretty much everything they can do to make tape backups as fast as possible, but the technology suffers from two huge drawbacks. First, it's tape, which means all data must be stored and restored in sequential access. The drive has to go through Files 1 and 2 before reaching File 3, in other words. Second, tape is painfully slow in comparison to hard drives, optical drives, or Flash-media drives.

The only great benefit to tape is that it's relatively cheap to buy multiple tapes with a lot of storage capacity. With hard drive and recordable DVD prices at rock bottom today, though, tape's days are numbered.

Backup Options The goal of backing up data is to ensure that when a system dies, there will be an available, recent copy you can use to restore the system. You could simply back up the complete system at the end of each day—or whatever interval you feel is prudent to keep the backups fresh—but complete backups can be a tremendous waste of time and materials. Instead of backing up the entire system, take advantage of the fact that all the files won't be changed in any given period; much of the time you only need to back up what's changed since your last backup. Recognizing this, most backup software solutions have a series of options available beyond the complete backup.

The key to understanding backups other than the full backup is *attributes*, 1-bit storage areas that all files have. The most common attributes are Hidden (don't show the file in Computer or when `dir` is typed at the command line), System (it's a critical file for the system), Read-Only (can't erase it), and Archive. These attributes were first used in FAT-formatted drives in the DOS era, but they are still completely supported by all file formats. The *archive bit* works basically like this: Whenever a file is saved, the archive bit is turned on. Simply opening a file affects the current state of the archive bit. Backup programs usually turn off a file's archive bit when the file is backed up.

In theory, if a file's archive bit is turned off, there's a good backup of that file on some tape. If the archive bit is turned on, it means that the file has been changed since it was last backed up (see Figure 17-44).

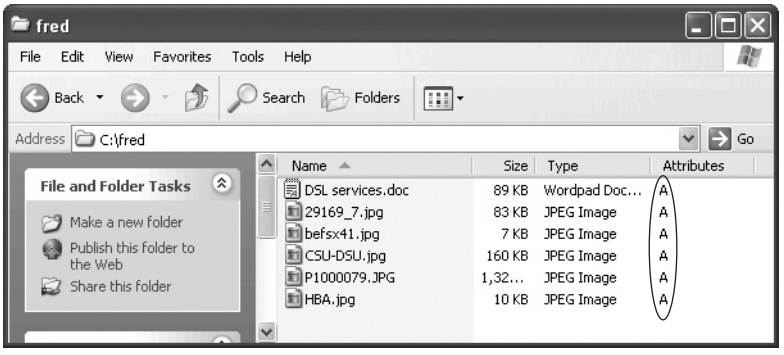


Figure 17-44 The archive bit on these files is on

NOTE Windows Explorer (My Computer in Windows XP, Computer in Vista) by default does not show much about files in any view, even when you select Details from the View menu. The Details view is highly customizable, however, and can reveal a phenomenal amount and variety of information about files.

To customize your view, right-click the column bar (the gray bar that says Name, Size, Type, Date Modified, and so forth) to look at the default choices. You'll see everything from Attributes, Owner, Author, and Title to file-type specific information such as Genre, Duration, and Bit Rate (for music files). If the default extra view options don't get your motor revving, selecting the More option brings up a menu offering many more view options! For the purposes of this section, click the Attribute box to display file and folder attributes.

Archive bits are used to perform backups that are not full backups. The following backup types are most often supported:

- A *normal backup* is a full backup. Every file selected is backed up, and the archive bit is turned off for every file backed up. This is the standard "back it all up" option.
- A *copy backup* is identical to a normal backup, with the important distinction being that the archive bits are *not* changed. This is used (although not often) for making extra copies of a previously completed backup.
- An *incremental backup* includes only files with the archive bit turned on. In other words, it copies only the files that have been changed since the last backup. This backup turns off the archive bits.
- A *differential backup* is identical to an incremental backup, except that it doesn't turn off the archive bits.
- A *daily backup*, also known as a *daily copy backup*, makes copies of all the files that have been changed that day. It does not change the archive bits.

EXAM TIP Be sure you know the types of backups, including which ones change the archive bits and which ones do not.

The motivation for having both the incremental and differential backups may not be clear at first glance—they seem so similar as to be basically the same. Incremental seems the better option at first. If a file is backed up, you would want to turn off the archive bit, right? Well, maybe. But there is one scenario where that might not be too attractive. Most backups do a big weekly normal backup, followed by daily incremental or differential backups at the end of every business day. Figure 17-45 shows the difference between incremental and differential backups.

Figure 17-45 Incremental versus differential

Incremental

MON	TUE	WED	THU	FRI
Full backup	All Tuesday changes	All Wednesday changes	All Thursday changes	All Friday changes

Differential

MON	TUE	WED	THU	FRI
Full backup	All changes through Tuesday	All changes through Wednesday	All changes through Thursday	All changes through Friday

Notice that a differential backup is a cumulative backup. Because the archive bits are not set, it keeps backing up all changes since the last normal backup. This means the backup files will get progressively larger throughout the week (assuming a standard weekly normal backup). The incremental backup, by contrast, only backs up files changed since the last backup. Each incremental backup file will be relatively small and also totally different from the previous backup file.

Let's assume that the system is wiped out on a Thursday morning. How can you restore the system to a useful state?

If you're using an incremental backup, you will first have to restore the last weekly backup you ran on Monday, then the Tuesday backup, and then the Wednesday backup before the system is restored to its Thursday morning state. The longer the time between normal backups, the more incremental backups you must restore.

Using the same scenario but assuming you're doing differential instead of incremental backups, you' only need the weekly backup and then the Wednesday backup to restore your system. A differential backup always requires only two backups to restore a system. Suddenly, the differential backup looks better than the incremental! On the other hand, one big benefit of incremental over differential is backup file size. Differential backup files are massive compared to incremental ones.

Backup and Restore Center for Vista

One of the many changes between XP and Vista was the elimination of NTBackup, replaced with the Windows Backup and Restore Center. If you open this program, you'll notice that you only have two options: back up everything or restore from a backup (Figure 17-46).

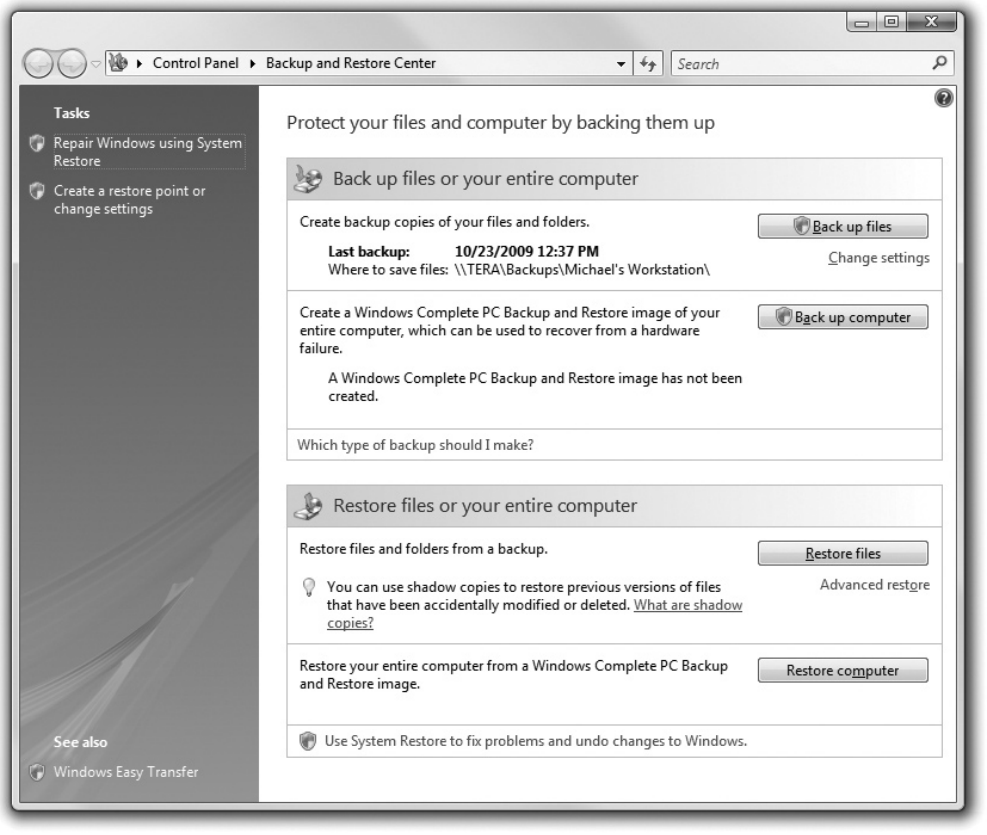


Figure 17-46 Backup and Restore Center

If you choose to back up your computer, you have another two choices: back up files or back up the entire computer. *Back up files* gives you a choice of the file types you wish to back up (Figure 17-47). *Back up computer* backs up the entire computer: every single file and folder. Vista no longer supports tape backups nor can you choose between differential or incremental backups. If you want these options, you need to buy a third-party backup tool.

