CHAPTER 15

Tools for Solving Windows Problems

In this chapter, you will learn:

- About Windows tools useful to solve problems caused by hardware, applications, and failed Windows components
- About Windows Vista tools that can help when Vista gives problems when starting
- About Windows 2000/XP tools that can help with XP or 2000 startup problems

This chapter is about the tools that you need to know how to use when solving problems with Windows 2000/XP/Vista. We first focus on the tools that can help you when a hardware device, application, or a Windows component fails. Then you'll learn about the tools used when Windows Vista gives problems at startup. Finally, you'll learn about tools that are useful for solving Windows 2000/XP startup problems. Understanding how Vista and 2000/XP start up can help you understand why and how a particular Windows tool functions. Therefore, in the chapter, you'll also learn what happens when these operating systems are loaded.

In the next chapter, we continue our discussion of how to solve Windows problems by learning the strategies and techniques for solving problems with hardware, applications, and Windows. In that chapter, you'll learn how to diagnose a Windows problem and learn which tool is best to use for each situation you face. Consider this chapter and the next a one-two punch for learning to be an expert Windows troubleshooter.

A+ Exam Tip All the content in this chapter applies to the A+ 220-701 Essentials exam, covering the tools and utilities needed to solve Windows problems. The next chapter covers the content on the A+ 220-702 Practical Application exam, where you are expected to know when and where to use Windows problem-solving tools in troubleshooting situations.

TOOLS TO HELP WITH BLUE SCREEN ERRORS, SYSTEM LOCKUPS, AND I/O DEVICE ERRORS

A+
220-701
2.2

In this part of the chapter, you will learn to use several tools and settings useful when dealing with Windows problems that occur after startup. These tools and settings include Vista Problem Reports and Solutions window, XP Error Reporting, Vista Memory Diagnostics, System File Checker, Driver Verifier, startup settings, tools to verify driver signatures, Device Manager, and diagnostic utilities that come bundled with a hardware device. Then we'll summarize when to use each tool when faced with a specific type of Windows problem.

Table 15-1 is a summary of the Windows tools covered in this and other chapters and is given to you as a quick-and-easy reference of these tools.

Tool	Available in Win Vista	Available in Win XP	Description
Add or Remove		X	◢ Accessed from Control Panel. ◢ Use it to uninstall, repair, or update software or certain device drivers that are causing a problem.
Advanced Boot Options Menu	X	X	◢ Accessed by pressing the F8 key when Windows first starts to load. ◢ Use several options on this menu to help you troubleshoot boot problems.
Automated System Recovery (ASR)		X	◢ Accessed from the Windows XP setup CD. ◢ Use ASR as a last resort because the volume on which Windows is installed is formatted and then restored from the most recent backup. All data and applications written to the drive since the last backup are lost.
Backup (Ntbackup.exe)		X	◢ Enter Ntbackup.exe in the XP Run dialog box. ◢ Use it to restore the system state, data, and software from previously made backups.
Backup and Restore Center	X		◢ Accessed from the Start menu. ◢ Use it to back up user data.
Boot logging	X	X	◢ Press F8 at startup and select from the Advanced Boot Options menu. ◢ Use events logged to the Ntbtlog.txt file to investigate the source of an unknown startup error.
Bootcfg (Bootcfg.exe)		X	◢ Enter Bootcfg at a command prompt. ◢ Use it to view the contents of the Boot.ini file.

Table 15-1 Windows Vista/XP maintenance and troubleshooting tools

A+
220-701
2.2

Tool	Available in Win Vista	Available in Win XP	Description
Cacls.exe	X	X	◢ At a command prompt, enter Cacls with parameters. ◢ Use it to gain access to a file when permissions to the file are in error or corrupted. The utility can change the access control list (ACL) assigned to a file or group of files to control which users have access to a file.
Chkdsk (Chkdsk.exe)	X	X	◢ At a command prompt, enter Chkdsk with parameters. ◢ Use it to check and repair errors on a volume or logical drive. If critical system files are affected by these errors, repairing the drive might solve a startup problem.
Cipher.exe	X	X	◢ At a command prompt, enter Cipher with parameters. ◢ Log in as an administrator and use this command to decrypt a file that is not available because the user account that encrypted the file is no longer accessible.
Compact.exe	X	X	◢ At a command prompt, enter Compact with parameters. ◢ Use it with an NTFS file system to display and change the compressions applied to files and folders.
Complete PC Backup	X		◢ Accessed from Control Panel. ◢ Use it to back up the entire Windows volume. Vista can also keep future incremental backups of the volume. ◢ When restoring the system using Complete PC Backup, all data on the Windows volume is lost.
Computer Management (Compmgmt.msc)	X	X	◢ Accessed from Control Panel or you can enter Compmgmt.msc at a command prompt. ◢ Use it to access several snap-ins to manage and troubleshoot a system.
Defrag.exe	X	X	◢ At a command prompt, enter Defrag with parameters. ◢ Use it to defragment a drive to improve drive performance and access time.
Device Driver Roll Back	X	X	◢ Accessed from Device Manager. ◢ Use it to replace a driver with the one that worked before the current driver was installed.

Table 15-1 Windows Vista/XP maintenance and troubleshooting tools (continued)

A+
220-701
2.2

Tool	Available in Win Vista	Available in Win XP	Description
Device Manager (Devmgmt.msc)	X	X	◢ Accessed from the Vista System window or XP System Properties window. ◢ Use it to solve problems with hardware devices, to update device drivers, and to disable and uninstall a device.
Disk Cleanup (Cleanmgr.exe)	X	X	◢ Accessed from a drive's properties window or by entering Cleanmgr at a command prompt. ◢ Use it to delete unused files to make more disk space available. Not enough free hard drive space can cause boot problems.
Disk Defragmenter (Dfrg.msc)	X	X	◢ Accessed from a drive's properties window. ◢ Use it to defragment a volume to improve performance.
Disk Management (Diskmgmt.msc)	X	X	◢ Accessed from the Computer Management console, or enter Diskmgmt.msc at a command prompt. ◢ Use it to view and change partitions on hard drives and to format drives.
Driver Signing and Digital Signatures (Sigverif.exe)	X	X	◢ At a command prompt, enter Sigverif with parameters. ◢ When a device driver or other software is giving problems, use it to verify that the software has been approved by Microsoft.
Driver Verifier (verifier.exe)	X	X	◢ Enter verifier.exe at a command prompt. ◢ Use it to identify a driver that is causing a problem. The tool puts stress on selected drivers, which causes the driver with a problem to crash.
Error Reporting	X	X	◢ This automated Windows service displays error messages when an application error occurs. ◢ Follow directions on-screen to produce an error report and send it to Microsoft. Sometimes the Microsoft Web site responds with suggestions to solve the problem. ◢ Vista keeps a history of past problems and solutions, but XP does not.