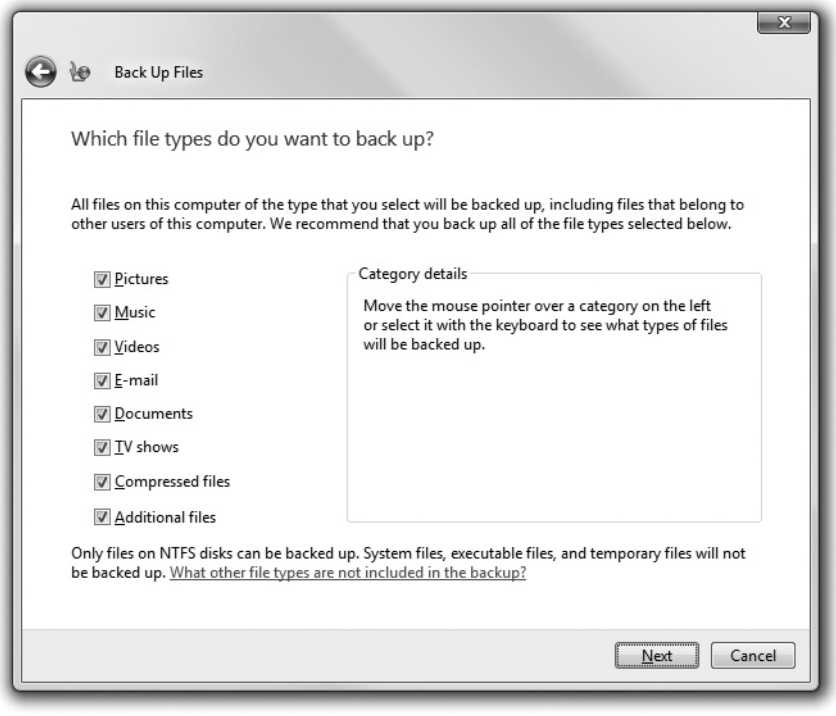


Figure 17-47 Backup Files option

The Vista tool comes with a handy wizard that automatically configures when you want to back up. So although you lose some of the options from NTBackup, you'll find this to be a powerful tool that works for most of your backup needs.

System Restore

Every technician has war stories about the user who likes to add the latest gadget and cool software to his computer. Then he's amazed when things go very, very wrong: the system locks up, refuses to boot, or simply acts weird. This guy also can't remember what he added or when. All he knows is that you should be able to fix it—fast.

This is not news to the folks at Microsoft, and they have a solution to this problem. It's called *System Restore*, and they first introduced it in Windows Me, with further refinements in Windows XP. The System Restore tool enables you to create a *restore point*, a copy of your computer's configuration at a specific point in time. If you later crash or have a corrupted OS, you can restore the system to its previous state.

To create a restore point, go to Start | All Programs | Accessories | System Tools | System Restore. When the tool opens, select Create a restore point and then click Next (Figure 17-48). Type in a description on the next screen. There's no need to include the

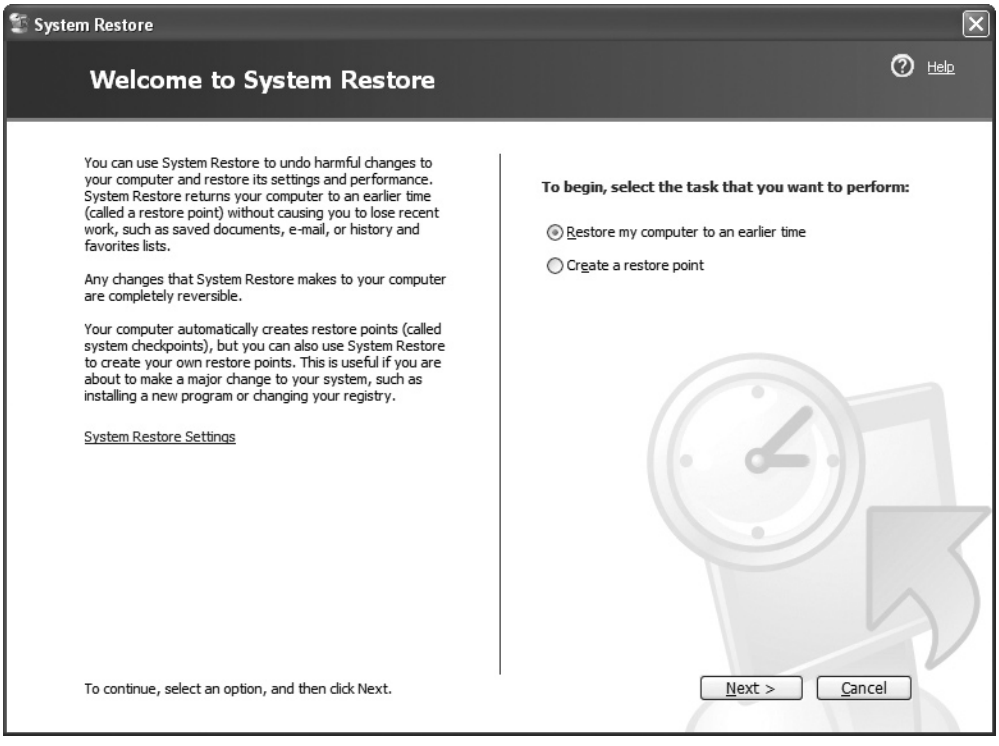


Figure 17-48 Create a restore point

date and time because the System Restore adds them automatically. Click Create and you're finished.

System Restore in Windows Vista is much more automatic, with the operating system making a number of restore points automatically. To make your own restore point, go to System Properties, select System Protection, and then click the Create button as shown in Figure 17-49.

If you click the System Restore button, you might be surprised at how many system restore points are already made for you (Figure 17-50). In most cases, one of these is all you'll need to return your system to an earlier point.

The System Restore tool creates some of the restore points in time automatically. For instance, by default, every time you install new software, XP creates a restore point. Thus, if installation of a program causes your computer to malfunction, simply restore the system to a time point prior to that installation, and the computer should work again.

During the restore process, only settings and programs are changed. No data is lost. Your computer includes all programs and settings as of the restore date. This feature is

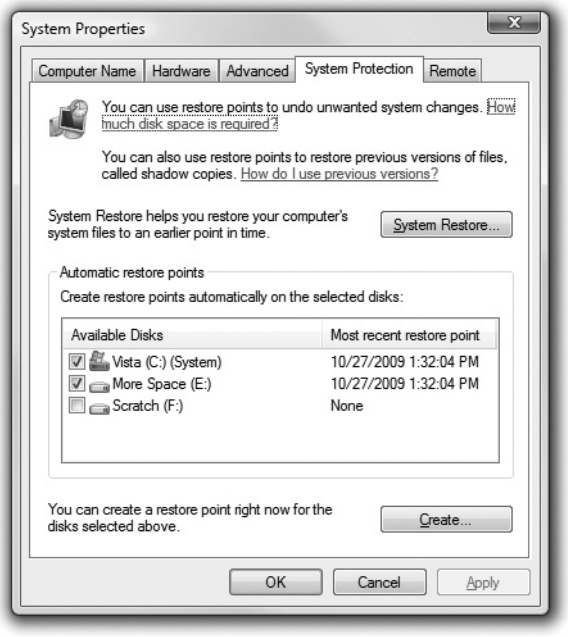


Figure 17-49 Creating a manual System Restore in Vista

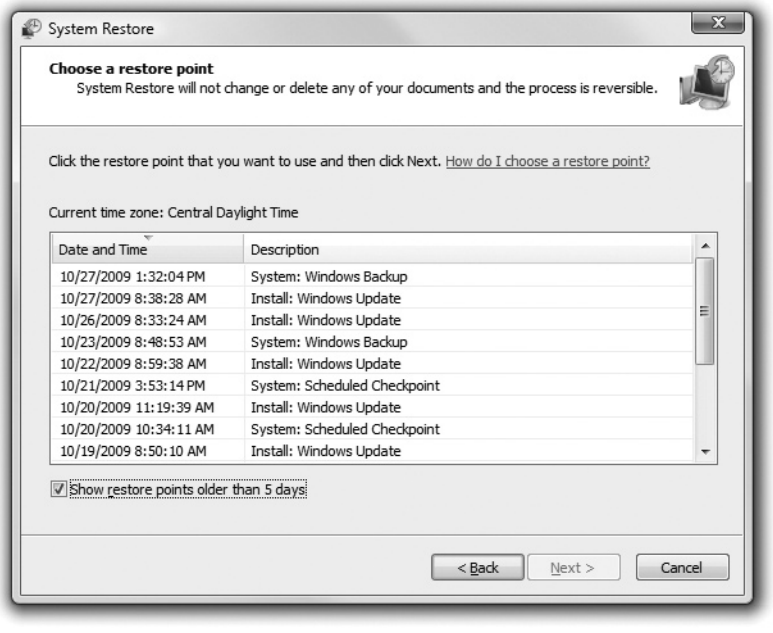


Figure 17-50 Restore points in Vista

absolutely invaluable for overworked techs. A simple restore fixes many user-generated problems.

To restore to a previous time point, start the System Restore Wizard by choosing Start | All Programs | Accessories | System Tools | System Restore. Then select the first radio button, *Restore my computer to an earlier time,* and click Next. Figure 17-51 shows a calendar with restore points. Any day with a boldface date has at least one restore point. These points are created after you add or remove software or install Windows updates and during the normal shutdown of your computer. Select a date on the calendar; then select a restore point from the list on the right and click Next.