Table 15-1 Windows Vista/XP maintenance and troubleshooting tools (continued)

A+
220-701
2.2

Tool	Available in Win Vista	Available in Win XP	Description
Event Viewer (Eventvwr.msc)	X	X	◢ Accessed from the Computer Management console. ◢ Check the Event Viewer logs for error messages to help you investigate all kinds of hardware, security, and system problems.
Group Policy (Gpedit.msc)	X	X	◢ At a command prompt, enter Gpedit.msc or use the Computer Management console. ◢ Use it to display and change policies controlling users and the computer.
Last Known Good Configuration	X	X	◢ Press F8 at startup and select from the Advanced Boot Options menu. ◢ Use this tool when Windows won't start normally and you want to revert the system to before a Windows setting, driver, or application that is causing problems was changed.
Memory Diagnostics (mdsched.exe)	X		◢ Enter mdsched.exe in a command prompt window. ◢ Use it to test memory.
Performance Monitor (Perfmon.msc)	X	X	◢ At a command prompt, enter Perfmon.msc. ◢ Use it to view information about performance to help you identify a performance bottleneck. ◢ Vista calls the tool the Reliability and Performance Monitor.
Program Compatibility Wizard	X	X	◢ Accessed by way of a desktop shortcut to a legacy application. ◢ Use it to resolve issues that prevent legacy software from working.
Programs and Features window	X		◢ Accessed from Control Panel. ◢ Use it to uninstall, repair, or update software or certain device drivers that are causing a problem.
Recovery Console		X	◢ Accessed from the Windows XP/2000 setup CD. ◢ Boot up this command-driven OS when you cannot boot from the hard drive. Use it to troubleshoot a Windows XP/2000 startup problem and recover data from the hard drive.
Registry Editor (Regedit.exe)	X	X	◢ At a command prompt, enter Regedit. ◢ Use it to view and edit the registry.

Table 15-1 Windows Vista/XP maintenance and troubleshooting tools (continued)

A+
220-701
2.2

Tool	Available in Win Vista	Available in Win XP	Description
Runas.exe	X	X	◢ At a command prompt, enter Runas with parameters. ◢ Use it to run a program using different permissions than those assigned to the currently logged-on user.
Safe Mode	X	X	◢ At startup, press F8 and select the option from the Advanced Boot Options menu. ◢ Use it when Windows does not start or starts with errors. Safe Mode loads the Windows desktop with a minimum configuration. In this minimized environment, you can solve a problem with a device driver, display setting, or corrupted or malicious applications.
SC (Sc.exe)	X	X	◢ At a command prompt, enter Sc with parameters. ◢ Use it to stop or start a service that runs in the background.
Services (Services.msc)	X	X	◢ At a command prompt, enter Services.msc. ◢ Graphical version of SC.
Software Explorer	X		◢ Accessed from the Windows Defender window. ◢ Use it to view and change programs launched at startup.
System Configuration Utility (Msconfig.exe)	X	X	◢ Enter Msconfig.exe in the Vista Start Search box or the XP Run box. ◢ Troubleshoot the startup process by temporarily disabling startup programs and services.
System File Checker (Sfc.exe)	X	X	◢ At a command prompt, enter Sfc with parameters. ◢ Use it to verify the version of all system files when Windows loads. Useful when you suspect system files are corrupted, but you can still access the Windows desktop.
System Information (Msinfo32.exe)	X	X	◢ Enter Msinfo32.exe in the Vista Start Search box or the XP Run box. ◢ Use it to display information about hardware, applications, and Windows.
System Information (Systeminfo.exe)	X	X	◢ At a command prompt, enter Systeminfo. ◢ A text-only version of the System Information window. To direct that information to a file, use the command Systeminfo.exe >Myfile.txt. Later the file can be printed and used to document information about the system.

Table 15-1 Windows Vista/XP maintenance and troubleshooting tools (continued)

A+
220-701
2.2

Tool	Available in Win Vista	Available in Win XP	Description
System Restore	X	X	◢ Accessed from the Start menu or when loading Safe Mode. ◢ Use it to restore the system to a previously working condition; it restores the registry, some system files, and some application files.
Task Killing Utility (Tskill.exe)	X	X	◢ At a command prompt, enter Tskill with parameters. ◢ Use it to stop or kill a process or program currently running. Useful when managing background services such as an e-mail server or Web server.
Task Lister (Tasklist.exe)	X	X	◢ At a command prompt, enter Tasklist. ◢ Use it to list currently running processes similar to the list provided by Task Manager.
Task Manager (Taskman.exe)	X	X	◢ Right-click the taskbar and select Task Manager. ◢ Use it to list and stop currently running processes. Useful when you need to stop a locked-up application.
Windows Defender	X		◢ Accessed from Control Panel. ◢ Monitors activity and alerts you if a running program appears to be malicious or damaging the system.
Windows File Protection	X	X	◢ Windows background service ◢ Runs in the background to protect system files and restore overwritten system files as needed.
Windows Firewall	X	X	◢ Service that runs in the background to prevent or filter uninvited communication from another computer.
Windows Recovery Environment (recenv.exe)	X		◢ Windows RE is an OS loaded from the Vista setup DVD, which provides a graphic and command-line interface. ◢ Use the tool to solve Vista startup problems.
Windows Update (Wupdmgr.exe)	X	X	◢ Accessed from the Start menu. ◢ Use it to update Windows by downloading the latest patches from the Microsoft Web site.

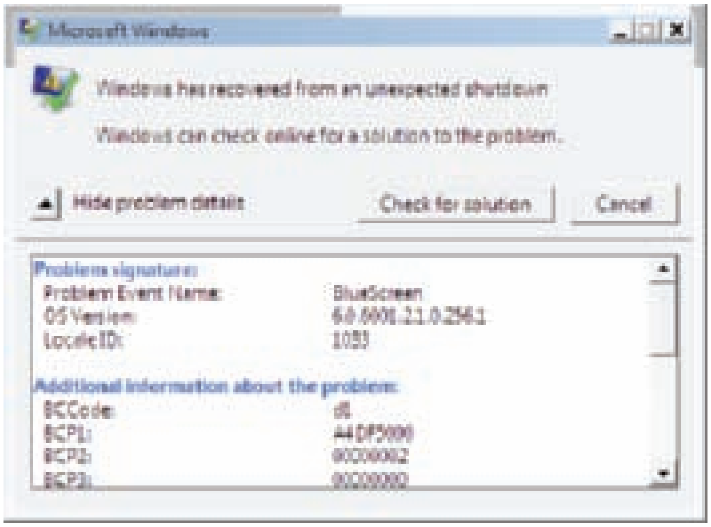
Table 15-1 Windows Vista/XP maintenance and troubleshooting tools (continued)

A+
220-701
2.2

A+ Exam Tip If an often-used Windows utility can be launched from a command prompt, the A+ 220-701 Essentials exam expects you to know the program name of that utility.

VISTA PROBLEM REPORTS AND SOLUTIONS

Use the Windows Vista Problem Reports and Solutions tool to deal with an immediate hardware or software problem and use its history feature to help you understand the history of a specific problem or the general history of problems with the system. When a problem occurs, Vista Error Reporting displays an error screen and invites you to check for a solution. If the problem happens in the kernel mode of Windows, a STOP or blue screen error occurs, and the error screen appears on the next restart. For example, after a STOP error occurred on one system and the system was restarted, the screen in Figure 15-1 appeared. If the user clicks **Check for solution**, Microsoft displays information about the problem and its solution. User mode errors that don't produce a STOP error can appear as a bubble in the notification area (see Figure 15-2). Click the bubble to see possible solutions for the problem. One such solution is shown in Figure 15-3.



Microsoft Windows

Windows has recovered from an unexpected shutdown

Windows can check online for a solution to the problem.