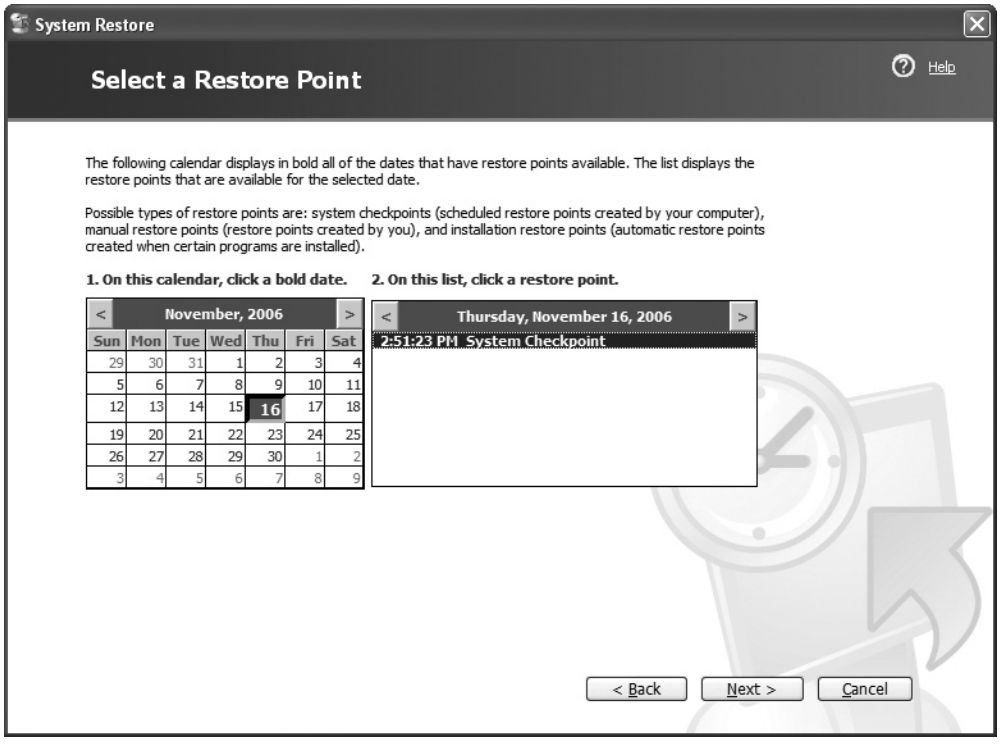


Figure 17-51 Calendar of restore points

The last screen before the system is restored shows a warning. It advises you to close all open programs and reminds you that Windows will shut down during the restore process. It also states that the restore operation is completely reversible. Thus, if you go too far back in time, you can restore to a more recent date.

You don't have to count on the automatic creation of restore points. You can open System Restore at any time and simply select *Create a restore point*. Consider doing this

before making changes that might not trigger an automatic restore point, such as directly editing the Registry.

System Restore is turned on by default and uses some of your disk space to save information on restore points. To turn System Restore off or change the disk space usage, open the System Properties applet in Control Panel and select the System Restore tab (Figure 17-52).

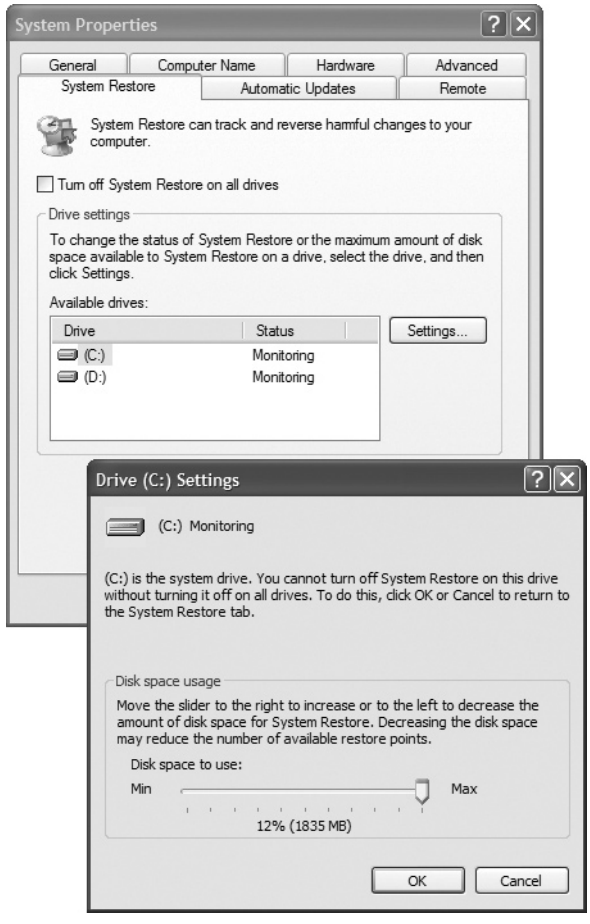


Figure 17-52 System Restore tab in System Properties applet

Installing Recovery Console

When things get really bad on a Windows system, you need to turn to the Recovery Console. The *Recovery Console* is a text-based startup of Windows that gets you to a command prompt similar to the Windows command prompt.

If you have the Windows 2000/XP CD-ROM, you can start the Recovery Console by running Setup, selecting Repair, and then selecting Recovery Console. If you like to be proactive, however, you can install the Recovery Console on your hard drive so that it is one of your startup options and does not require the Windows 2000 or

XP CD-ROM to run. The steps to do this in Windows 2000 and Windows XP are very nearly identical.

First, you need to log into the system with the Administrator account. Grab your Windows 2000 or XP installation CD-ROM and drop it in your system. If the Autorun function kicks in, just click the No button. To install the Recovery Console and make it a part of your startup options, click the Start button, select Run, and type the following:

```
d:\i386\winnt32 /cmdcons
```

If your CD-ROM drive uses a different drive letter, substitute it for the D: drive. Then just follow the instructions on the screen. If you are connected to the Internet, allow the Setup program to download updated files. From now on, every time the system boots, the OS selection menu will show your Windows OS (Windows 2000 Professional or Windows XP) and the Microsoft Windows Recovery Console. It may also show other choices if yours is a multi-boot computer.

System Recovery Options

Windows Vista and Windows 7 have dropped the Recovery Console, replacing it with the graphical System Recovery Options. System Recovery Options is on the Vista/7 installation media, and you run it by booting to the media as though you were installing Windows. When you boot from the installation media, choose your language settings, click Next, select *Repair your computer* and then click Next a second time to see the System Recovery Options menu, as shown in Figure 17-53. The System Recover Options Menu has a number of items, each designed to help in a particular situation.

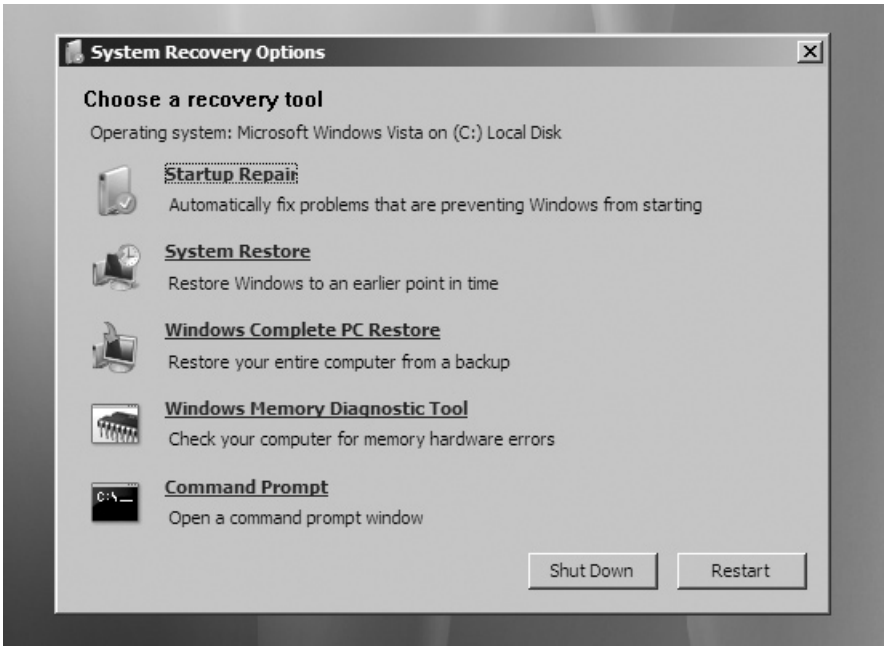


Figure 17-53 System Recovery Options in Windows Vista

Startup Repair Startup Repair should be your first choice when running System Recovery. This option tells Windows to attempt to repair your system automatically. Startup Repair rebuilds all of your most important system files, which in most cases will at least enable you to get Windows to boot. If Startup Repair doesn't work, hope you made some system restore points!

System Restore The System Restore option searches your computer for restore points, enabling you to choose one. This will hopefully fix whatever is preventing you system from booting. If not, you may want to consider the Complete PC Backup option.

Windows Complete PC Backup Assuming you made a backup while the system was running properly, you can select this option to restore your PC.

Windows Memory Diagnostic Tool Bad RAM is an all-too-common problem for any computer and often shows itself during startup. Recognizing this, Microsoft added this tool to test your RAM for errors. This is an incredibly powerful tool for the job. If your RAM is bad, the Memory Diagnostic Tool will locate and report the error to you. You replace your RAM and the problem is solved.

Command Prompt The Command Prompt is just as it is named: a full-blown command prompt, not to be confused with the Windows 2000/XP Recovery Console. You can run any command prompt program from here.

Practical Application

Troubleshooting Windows

Chapters 4, 12, 14, 15, and 16 introduced you to the essential tools for troubleshooting and repairing Windows. You know about Disk Management, Device Manager, Event Viewer, and more. You've spent countless hours preparing systems for disaster with Windows Backup and System Restore. While learning about the tools, you also learned how to use them. This section puts it all together and shows you a plan to deal with potential disasters for a Windows computer.