Problem signature:

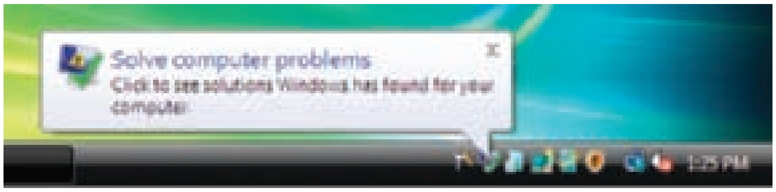
Problem Event Name:	BlueScreen
OS Version:	6.0.6001.2.1.0.256.1
Locale ID:	1033

Additional information about the problem:

BCCode:	d1
BCP1:	A4DF5000
BCP2:	0C000002
BCP3:	0C000000

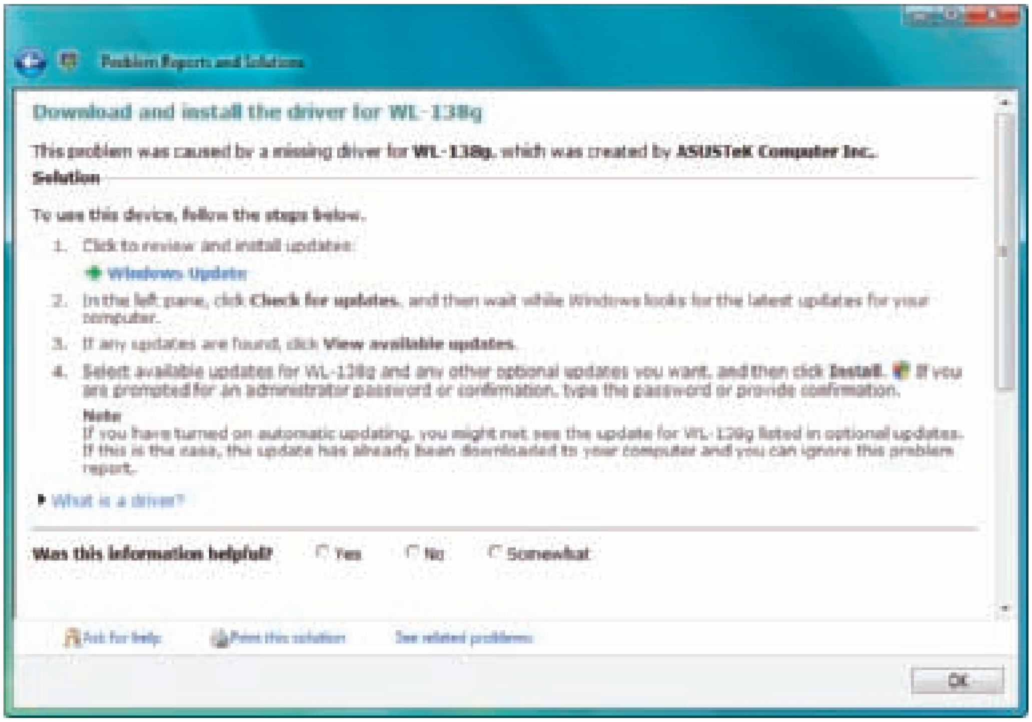
Figure 15-1 Windows reports information about an error
Courtesy: Course Technology/Cengage Learning

When a problem occurs, Windows records the error and possible solutions. Some of these solutions might not have yet been tried. To see a list of solutions that have not yet been applied for known problems, click **Start**, click **All Programs**, click **Maintenance**, and click **Problem Reports and Solutions**. The Problem Reports and Solutions window in Figure 15-4 appears. Click an item in the list to get more details and possibly apply the solution. Click **Check for new solutions** to send information to Microsoft and possibly find new solutions to known problems. These new solutions to old problems appear with the red word "New" in the figure.



Solve computer problems
Click to see solutions Windows has found for your computer.

Figure 15-2 Vista error reporting gives an error alert
Courtesy: Course Technology/Cengage Learning



Download and install the driver for WL-138g

This problem was caused by a missing driver for **WL-138g**, which was created by **ASUSTeK Computer Inc.**

Solution

To use this device, follow the steps below.

1. Click to review and install updates:

   Windows Update

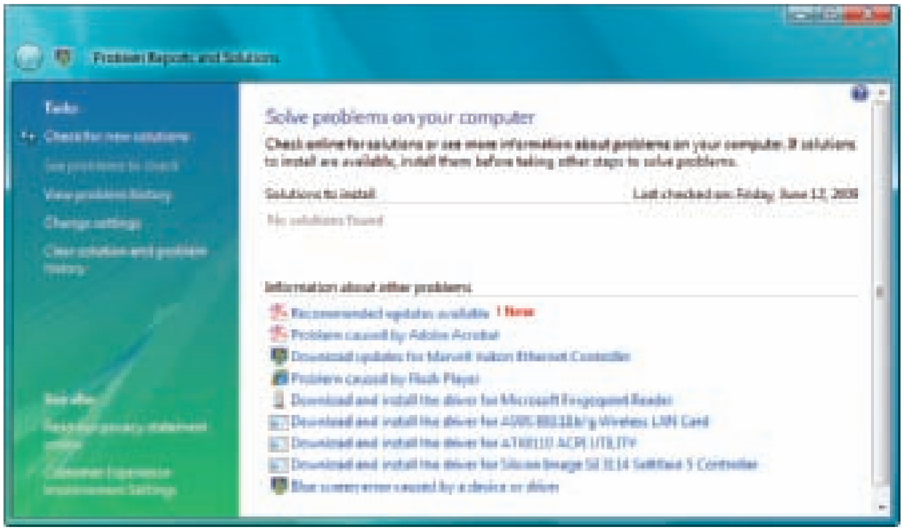
2. In the left pane, click **Check for updates**, and then wait while Windows looks for the latest updates for your computer.
3. If any updates are found, click **View available updates**.
4. Select available updates for WL-138g and any other optional updates you want, and then click **Install**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

   Note
   If you have turned on automatic updating, you might not see the update for WL-138g listed in optional updates. If this is the case, the update has already been downloaded to your computer and you can ignore this problem report.

What is a driver?

Was this information helpful? ○ Yes ○ No ○ Somewhat

Figure 15-3 Microsoft gives suggestions for a solution to a problem
Courtesy: Course Technology/Cengage Learning



Problem Reports and Solutions
Tasks
Check for new solutions
See problems to check
View problem history
Change settings
Clear solution and problem history
See also
Read our privacy statement online
Customer Experience Improvement Settings

Solve problems on your computer

Check online for solutions or see more information about problems on your computer. If solutions to install are available, install them before taking other steps to solve problems.

Solutions to install Last checked on: Friday, June 12, 2009

No solutions found

Information about other problems

- Recommended updates available ! New
- Problem caused by Adobe Acrobat
- Download updates for Marvell Yukon Ethernet Controller
- Problems caused by Flash Player
- Download and install the driver for Microsoft Fingerprint Reader
- Download and install the driver for ASUS 802.11b/g Wireless LAN Card
- Download and install the driver for ATK0110 ACPI UTILITY
- Download and install the driver for Silicon Image SiI 3114 SATARaid 5 Controller
- Blue screen error caused by a device or driver

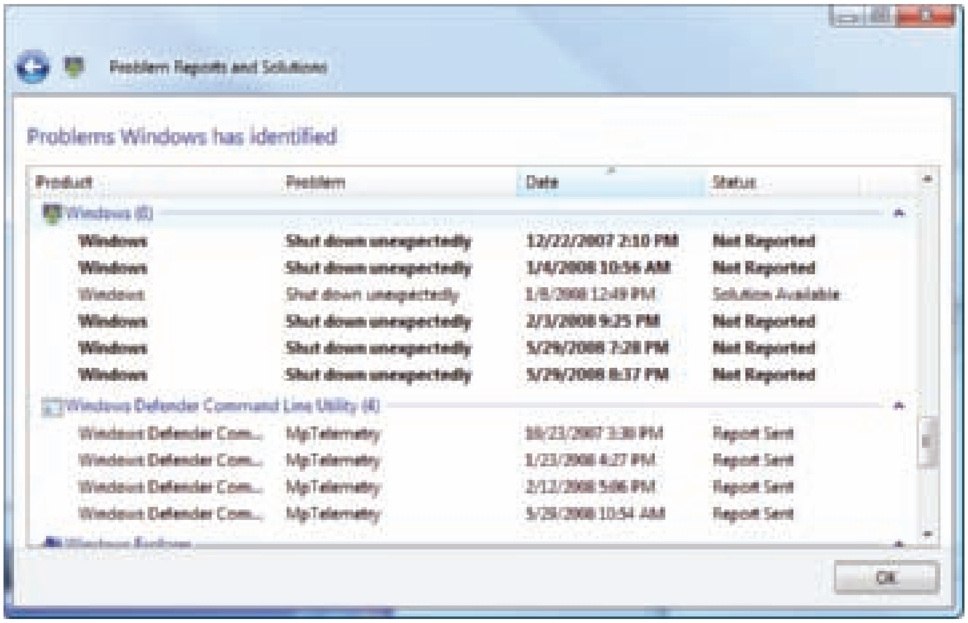
Figure 15-4 Known problems and solutions
Courtesy: Course Technology/Cengage Learning

To see a history of past problems, click **View problem history**; the window in Figure 15-5 appears. Problems are listed by category. Click a problem to see details about the problem. This window is a great tool if you need to understand the history of problems on a computer that you are troubleshooting.