This section looks at Windows problems from the ground up. It starts with catastrophic failure—a PC that won't boot—and then discusses ways to get past that problem. The next section covers the causes and work-arounds when the Windows GUI fails to load. Once you can access the GUI, the world of Windows diagnostic and troubleshooting tools that you've spent so much time learning about comes to your fingertips. First, though, you have to get there.

Failure to Boot

Windows boot errors take place in those short moments between the time the POST ends and the Loading Windows screen begins. For Windows 2000/XP to start loading the main operating system, the critical system files NTLDR, NTDETECT.COM,

and BOOT.INI must reside in the root directory of the C: drive, and BOOT.INI must point to the Windows boot files. If any of these requirements isn't in place, the system won't get past this step. Here are some of the common errors you see at this point:

No Boot Device Present

NTLDR Bad or Missing

Invalid BOOT.INI

Windows Vista or 7 no longer use these files, so you need to look for an entirely new set of errors to tell you that there's a boot failure. Luckily, the only truly critical file that has any hope of corruption is the BOOTMGR file, and Windows Vista will normally restore this on the fly if it detects an error. In all but the rarest cases, the Windows Boot Manager detects a problem and brings up a Windows Boot Manager error like the one shown in Figure 17-54.

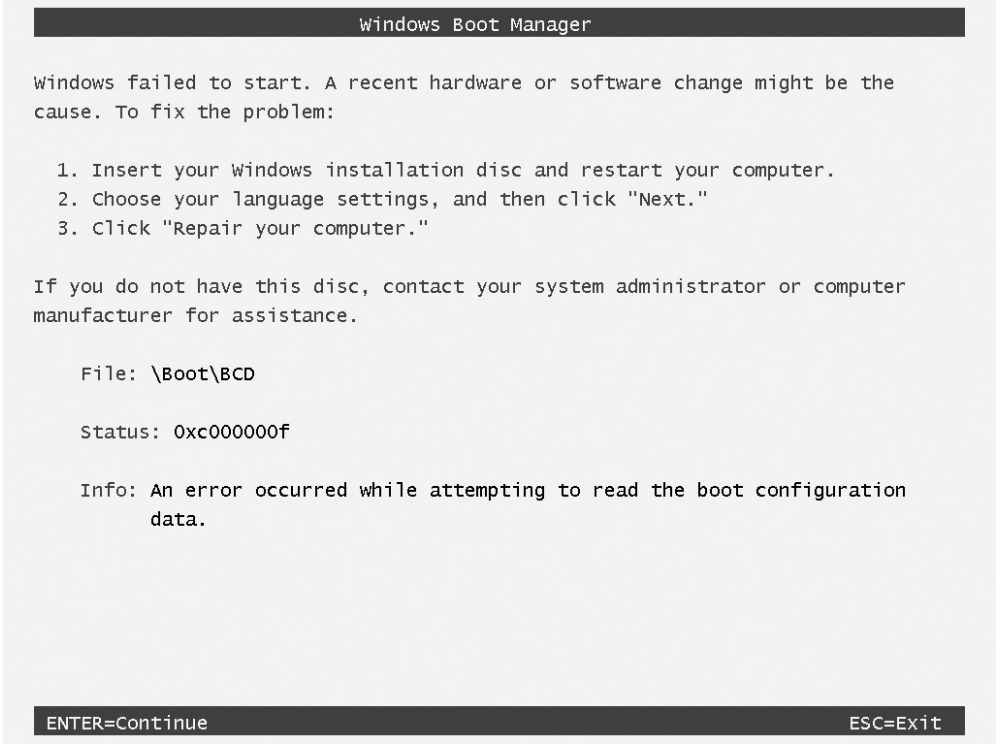


Figure 17-54 Boot Manager error

Note that these text errors take place very early in the startup process. That's your big clue that you have a boot issue. If you get to the Windows splash screen and then lock up, that's a whole different game, so know the difference.

If you get one of the catastrophic error messages and you're running Windows 2000 or XP, you have a three-level process to get back up and running. You first should attempt to repair. If that fails, attempt to restore from a backup copy of Windows. If restore is either not available or fails, your only recourse is to rebuild. You will lose data at the restore and rebuild phases, so you definitely want to spend a lot of energy on the repair effort first! If you're running Vista, the repair process for boot failures is exactly the same as a failure to load the GUI. Read about the System Recovery Options in the next section to see what you need to do.

Attempt to Repair by Using Recovery Console (2000/XP)

To begin troubleshooting one of these errors, boot from the installation CD-ROM and have Windows do a repair of an existing installation. Windows prompts you if you want to use the Recovery Console or the emergency repair process (ASR/ERD). Start with the Recovery Console.

If you followed the instructions earlier in the lesson, you've installed the Recovery Console onto your system and have it as an option when you boot the system. If not, start it as described earlier, using the Windows 2000 or XP installation CD-ROM. When you select the Recovery Console, you will see a message about NTDETECT, another one that the Recovery Console is starting up, and then you are greeted with the following message and command prompt:

```
Microsoft Windows XP<TM> Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type Exit to quit the Recovery Console and restart the computer.

1: C:\WINDOWS
Which Windows XP installation would you like to log onto
<To cancel, press ENTER>?
```

The cursor is a small, white rectangle sitting to the right of the question mark on the last line. If you are not accustomed to working at the command prompt, this may be disorienting. If there is only one installation of Windows XP on your computer, type the number **1** at the prompt and press the ENTER key. If you press ENTER before typing in a valid selection, the Recovery Console will cancel and the computer will reboot. The only choice you can make in this example is 1. Having made that choice, the screen displays a new line, followed by the cursor:

```
Type the Administrator password:
```

Enter the Administrator password for that computer and press ENTER. The password does not display on the screen; you see asterisks in place of the password. The screen still shows everything that has happened so far, unless something has happened to cause an error message. It now looks like this:

```
Microsoft Windows XP<TM> Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type Exit to quit the Recovery Console and restart the computer.

1: C:\WINDOWS
Which Windows XP installation would you like to log onto
```

```
<To cancel, press ENTER>? 1
Type the Administrator password: ********
C:\Windows>
```

By now, you've caught on and know that there is a rectangular prompt immediately after the last line. Now what do you do? Use the Recovery Console commands, of course. Recovery Console uses many of the commands that worked in the Windows command-line interface that you explored in Chapter 15, "Working with the Command-Line Interface," as well as some uniquely its own. Table 17-1 lists the common Recovery Console commands.

Command	Description
attrib	Changes attributes of selected file or folder
cd (or chdir)	Displays current directory or changes directories
chkdsk	Runs CheckDisk utility
cls	Clears screen
copy	Copies from removable media to system folders on hard disk. No wildcards
del (or delete)	Deletes service or folder
dir	Lists contents of selected directory on system partition only
disable	Disables service or driver
diskpart	Replaces FDISK—creates/deletes partitions
enable	Enables service or driver
extract	Extracts components from .CAB files
fixboot	Writes new partition boot sector on system partition
fixmbr	Writes new Master Boot Record for partition boot sector
format	Formats selected disk
listsvc	Lists all services on system
logon	Lets you choose which Windows installation to logon to if you have more than one
map	Displays current drive letter mappings
md (or mkdir)	Creates a directory
more (or type)	Displays contents of text file
rd (or rmdir)	Removes a directory
ren (or rename)	Renames a single file
systemroot	Makes current directory system root of drive you're logged into
type	Displays a text file

Table 17-1 Common Recovery Console Commands

The Recovery Console shines in the business of manually restoring Registries, stopping problem services, rebuilding partitions (other than the system partition), and using the EXPAND program to extract copies of corrupted files from a CD-ROM or floppy disk.

Using the Recovery Console, you can reconfigure a service so that it starts with different settings, format drives on the hard disk, read and write on local FAT or NTFS volumes, and copy replacement files from a floppy or CD-ROM. The Recovery Console enables you to access the file system and is still constrained by the file and folder security of NTFS, which makes it a more secure tool to use than some third-party solutions.

The Recovery Console is best at fixing three items: repairing the MBR, reinstalling the boot files, and rebuilding BOOT.INI. Let's look at each of these.

A bad boot sector usually shows up as a No Boot Device error. If it turns out that this isn't the problem, the Recovery Console command to fix it won't hurt anything. At the Recovery Console prompt, just type:

```
fixmbr
```

This fixes the master boot record.

The second problem the Recovery Console is best at fixing is missing system files, usually indicated by the error *NTLDR bad or missing*. Odds are good that if NTDLR is missing, so are the rest of the system files. To fix this, get to the root directory (CD\—remember that from Chapter 15, "Working with the Command Line-Interface"?) and type the following line:

```
copy d:\i386\ntldr
```

Then type this line:

```
copy d:\i386\ntdetect.com
```

This takes care of two of the big three and leads us to the last issue, rebuilding BOOT.INI. If the BOOT.INI file is gone or corrupted, run this command from the recovery console:

```
bootcfg /rebuild
```

The Recovery console will then try to locate all installed copies of Windows and ask you if you want to add them to the new BOOT.INI file it's about to create. Say yes to the ones you want.

If all goes well with the Recovery Console, do a thorough backup as soon as possible (just in case something else goes wrong). If the Recovery Console does not do the trick, the next step is to restore Windows XP.

Attempt to Restore

If you've been diligent about backing up, you can attempt to restore to an earlier, working copy of Windows. You have two basic choices, depending on your OS. In Windows 2000, you can try the ERD. Windows XP limits you to the ASR.