XP ERROR REPORTING

Windows XP offers a similar tool, called Error Reporting. When XP encounters a problem with an application, one thing it might do is display a message about the problem similar to the one shown in Figure 15-6. If you are connected to the Internet, you can click **Send Error Report** to

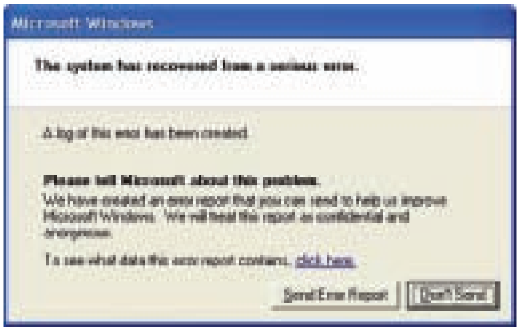
A+
220-701
2.2


Problem Reports and Solutions

Problems Windows has identified

Product	Problem	Date	Status
Windows (6)			
Windows	Shut down unexpectedly	12/22/2007 2:10 PM	Not Reported
Windows	Shut down unexpectedly	1/4/2008 10:56 AM	Not Reported
Windows	Shut down unexpectedly	1/8/2008 12:49 PM	Solution Available
Windows	Shut down unexpectedly	2/3/2008 9:25 PM	Not Reported
Windows	Shut down unexpectedly	5/29/2008 7:28 PM	Not Reported
Windows	Shut down unexpectedly	5/29/2008 8:37 PM	Not Reported
Windows Defender Command Line Utility (4)			
Windows Defender Com...	MpTelemetry	10/23/2007 3:38 PM	Report Sent
Windows Defender Com...	MpTelemetry	1/23/2008 4:27 PM	Report Sent
Windows Defender Com...	MpTelemetry	2/12/2008 5:06 PM	Report Sent
Windows Defender Com...	MpTelemetry	5/28/2008 10:54 AM	Report Sent
Windows Explorer			

Figure 15-5 Use the Problem Reports and Solutions tool to view a history of past problems
Courtesy: Course Technology/Cengage Learning


Microsoft Windows

The system has recovered from a serious error.

A log of this error has been created.

Please tell Microsoft about this problem.
We have created an error report that you can send to help us improve Microsoft Windows. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

Figure 15-6 A serious Windows error sometimes generates this
Microsoft Windows error reporting box
Courtesy: Course Technology/Cengage Learning

get suggestions about the problem from Microsoft. Microsoft will also use the information you send to help with future Windows updates and patches.

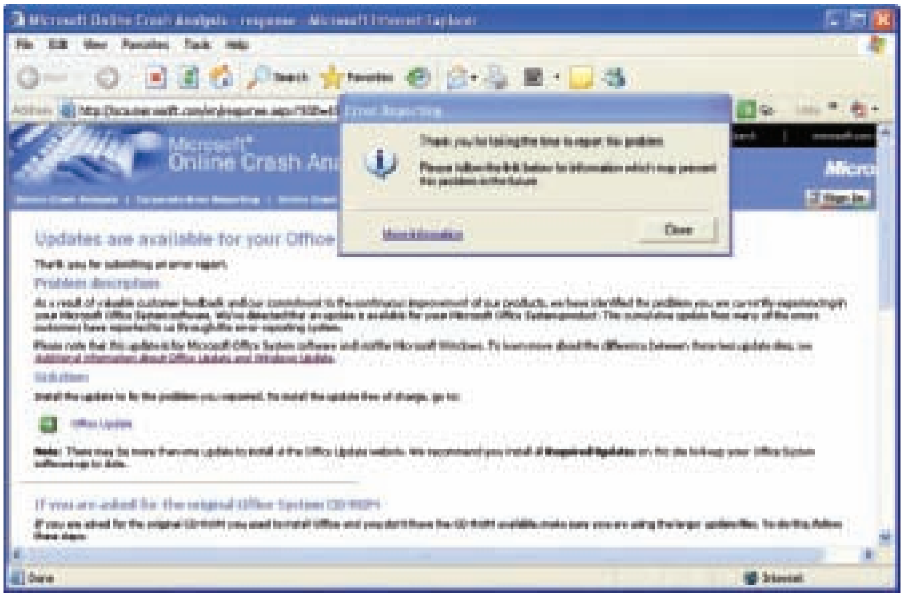
After the information is sent, a dialog box similar to the one in Figure 15-7 appears. Click **More information** to see Microsoft insights and suggestions about the problem. Your browser will open and display information from Microsoft. If the problem is caused by a Microsoft product such as Internet Explorer or Microsoft Office, sometimes the Web site will point you to a patch you can download to fix the problem. An example of an available patch is also shown in Figure 15-7.

The XP Error Reporting does not keep a history of previous errors as does the Vista Problem Reports and Solutions tool.

MEMORY DIAGNOSTICS

Errors with memory are often difficult to diagnose because they can appear intermittently and might be mistaken as application errors, user errors, or other hardware component errors. Sometimes these errors cause the system to hang, a blue screen error might occur, or the system continues to function with applications giving errors or data getting corrupted. You can quickly identify a problem with memory or eliminate memory as the source of a problem by

A+
220-701
2.2


Microsoft Online Crash Analysis - response - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search
Favorites
Address
Go
Microsoft Online Crash Analysis
Sign In
Error Reporting
More information
Close
Done
Internet

Thank you for taking the time to report this problem

Please follow the link below for information which may prevent the problem in the future

Updates are available for your Office

Thank you for submitting an error report.

Problem description

As a result of valuable customer feedback and our commitment to the continuous improvement of our products, we have identified the problem you are currently experiencing with your Microsoft Office System software. We've detected that an update is available for your Microsoft Office System product. The cumulative update fixes many of the errors customers have reported to us through the error reporting system.

Please note that this update is for Microsoft Office System software and not the Microsoft Windows. To learn more about the differences between these two update sites, see Additional information about Office Update and Windows Update.

Solution

Install the update to fix the problem you reported. To install the update free of charge, go to:

Office Update

Note: There may be more than one update to install at the Office Update website. We recommend you install all **Required Updates** on the site to keep your Office System software up to date.

If you are asked for the original Office System CD-ROM

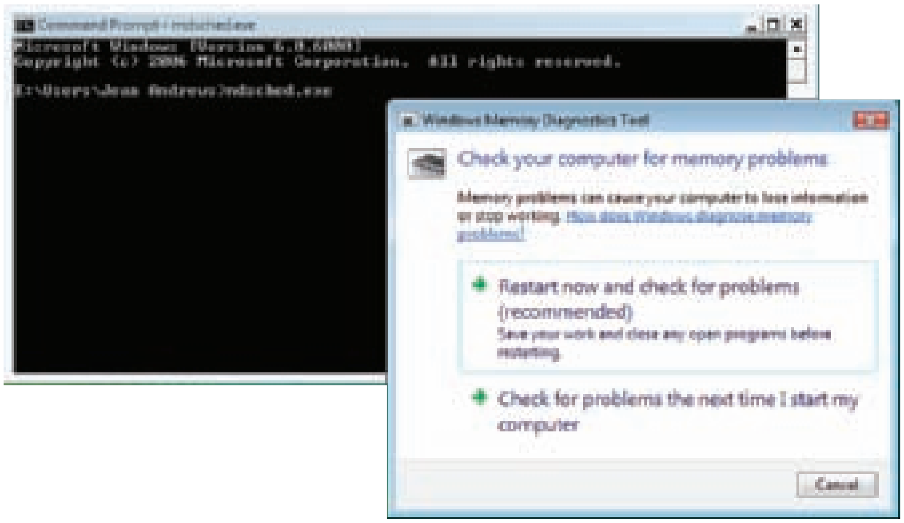
If you are asked for the original CD-ROM you used to install Office and you don't have the CD-ROM available, make sure you are using the larger update files. To do this, follow these steps:

Figure 15-7 Click More information to see Microsoft insights into a problem
Courtesy: Course Technology/Cengage Learning

using the Vista Memory Diagnostics tool. It tests memory for errors and works before Windows Vista is loaded. The diagnostic test can be initiated using one of these four methods:

Method 1: If Vista Error Reporting detects that memory might be failing, the utility will prompt the user to test memory on the next reboot. If the user agrees by clicking **Check for problems the next time you start your computer**, then diagnostic tests are run on the next restart. After the Windows desktop loads, a bubble message appears giving the test results. If the test shows that memory is giving errors, replace the memory modules.

Method 2: You can test memory at any time using the command prompt. To do so, click **Start, All Programs, Accessories, Command Prompt**. The Command Prompt window opens. Type **mdsched.exe**, press **Enter**, and respond to the UAC box. In the dialog box that appears (see Figure 15-8), you can choose to run the test now or on the next restart.



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Jean Andrews>mdsched.exe
```

Check your computer for memory problems

Memory problems can cause your computer to lose information or stop working. How does Windows diagnose memory problems?

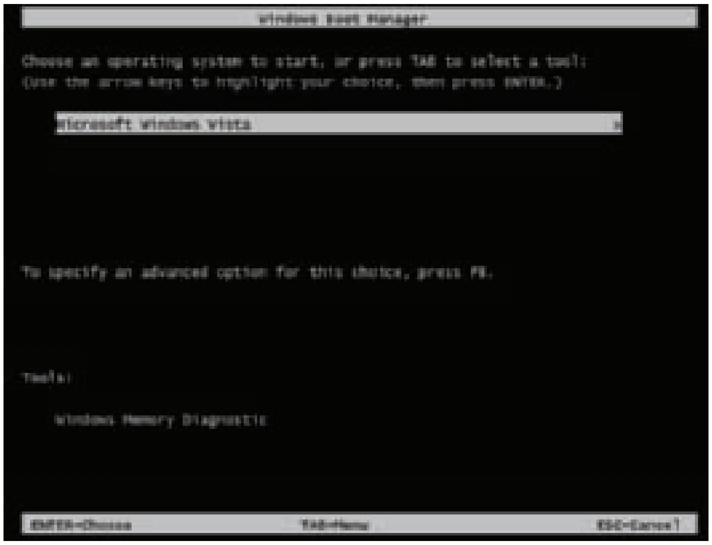
Restart now and check for problems (recommended)
Save your work and close any open programs before restarting.

Check for problems the next time I start my computer

Figure 15-8 Use the mdsched.exe command to test memory
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

Method 3: When troubleshooting a failed system, if the Windows Vista desktop cannot load, you can run the memory diagnostic test from the Windows Vista boot menu. This menu normally is displayed with a dual-boot configuration so you can select the OS to load. If you are not using a dual-boot machine, you can force the menu to be displayed by pressing the Spacebar during the boot. The resulting menu appears, as shown in Figure 15-9. Use the Tab key to highlight the option **Windows Memory Diagnostic** and press **Enter**.



```
                         Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    Microsoft Windows Vista                                      >




To specify an advanced option for this choice, press F8.




Tools:

    Windows Memory Diagnostic



ENTER=Choose                    TAB=Menu                    ESC=Cancel
```

Figure 15-9 Force the Windows Boot Manager menu to display by pressing the Spacebar during the boot
Courtesy: Course Technology/Cengage Learning

Method 4: For any computer that has a DVD drive, you can run the test using the Windows Vista DVD, even if the computer is using a different OS than Vista, by doing the following:

1. Boot from the Vista DVD. On the window that appears, select your language preference and click **Next**.
2. On the opening menu of the Vista DVD, click **Repair your computer**, as shown in Figure 15-10. In the next box, select the Vista installation to repair and click **Next**.

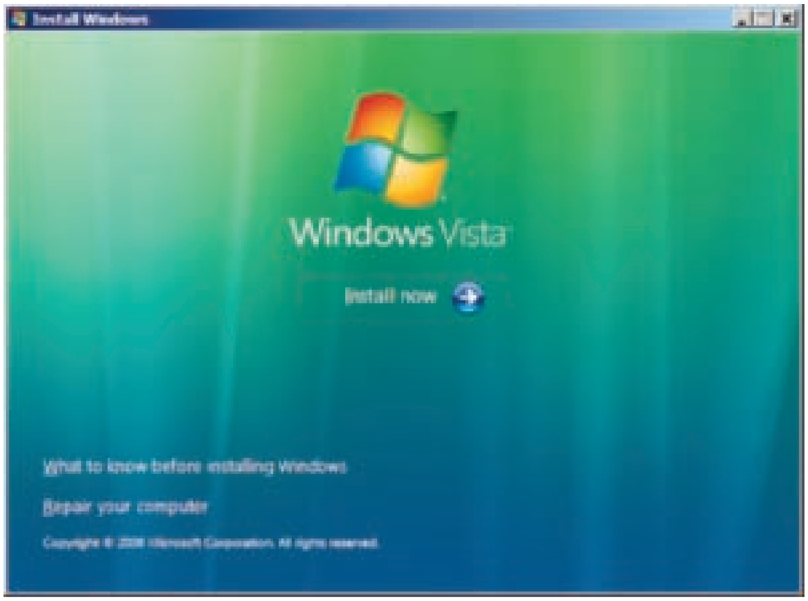
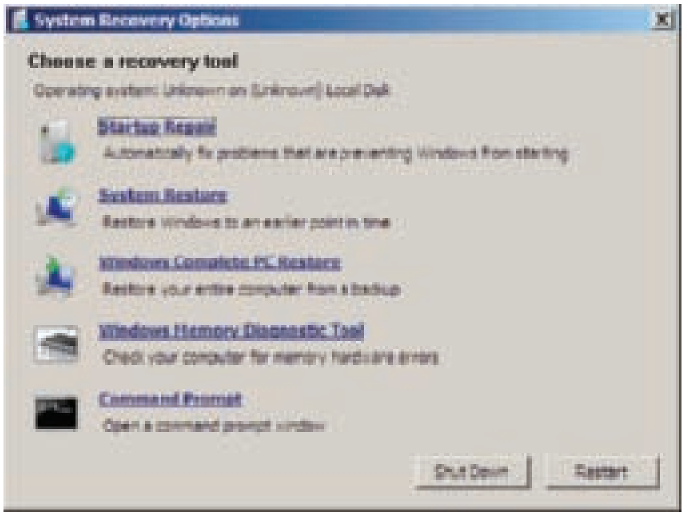

Install Windows
Windows Vista
Install now
What to know before installing Windows
Repair your computer
Copyright © 2006 Microsoft Corporation. All rights reserved.

Figure 15-10 Opening menu when you boot from the Vista DVD
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

3. The System Recovery Options window appears (see Figure 15-11). Click **Windows Memory Diagnostic Tool**.



System Recovery Options

Choose a recovery tool

Operating system: Unknown on (Unknown) Local Disk

Startup Repair
Automatically fix problems that are preventing Windows from starting

System Restore
Restore Windows to an earlier point in time

Windows Complete PC Restore
Restore your entire computer from a backup

Windows Memory Diagnostic Tool
Check your computer for memory hardware errors

Command Prompt
Open a command prompt window

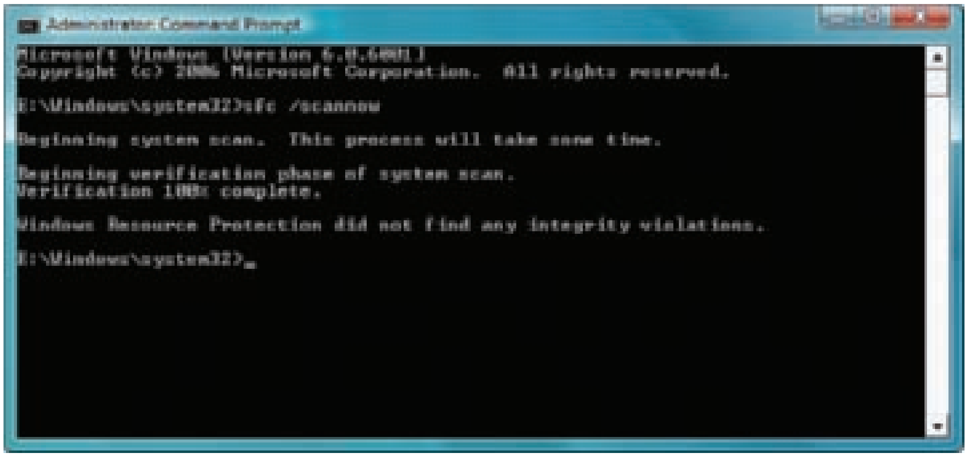
Figure 15-11 Test memory using the System Recovery Options menu
Courtesy: Course Technology/Cengage Learning

4. On the next window, click **Restart now and check for problems (recommended)**. The system will reboot and the memory test will start.

When the Vista desktop refuses to load but you can boot from the hard drive to the Vista boot menu, use Method 3. If you cannot boot from the hard drive or if Vista is not installed on the drive, use Method 4.

SYSTEM FILE CHECKER

A Windows application or hardware problem might be caused by a corrupted Windows system file. That's where System File Checker might help. System File Checker (SFC) is a Windows Vista and XP utility that protects system files and keeps a cache of current system files in case it needs to refresh a damaged file. To use the utility to scan all system files and verify them, first close all applications and then enter the command **sfc /scannow** in a command prompt window (see Figure 15-12). For Vista, use an elevated



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

E:\Windows\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.

E:\Windows\system32>_
```