NOTE To use the Windows XP System Restore, you need to be able to get into Windows. "Restore" in the context used here means to give you an option to get into Windows.

If you elected to create an ERD in Windows 2000, you can attempt to restore your system with it. Boot your system to the Windows 2000 installation CD-ROM and select repair installation, but in this case opt for the ERD. Follow the steps outlined earlier in the chapter and you might have some success.

ASR can restore your system to a previously installed state, but you should use it as a last resort. You lose everything on the system that was installed or added after you created the ASR disk. If that's the best option, though, follow the steps outlined earlier in the chapter.

Rebuild

If faced with a full system rebuild, you have several options, depending on the particular system. You could simply reboot to the Windows CD-ROM and install right on top of the existing system, but that's usually not the optimal solution. To avoid losing anything important, you'd be better off swapping the C: drive for a blank hard drive and installing a clean version of Windows.

Most OEM systems come with a misleadingly named *Recover CD* or *recovery partition*. The Recover CD is a CD-ROM that you boot to and run. The recovery partition is a hidden partition on the hard drive that you activate at boot by holding down a key combination specific to the manufacturer of that system. (See the motherboard manual or users' guide for the key combination and other details.) Both "recover" options do the same thing—restore your computer to the factory-installed state. If you run one of these tools, you will wipe everything off your system—all personal files, folders, and programs will go away! Before running either tool, make sure all important files and folders are backed up on an optical disc or spare hard drive.

Failure to Load the GUI

Assuming that Windows gets past the boot part of the startup, it then begins to load the real Windows OS. You will see the Windows startup image on the screen, hiding everything until Windows loads the Desktop (Figure 17-55).

Several issues can cause Windows to hang during the GUI-loading phase, such as buggy device drivers or Registry problems. Even autoloading programs can cause the GUI to hang on load. The first step in troubleshooting these issues is to use one of the Advanced Startup options (covered later in the chapter) to try to get past the hang spot and into Windows.

Device Drivers

Device driver problems that stop Windows GUI from loading look pretty scary. Figure 17-56 shows the infamous Windows *Stop error*, better known as the *Blue Screen of Death* (*BSoD*). The BSoD only appears when something causes an error from which Windows cannot recover. The BSoD is not limited to device driver problems, but device drivers are one of the reasons you'll see the BSoD.

Figure 17-55 GUI time!

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

NO_MORE_IRP_STACK_LOCATIONS

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure that any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000035 (0x00000000,0xF7E562B2,0x00000008,0xC00000000)


***    wdmaud.sys - Address F7E562B2 base at F7E56000, DateStamp 36B047A5
```

Figure 17-56 BSoD

Whenever you get a BSoD, take a moment and read what it says. Windows BSoDs tell you the name of the file that caused the problem and usually suggests a recommended action. Once in a while these are helpful—but not often.

BSoD problems due to device drivers almost always take place immediately after you've installed a new device and rebooted. Take out the device and reboot. If Windows loads properly, head over to the manufacturer's Web site. A new device producing this type of problem is a serious issue that should have been caught before the device was released. In many cases, the manufacturer will have updated drivers available for download or will recommend a replacement device.

The second indication of a device problem that shows up during the GUI part of startup is a freeze-up: the Windows startup screen just stays there and you never get a chance to log on. If this happens, try one of the Advanced Startup Options, covered below.

Registry

Your Registry files load every time the computer boots. Windows does a pretty good job of protecting your Registry files from corruption, but from time to time something may slip by Windows and it will attempt to load a bad Registry. These errors may show up as BSoDs that say "Registry File Failure" or text errors that say "Windows could not start." Whatever the case, you need to restore a good Registry copy. The best way to do this is the Last Known Good Configuration boot option (see the upcoming section). If that fails, you can restore an earlier version of the Registry through the Recovery Console.

Boot to the Windows installation CD-ROM, select the repair installation to get to the Recovery Console, and type these commands to restore a Registry. Notice I didn't say "your" Registry in the previous sentence. Your Registry is corrupted and gone, so you need to rebuild.

```
delete c:\windows\system32\config\system
delete c:\windows\system32\config\software
delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\default