Figure 15-12 Use System File Checker to verify Windows system files
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

command prompt window. If corrupted system files are found, you might need to provide the Windows setup CD or DVD to restore the files. If you have problems running the utility, try the command **sfc/ scanonce**, which scans files immediately after the next reboot.

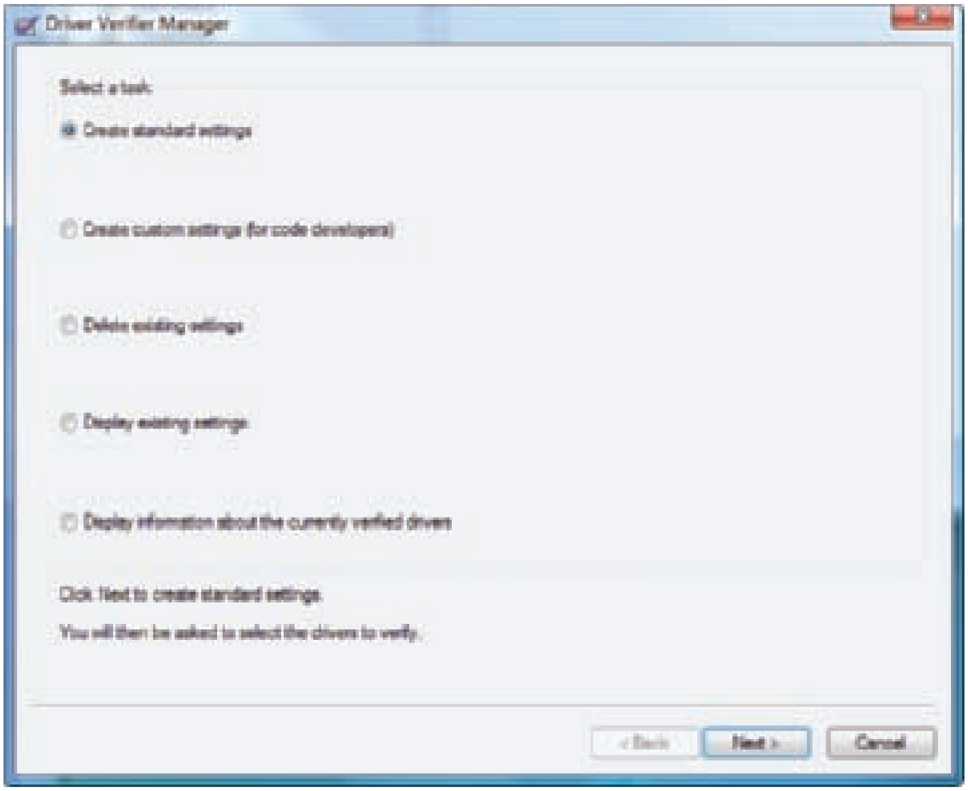
Tip Recall from Chapter 13 that you can get an elevated command prompt window in Vista by clicking **Start**, **All Programs**, and **Accessories**. Then right-click **Command Prompt** and select **Run as administrator** from the shortcut menu.

DRIVER VERIFIER

For hardware problems, Driver Verifier (verifier.exe) is a Windows Vista/XP/2000 utility that runs in the background to put stress on drivers as they are loaded and running. When a problem occurs, a STOP error is generated so you can identify the problem driver. The tool is useful for troubleshooting intermittent problems that are not easily detected by other means.

To use Driver Verifier to monitor drivers, follow these steps:

1. Click **Start**, enter **verifier.exe** in the Start Search box, press **Enter**, and respond to the UAC box. The Driver Verifier Manager window opens (see Figure 15-13).