copy c:\windows\repair\system c:\windows\system32\config\system
copy c:\windows\repair\software c:\windows\system32\config\software
copy c:\windows\repair\sam c:\windows\system32\config\sam
copy c:\windows\repair\security c:\windows\system32\config\security
copy c:\windows\repair\default c:\windows\system32\config\default
```

Advanced Startup Options

If Windows fails to start up, use the Windows *Advanced Startup Options* menu to discover the cause. To get to this menu, restart the computer and press F8 after the POST messages but before the Windows logo screen appears. Windows 2000 and Windows XP have similar menus. Vista's is just a tad different. Central to these advanced options are Safe Mode and Last Known Good Configuration. Here's a rundown of the menu options.

EXAM TIP Windows 9*x* had an option for step-by-step confirmation, but that is not a choice in Windows 2000/XP/Vista. Look for it as a wrong answer on the exams!

Safe Mode (All Versions) *Safe Mode* starts up Windows but loads only very basic, non–vendor-specific drivers for mouse, VGA monitor (not in Vista), keyboard, mass storage, and system services (see Figure 17-57).

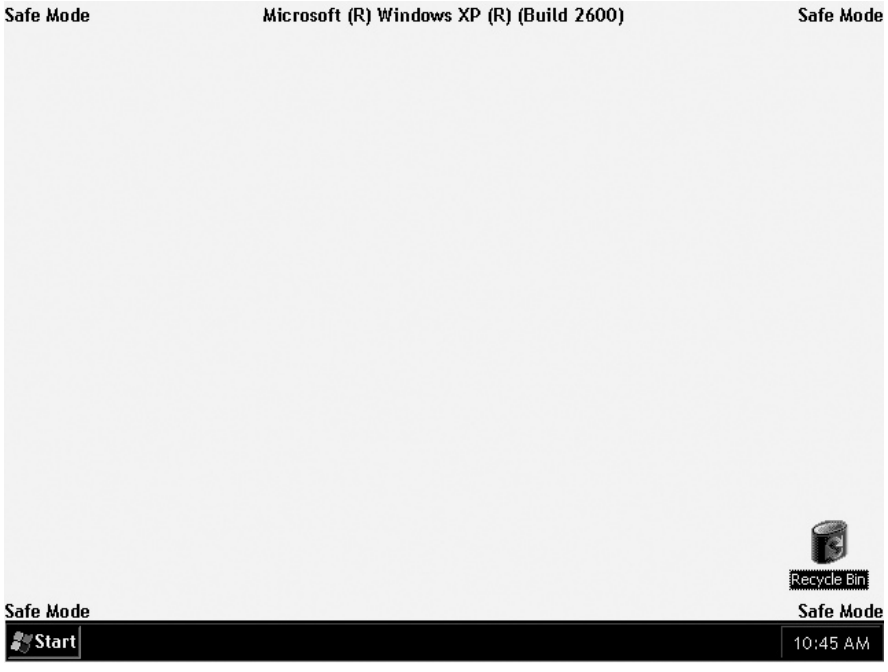


Figure 17-57 Safe Mode

Once in Safe Mode, you can use tools such as Device Manager to locate and correct the source of the problem. When you use Device Manager in Safe Mode, you can access the properties for all the devices, even those that are not working in Safe Mode. The status displayed for the device is the status for a normal startup. Even the network card will show as enabled. You can disable any suspect device or perform other tasks, such as removing or updating drivers. If a problem with a device driver is preventing the operating system from starting normally, check the Device Manager for warning icons that indicate an unknown device.

Safe Mode with Networking (All Versions) This mode is identical to plain Safe Mode except that you get network support. I use this mode to test for a problem with network drivers. If Windows won't start up normally but does start up in Safe Mode, I reboot into Safe Mode with Networking. If it fails to start up with Networking, the problem is a network driver. I reboot back to Safe Mode, open Device Manager, and start disabling network components, beginning with the network adapter.

Safe Mode with Command Prompt (All Versions) When you start Windows in this mode, rather than loading the GUI desktop, it loads the command prompt (CMD.EXE) as the shell to the operating system after you log on, as shown in Figure 17-58. This is a handy option to remember if the desktop does not display at all, which, after you have eliminated video drivers, can be caused by corruption of the EXPLORER.EXE program. From the command prompt, you can delete the corrupted version of EXPLORER.EXE and copy in an undamaged version. This requires knowing the command-line commands for navigating the directory structure, as well as knowing the location of the file you are replacing. Although Explorer is not loaded, you can load other GUI tools that don't depend on Explorer. All you have to do is enter the correct command. For instance, to load Event Viewer, type **eventvwr.msc** at the command line and press ENTER.

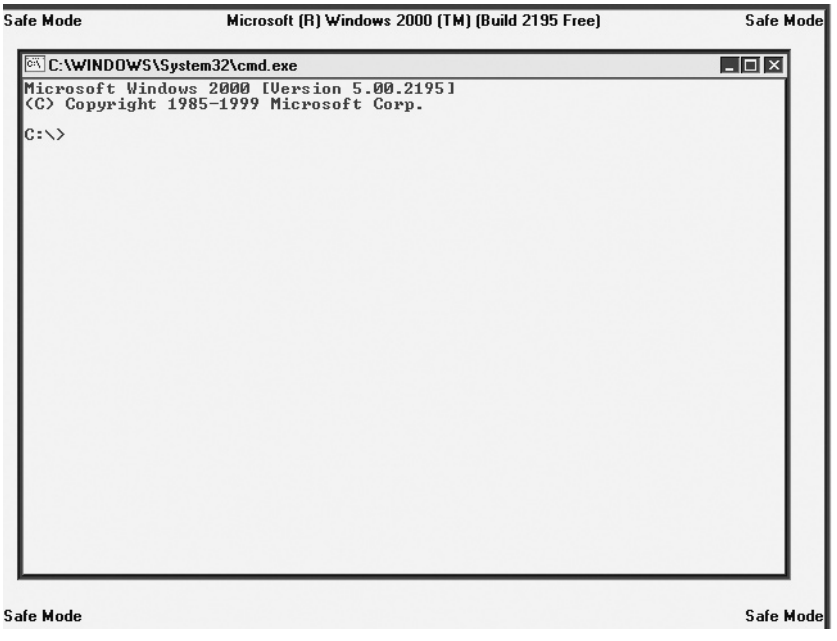


Figure 17-58 Safe Mode with command prompt

Enable Boot Logging (All Versions) This option starts Windows normally and creates a log file of the drivers as they load into memory. The file is named Ntbtlog.txt and is saved in the %SystemRoot% folder. If the startup failed because of a bad driver, the last entry in this file may be the driver the OS was initializing when it failed.

Reboot and go into the Recovery Console. Use the Recovery Console tools to read the boot log (type **ntbtlog.txt**) and disable or enable problematic devices or services.

Enable VGA Mode (2000/XP)/Enable Low-Resolution Mode (Vista) Enable VGA Mode/Enable Low-resolution Mode starts Windows normally but only loads a default VGA driver. If this mode works, it may mean you have a bad driver, or it may mean you are using the correct video driver but it is configured incorrectly (perhaps with the wrong refresh rate and/or resolution). Whereas Safe Mode loads a generic VGA driver, this mode loads the driver Windows is configured to use but starts it up in standard VGA mode rather than using the settings for which it is configured. After successfully starting in this mode, open the Display Properties and change the settings.

Last Known Good Configuration (All Versions) When Windows' startup fails immediately after installing a new driver but before you have logged on again, you may want to try the *Last Known Good Configuration* option. This can be a rather fickle and limited tool, but it never hurts to try it.

Directory Services Restore Mode (All Versions) The title says it all here; this option only applies to Active Directory domain controllers, and only Windows Server versions can be domain controllers. I have no idea why Microsoft includes this option. If you choose it, you simply boot into Safe Mode.

Debugging Mode (All Versions) If you select this choice, Windows starts in kernel debug mode. It's a super-techie thing to do, and I doubt that even über techs do debug mode anymore. To do this, you have to connect the computer you are debugging to another computer via a serial connection, and as Windows starts up, a debug of the kernel is sent to the second computer, which must also be running a debugger program. I remember running debug for an early version of Windows 2000. My coworkers and I did it back then simply because we were studying for the MCSE exams and expected to be tested on it! We all decided it was an experience that we didn't need to repeat.

Disable Automatic Restart on System Failure (All Versions) Sometimes a BSoD will appear at startup, causing your computer to spontaneously reboot. That's all well and good, but if it happens too quickly, you might not be able to read the BSoD to see what caused the problem. Selecting *Disable automatic restart on system failure* from the Advanced Startup Options menu stops the computer from rebooting on Stop errors. This gives you the opportunity to write down the error and hopefully find a fix.

Disable Driver Signature Enforcement (Vista) Windows Vista (and 7) requires that all very low-level drivers (kernel drivers) must have a Microsoft driver signature. If you are using an older driver to connect to your hard drive controller or some other low-level feature, you must use this option to get Windows to load the driver. Hopefully you will always check your motherboard and hard drives for Vista compatibility and never have to use this option.

Start Windows Normally (All Versions) This choice will simply start Windows normally, without rebooting. You already rebooted to get to this menu. Select this if you changed your mind about using any of the other exotic choices.

Reboot (All Versions) This choice will actually do a soft reboot of the computer.

Return to OS Choices Menu (All Versions) On computers with multiple operating systems, you get an OS Choices menu to select which OS to load. If you load Windows and press F8 to get the Advanced Startup Options menu, you'll see this option. Choosing it returns you to the OS Choices menu, from which you can select the operating system to load.

Troubleshooting Tools in the GUI

Once you're able to load into Windows, whether through Safe Mode or one of the other options, the whole gamut of Windows tools is available for you. If a bad device driver caused the startup problems, for example, you can open Device Manager and begin troubleshooting just as you've learned in previous chapters. If you suspect some service or Registry issue caused the problem, head on over to Event Viewer and see what sort of logon events have happened recently.

NOTE Chapter 26, "Securing Computers," goes into a lot more detail on using Event Viewer, especially *auditing*, a way to troubleshoot a buggy system.

Event Viewer might reveal problems with applications failing to load, a big cause of Windows loading problems (Figure 17-59). It might also reveal problems with services failing to start. Finally, Windows might run into problems loading DLLs. You can troubleshoot these issues individually or you can use System Restore in Windows XP to load a restore point that predates the bugginess.

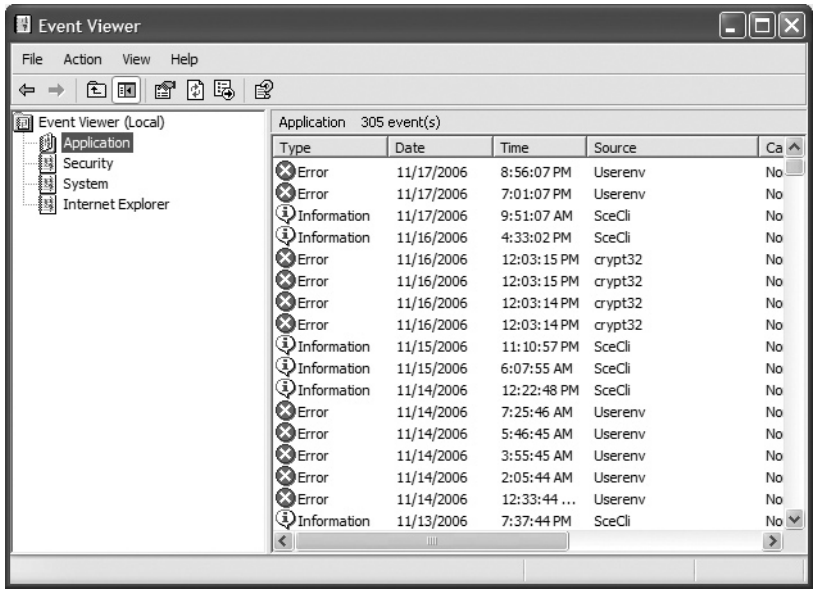


Figure 17-59 Event Viewer showing some serious application errors!

Autoloading Programs

Windows loves to autoload programs so they start at boot. Most of the time this is an incredibly handy option, used by every Windows PC in existence. The problem with autoloading programs is that when one of them starts behaving badly, you need to shut off that program! Use the System Configuration utility to stop programs from autoloading.

Services

Windows loads a number of services as it starts. If any critical service fails to load, Windows tells you at this point with an error message. The important word here is *critical*. Windows will not report *all* service failures at this point. If a service that is less than critical in Windows' eyes doesn't start, Windows usually waits until you actually try to use a program that needs that service before it prompts you with an error message (Figure 17-60).

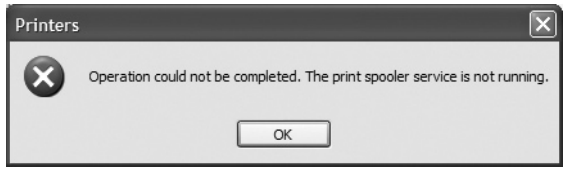


Figure 17-60 Service error

To work with your system's services, go to the Control Panel | Administrative Tools | Services and verify that the service you need is running. If not, turn it on. Also notice that each service has a Startup Type—Automatic, Manual, or Disabled—that defines when it starts. It's very common to find that a service has been set to Manual when it needs to be set to Automatic so that it starts when Windows boots (Figure 17-61).

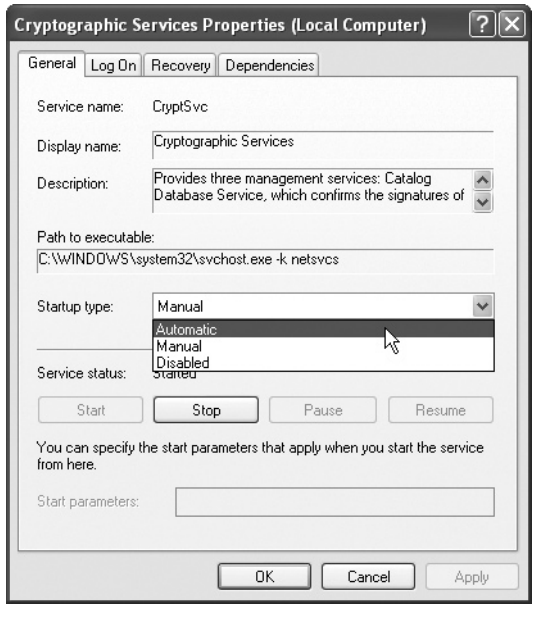


Figure 17-61 Autostarting a service

System Files

Windows lives on dynamic link library (DLL) files. Almost every program used by Windows—and certainly all of the important ones—call to DLL files to do most of the heavy lifting that makes Windows work. Windows protects all of the critical DLL files very carefully, but once in a while you may get an error saying Windows can't load a particular DLL. Although rare, the core system files that make up Windows itself may become corrupted, preventing Windows from starting properly. You usually see something like "Error loading XXXX.DLL," or sometimes a program you need simply won't start when you double-click its icon. In these cases, the tool you need is the System File Checker. The System File Checker is a command prompt program (SFC.EXE) you can use to check a number of critical files, including the ever-important DLL cache. SFC takes a number of switches, but by far the most important is /scannow. Go to a command prompt and type the following to start the program:

```
SFC /scannow
```

SFC automatically checks all critical files and replaces any it sees as corrupted. During this process, it may ask for the Windows installation CD-ROM, so keep it handy!

System Restore

With Windows XP and Vista systems, you can recover from a bad device or application installation by using System Restore to load a restore point. Follow the process explained earlier in the chapter. System Restore is the final step in recovering from a major Windows meltdown.

Application Problems

Almost all Windows programs come with some form of handy installer. You run the installer and the program runs. It almost couldn't be simpler.

A well-behaved program should always make itself easy to uninstall as well. In most cases, you should see an uninstallation option in the program's Start menu area; and in all cases (unless you have an application with a badly configured installer), the application should appear in either the Add/Remove Programs or Programs and Features Control Panel applet (Figure 17-62).

NOTE Remember that you need local administrator privileges to install applications in all versions of Windows.

Despite Microsoft's best efforts, you can run into trouble with applications. Although these errors come in hundreds of varieties, the overwhelming majority of problems can be broken down into three categories: installation problems, compatibility problems, or uninstallation problems.

Installation Problems

Programs that fail to install usually aren't to blame in and of themselves. In most cases, a problem with Windows prevents them from installing, most notably the lack of some

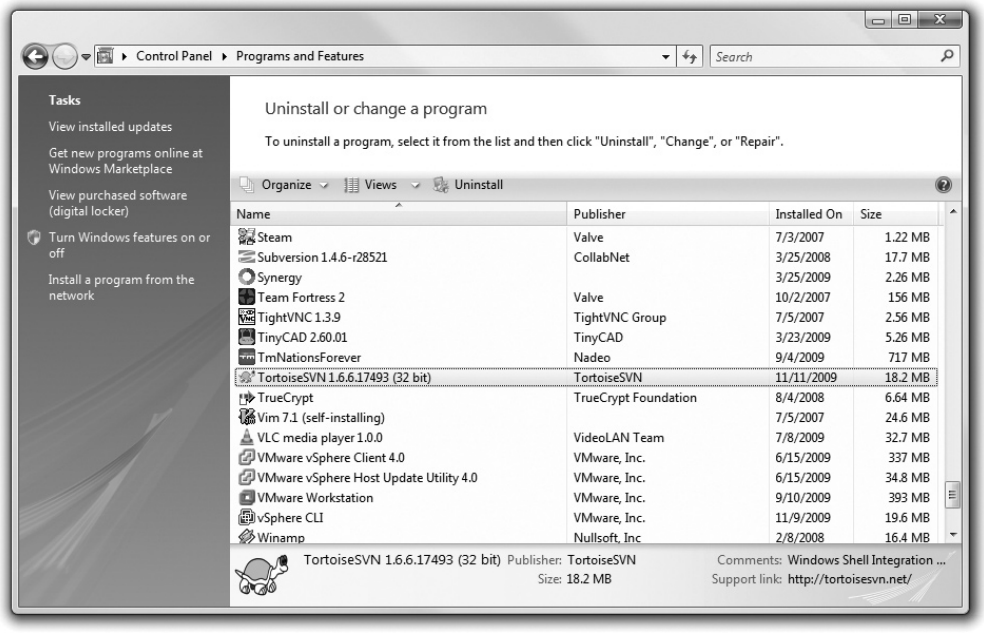


Figure 17-62 Programs and Features Control Panel applet

other program that the application needs so it can operate. One of the best examples of this is the popular .Net Framework. .Net is an extension to the Windows operating system that includes support for a number of powerful features, particularly more powerful interface tools and much more flexible database access. If a program is written to take advantage of .Net, .Net must itself be installed. In most cases if .Net is missing, the application should try to install it at the same time it is installed, but you can't count on this. If .Net is missing or if the version of .Net you are using is too old (there have been a number of .Net versions since it came out in 2002) you can get some of the most indecipherable errors in the history of Windows applications.

Figure 17-63 shows one such example in Windows 7 where the popular VMware vSphere client fails due to the wrong .Net version. Too bad the error doesn't give you any clues!

These types of errors invariably require you to go online and do Web searches, using the application name and the error. No matter how bad the error, someone else has already suffered from the same problem. The trick is to find out what they did to get around it.

Compatibility

Most applications are written with the most recent version of Windows in mind, but as you know, Windows versions change over time. In some cases, such as the jump

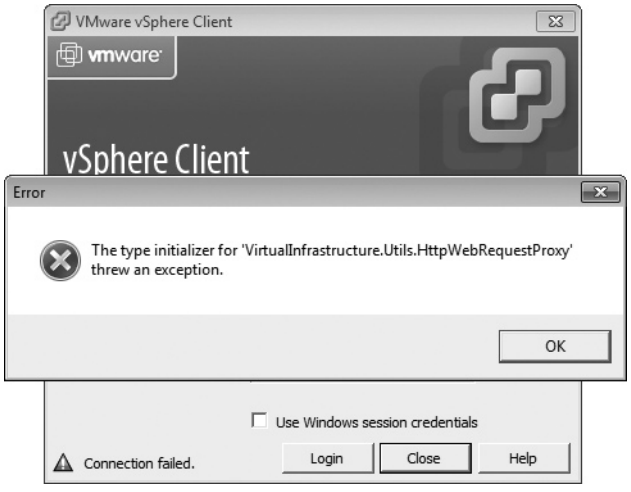


Figure 17-63
.Net error

from Windows 2000 to Windows XP, the changes are minor enough to cause few if any compatibility problems when running an application designed for an earlier version of Windows. In other cases, especially the jump from Windows XP to Vista (and beyond), the underpinnings of the OS differ so much that you have to perform certain steps to ensure that the older programs run. Windows 2000, XP, and Vista provide different forms of *compatibility modes* to support older applications.

NOTE Although it's sometimes a challenge to get an older application to run on a newer version of Windows, the opposite is no problem at all: Installers know to check Windows versions and pop an error if your version of Windows is too old.

Windows 2000 only provides compatibility support for ancient DOS programs. DOS programs know nothing of Windows, so you normally just copy the EXE file to your computer. In Windows 2000, right-clicking on a DOS program shows two tabs: Memory and Program. The memory tab enables you to adjust the amount of memory used by the DOS program. Back in the year 2000, RAM was still precious and you could save a few kilobytes by some careful adjustments. More interesting was the Advanced button under the Program tab (Figure 17-64). This enabled you to let the DOS program load a custom AUTOEXEC.BAT or CONFIG.SYS file.

Windows XP took the idea of compatibility a step further by adding another tab called Compatibility (Figure 17-65). This tab enabled you to configure older Windows programs to work in XP by introducing the concept of compatibility modes. You can also set specific video settings on the Compatibility tab.

Windows Vista takes the Compatibility tab one step further by adding two important features: Windows XP mode and *Run this program as an administrator* (Figure 17-66).

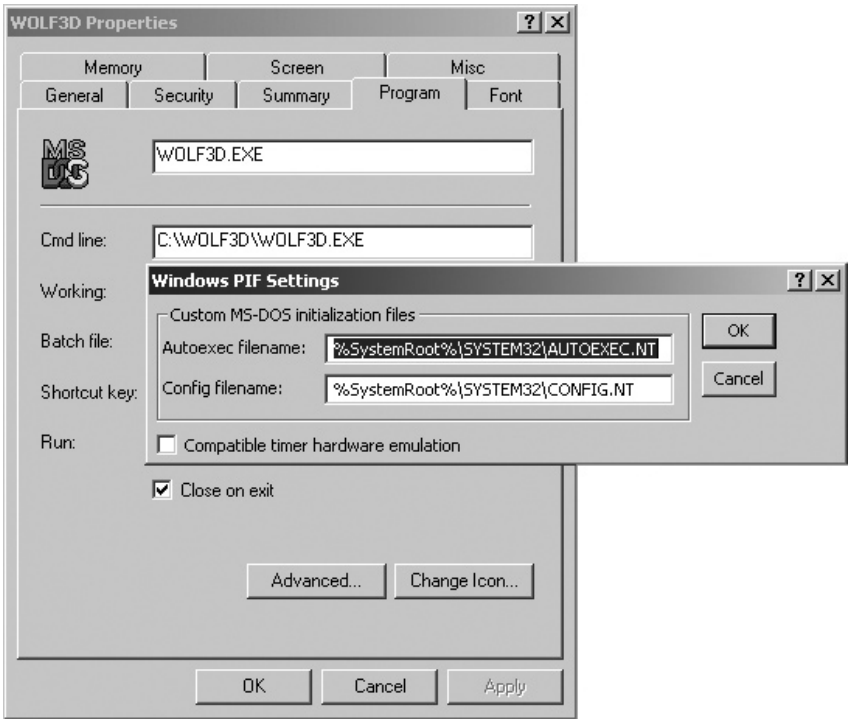
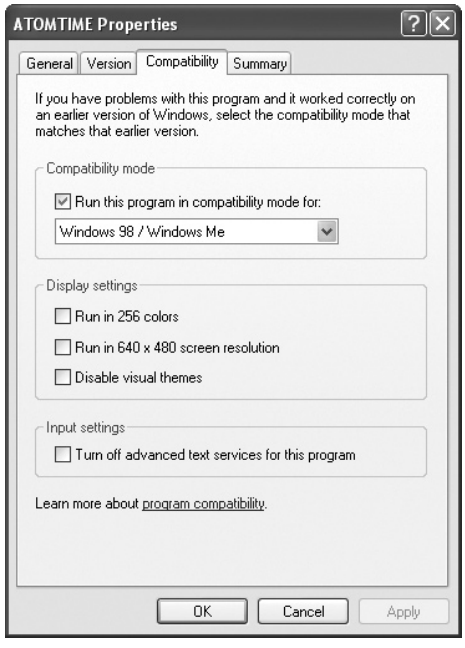


Figure 17-64 Windows 2000 Program tab for DOS program

Figure 17-65 XP compatibility mode



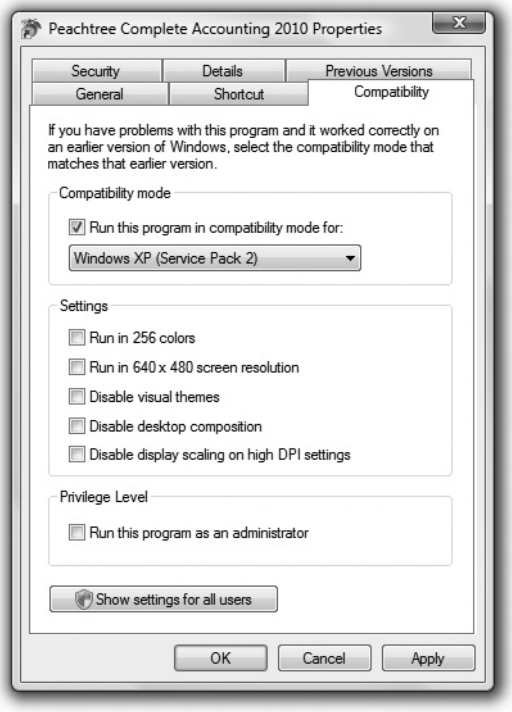


Figure 17-66
Vista compatibility mode

The secret to using compatibility mode isn't much of a secret at all: if the program doesn't run, try a compatibly mode! If you want to be really careful, do a Web search on your application before you try to run it. Compatibility mode is a handy tool to get older applications running.

One error common on older systems, but largely absent or invisible on modern systems, is a *general protection fault* (*GPF*). A GPF occurs when a program tries to do something not permitted, like writing to protected memory or something else Windows doesn't like. This can cause an error message to appear or even crash the computer. You are very unlikely to encounter a GPF today.