Driver Verifier Manager

Select a task:

● Create standard settings

○ Create custom settings (for code developers)

○ Delete existing settings

○ Display existing settings

○ Display information about the currently verified drivers

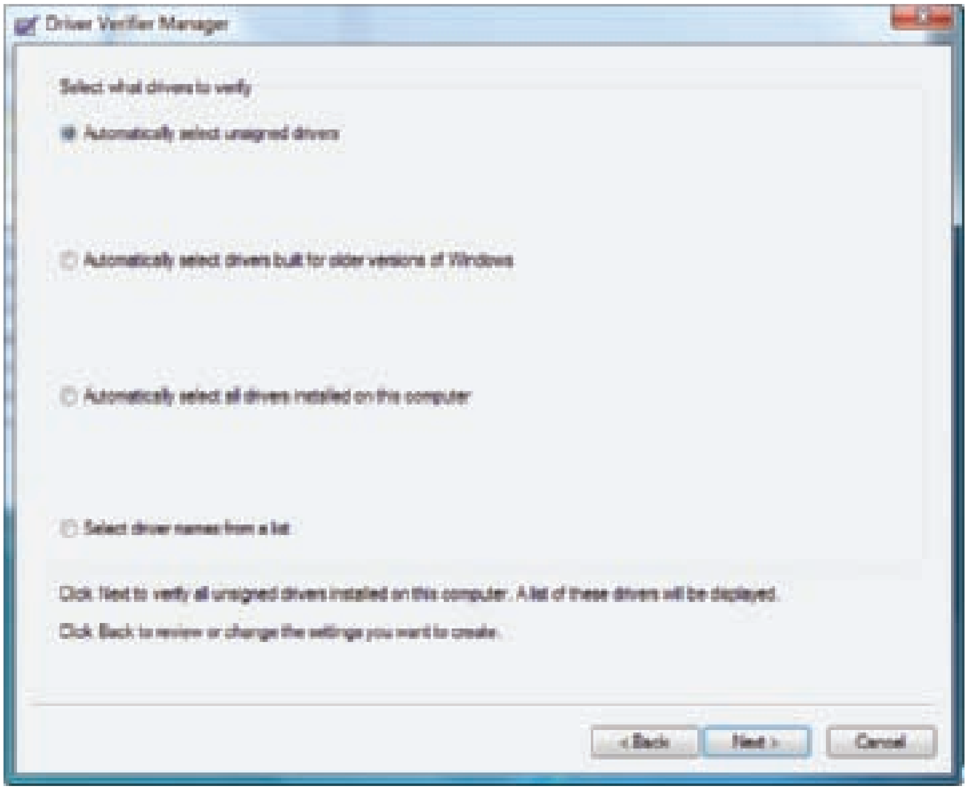
Click Next to create standard settings.

You will then be asked to select the drivers to verify.

Figure 15-13 Configure Driver Verifier to test drivers
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

2. Select **Create standard settings** and click **Next**. The window in Figure 15-14 appears.



Driver Verifier Manager

Select what drivers to verify

● Automatically select unsigned drivers

○ Automatically select drivers built for older versions of Windows

○ Automatically select all drivers installed on this computer

○ Select driver names from a list

Click Next to verify all unsigned drivers installed on this computer. A list of these drivers will be displayed.

Click Back to review or change the settings you want to create.

Figure 15-14 Select the type of drivers for Driver Verifier to test
Courtesy: Course Technology/Cengage Learning

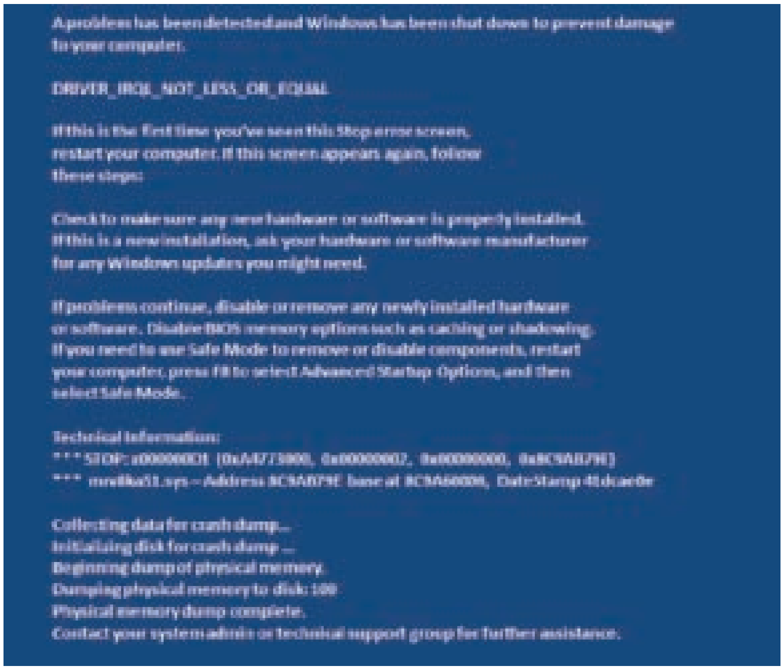
3. Depending on what you suspect to be the problem with your hardware, you need to select which type of drivers to monitor (unsigned drivers, older drivers, all drivers, or specific drivers that you can select from a list that appears on the next screen). If you are not sure which ones, to be on the safe side, select **Automatically select all drivers installed on this computer**. (When you do that, the Next in the window changes to Finish.) Then click **Finish**. However, be aware that the more drivers the utility monitors, the more system performance will be affected.

4. Restart the system.

Driver Verifier attempts to overload the drivers it monitors, which can cause a STOP error. The STOP error message tells you which driver caused the error, thus identifying a driver with problems. For example, Figure 15-15 shows a STOP error screen caused during startup by the driver, mrv8ka51.sys. Which device does this driver belong to? There are several ways to get at that information; one way is to look at the file Properties box. First find the file in the C:\Windows\System32\drivers folder. Right-click the file and select **Properties** from the shortcut menu. In the file Properties box, select the **Details** tab, which shows that this driver file belongs to the wireless adapter (see Figure 15-16). The next step to fix the problem is to update the driver.

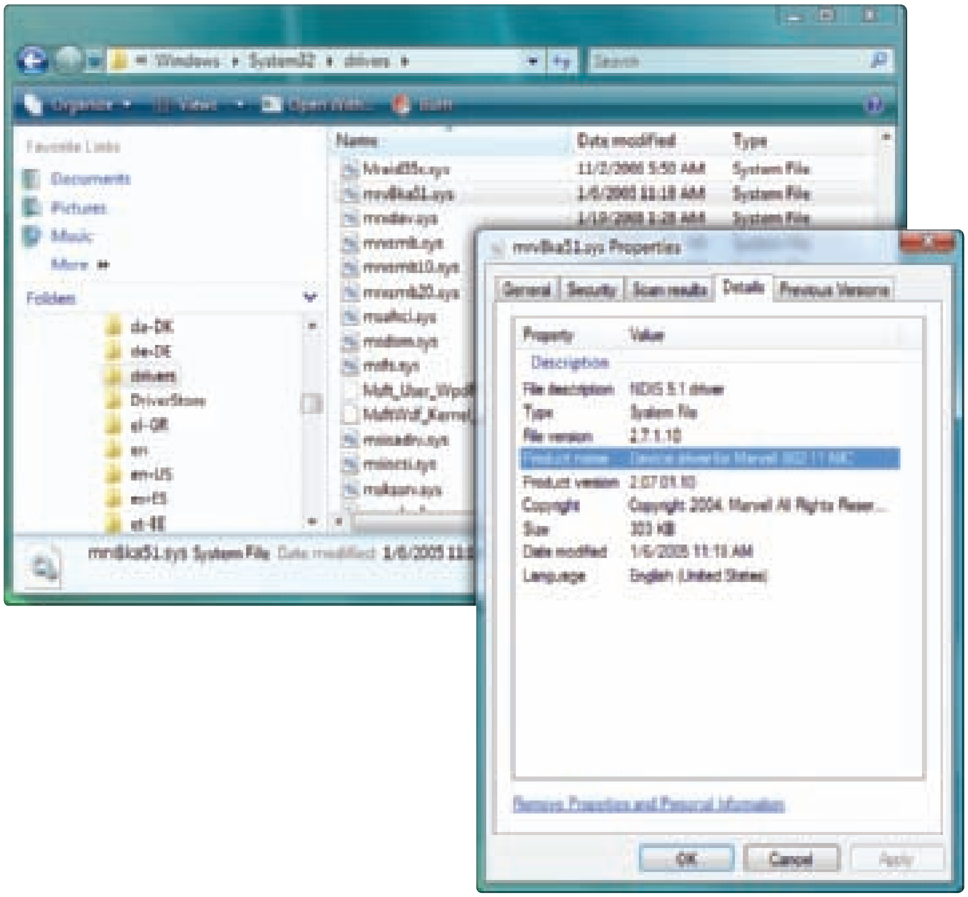
After Driver Verifier has located the problem, to turn it off, click **Start**, enter **verifier.exe** in the Start Search box, press **Enter**, and respond to the UAC box. The Driver Verifier Manager window opens (refer to Figure 15-13). Select **Delete existing settings** and click **Finish**. Click **Yes** in the warning box, and then click **OK**. Restart your computer.