Problems with Uninstalling

The single biggest problem with uninstalling is that people try to uninstall without administrator privileges. If you try to uninstall and get an error, log back in as an administrator and you should be fine. Don't forget you can right-click on most uninstallation menu options on the Programs menu and select *Run as administrator* to switch to administrator privileges (Figure 17-67).

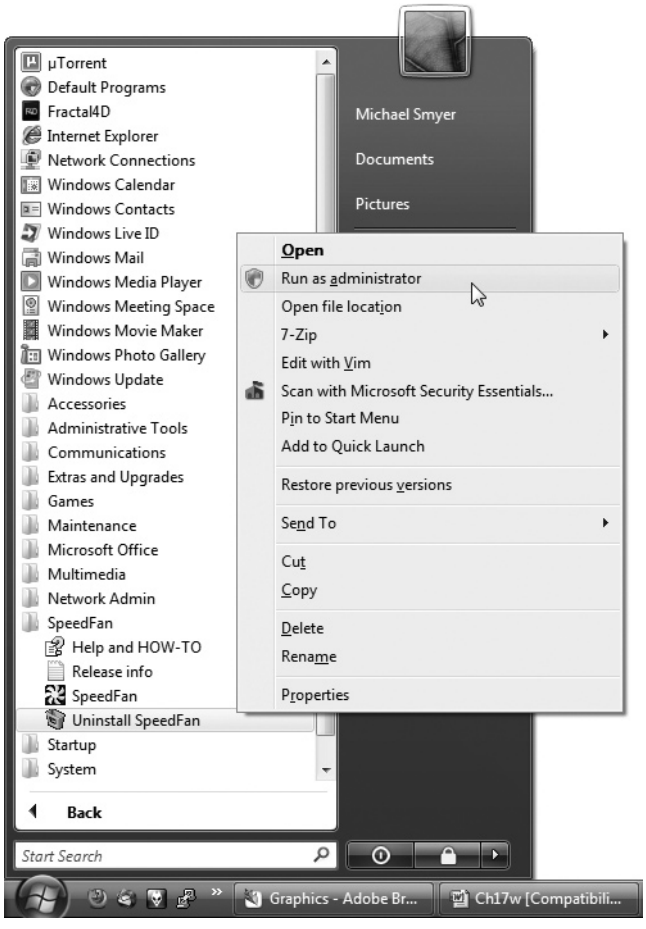


Figure 17-67 Selecting *Run as administrator* from context menu

Beyond A+

The majority of the tools and utilities discussed in this chapter are in direct correlation with the 2009 CompTIA A+ exams. There are also many others you should check out for your personal use. With that said, these commands available at the Windows Vista command prompt deserve mention:

- **CHOICE** A batch file command that allows users to select from a set of options.
- **CLIP** Redirects the output of another command to the Windows Clipboard.
- **CMDKEY** Creates, lists, and deletes stored user names, passwords, and other credentials.
- **FORFILES** Selects files in a particular folder for batch processing.
- **ICACLS** Displays, modifies, backs up, or restores ACLs for files and directories.

- **FSUTIL** Increases the file system memory cache.
- **MKLINK** Creates symbolic links and hard links.
- **TAKEOWN** Allows an administrator to take ownership of a file.
- **TIMEOUT** Pauses the command processor for the specified number of seconds.
- **VSP1CLN** Cleans up after a Windows Vista SP1 installation.
- **VSSADMIN** Volume Shadow Copy Service administration tool.
- **WHERE** Displays the location of files that match a search pattern.

Chapter Review Questions

1. How do you tell Windows Update to automatically download and install only high-priority security updates?
   - **A.** You can't customize Windows Update.
   - **B.** Click the Express button on the Windows Update page.
   - **C.** Check the "High-priority updates only" checkbox.
   - **D.** Run the Microsoft Security Updater.
2. What tool enables you to modify what programs start when Windows starts?
   - **A.** MSSTARTUP
   - **B.** MSINFO32
   - **C.** MSCONFIG
   - **D.** IPCONFIG
3. What does System Information do?
   - **A.** Provides you with a report about the hardware resources, components, and software environment in your computer
   - **B.** Enables you to select which programs and services start when Windows boots up
   - **C.** Enables you to schedule hard drive defragmentation, CHKDSK scans, and other computer tasks
   - **D.** Enables you to perform automatic custom backups of your files and settings
4. What is the backup utility for Windows 2000 and XP called?
   - **A.** Win Backup
   - **B.** Backup 2000
   - **C.** NTBackup
   - **D.** NSBackup

5. What is the difference between incremental and differential backups?
   - **A.** A differential backup turns off the archive bit, while an incremental backup leaves it alone.
   - **B.** A differential backup leaves the archive bit alone, while an incremental backup turns it off.
   - **C.** A differential backup backs up everything on the system, while an incremental backup only backs up things that have changed.
   - **D.** Differential backup is just another name for an incremental backup—they're the same thing.
6. What tool enables you to correct a corrupted Windows operating system by reverting your computer to a previous state?
   - **A.** Windows Restore
   - **B.** Restore State Manager
   - **C.** Time Machine
   - **D.** System Restore
7. What is an important tool for repairing non-booting Windows XP installations?
   - **A.** Bootup recovery
   - **B.** BOOTMGR
   - **C.** AUTORUN.INI
   - **D.** Recovery Console
8. How can you get an extensive, customizable report of your system's performance?
   - **A.** Task Manager
   - **B.** System Monitor
   - **C.** Performance Graph
   - **D.** System Performance
9. What is Data Execution Prevention (DEP)?
   - **A.** A technology that prevents viruses from taking over programs loaded in system memory
   - **B.** A technology that enables you to set permissions for different users on your computer
   - **C.** A technology that prevents programs from being installed on your computer
   - **D.** A technology that prevents files from being written to your hard drive

10. If you install a driver on your system and it causes problems, which tool can you use to roll back to a previous driver?
    - **A.** Driver Manager
    - **B.** MSCONFIG
    - **C.** Device Manager
    - **D.** System Info

Answers

1. **B.** The Express button on the Windows Update page will only install important updates.
2. **C.** MSCONFIG enables you to select the processes and services that start with Windows.
3. **A.** System Information gives you a wide variety of information about your system.
4. **C.** Windows 2000 and XP use NTBackup to back up files.
5. **B.** A differential backup is the same as an incremental backup, but it leaves the archive bit alone instead of turning it off.
6. **D.** Using System Restore, you can restore your computer to a previous restore point.
7. **D.** The Recovery Console is a powerful tool for repairing damaged Windows installations.
8. **B.** The System Monitor gathers data on your system and displays the results in a graph or a report.
9. **A.** Data Execution Prevention, introduced in XP Service Pack 2, prevents viruses from taking control of programs loaded into memory.
10. **C.** The Roll Back Driver option in Device Manager is a great tool for fixing driver problems.