A+
220-701
2.2



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

DRIVER_IRQL_NOT_LESS_OR_EQUAL

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 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: 0x000000D1 (0xA4773000, 0x00000002, 0x00000000, 0x8C9AB79E)
***  mrvlka51.sys – Address 8C9AB79E base at 8C9A0000, DateStamp 41dcae0e

Collecting data for crash dump...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Figure 15-15 This blue screen STOP error message identifies the driver file causing a problem
Courtesy: Course Technology/Cengage Learning



Name	Date modified	Type
Mraid35x.sys	11/2/2006 5:50 AM	System File
mrvlka51.sys	1/6/2005 11:18 AM	System File
mrxdav.sys	1/19/2008 1:28 AM	System File
mrxsmb.sys		
mrxsmb10.sys		
mrxsmb20.sys		
msahci.sys		
msdsm.sys		
msfs.sys		
Msft_User_Wpd...		
MsftWdf_Kernel...		
msisadrv.sys		
msiscsi.sys		
mskssrv.sys		

mrvlka51.sys System File Date modified: 1/6/2005 11:1...

mrvlka51.sys Properties

Property	Value
Description	
File description	NDIS 5.1 driver
Type	System File
File version	2.7.1.10
Product name	Device driver for Marvell 802.11 NIC
Product version	2.07.01.10
Copyright	Copyright 2004, Marvell All Rights Reser...
Size	303 KB
Date modified	1/6/2005 11:18 AM
Language	English (United States)

Figure 15-16 The file Properties box reports the driver product information
Courtesy: Course Technology/Cengage Learning

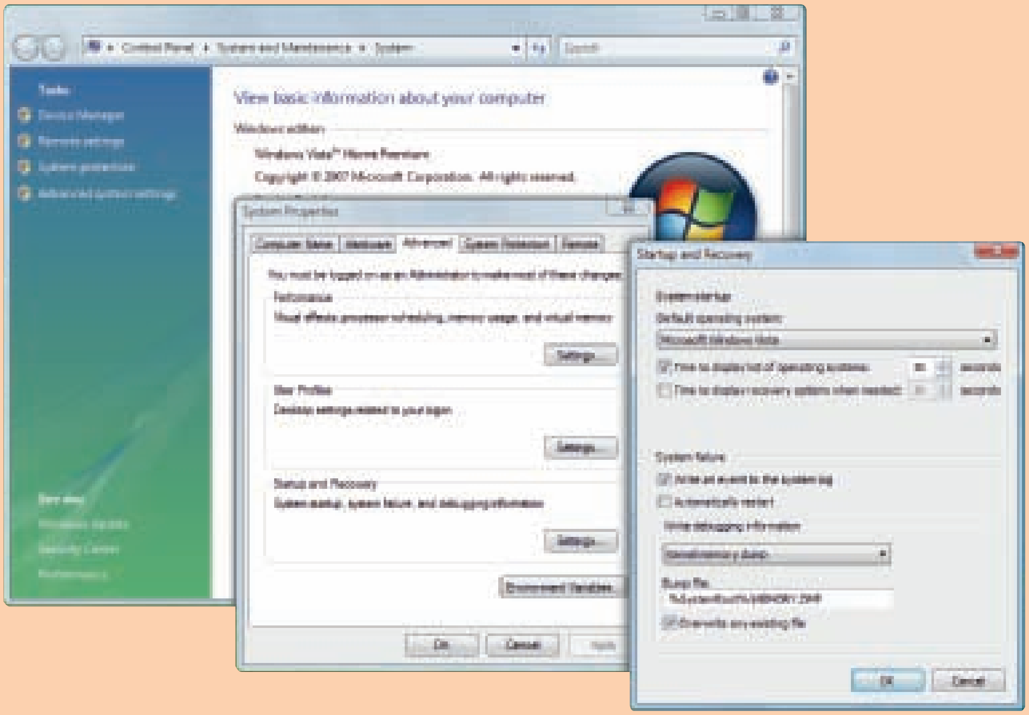
A+
220-701
2.2

If Driver Verifier runs for a few days and has still not found the problem, it probably will not help you. Turn it off so that it will not continue to degrade system performance. One other caution: If the computer is a file server that many users depend on for top performance, consider the problems you might cause these users before you decide to use the Driver Verifier.

APPLYING CONCEPTS STARTUP AND RECOVERY SETTINGS TO GET OUT OF AN ENDLESS LOOP

Remember that STOP error that happened during startup and is shown in Figure 15-15? With normal Windows settings, if a STOP error occurs during startup, the system displays the error screen for a moment and then automatically restarts the system, which can result in an endless cycle of restarts, which is exactly what happened in this example with the wireless adapter problem. The support technician got around the problem by booting the system into Safe Mode, which did not load Driver Verifier, and, therefore, allowed the Windows desktop to load. Then she changed the setting that caused Windows to automatically restart. Here's how to change that setting:

1. Click **Start**, right-click **Computer**, and select **Properties** from the shortcut menu.
2. In the System window (see the upper part of Figure 15-17), click **Advanced system settings** and respond to the UAC box. (For Windows XP, in the System Properties window, click the **Advance** tab.)
3. In the System Properties box (see the lower-left of Figure 15-17) in the Startup and Recovery section, click **Settings**.



☑ Write an event to the system log
☐ Automatically restart

Figure 15-17 Use the Startup and Recovery box to change the way Windows responds to a STOP error during startup
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

4. In the Startup and Recovery box (see the lower-right of Figure 15-17), uncheck **Automatically restart**. Click **OK** twice to close both boxes. Then close the System window.

Next, she restarted the system normally. This time the STOP error remained frozen on-screen so that she could read it. After she wrote down the information she needed, she restarted the system again in Safe Mode and this time stopped Driver Verifier. Then she restarted Windows normally, located the driver, and updated it. The process required a lot of restarts, but it did find the driver causing the problem.

TOOLS TO VERIFY DRIVER SIGNATURES

Boot problems, an unstable Windows system, or error messages might be caused by drivers that Microsoft has not validated and are not digitally signed or by drivers that have changed since they were signed. If you suspect a problem with a driver, do one of the following to verify that it is digitally signed by Microsoft:

- *Use the File Signature Verification tool*. The **File Signature Verification** tool displays information about digitally signed files, including device driver files and application files, and logs information to C:\Windows\Sigverif.txt. To use the tool, type the **sigverif.exe** command in the Vista Start Search box or the XP Run box.
- *Use the Driver Query tool*. The **Driver Query** tool can be used to direct information about drivers to a file, including information about digital signatures. Enter this command in the Vista Start Search box or the XP Run box: **driverquery /si >myfile.txt**. The file will be stored in the default drive and directory unless you specify some other path.
- *Use Device Manager*. If you know which device is causing a problem, use Device Manager. In the device's Properties dialog box, the digital signature information is given on the Driver tab.

Notes Use the Driver Query tool to save information about your system to a file when the system is healthy. Later, if you have a problem with drivers, you can compare reports to help identify the problem driver.

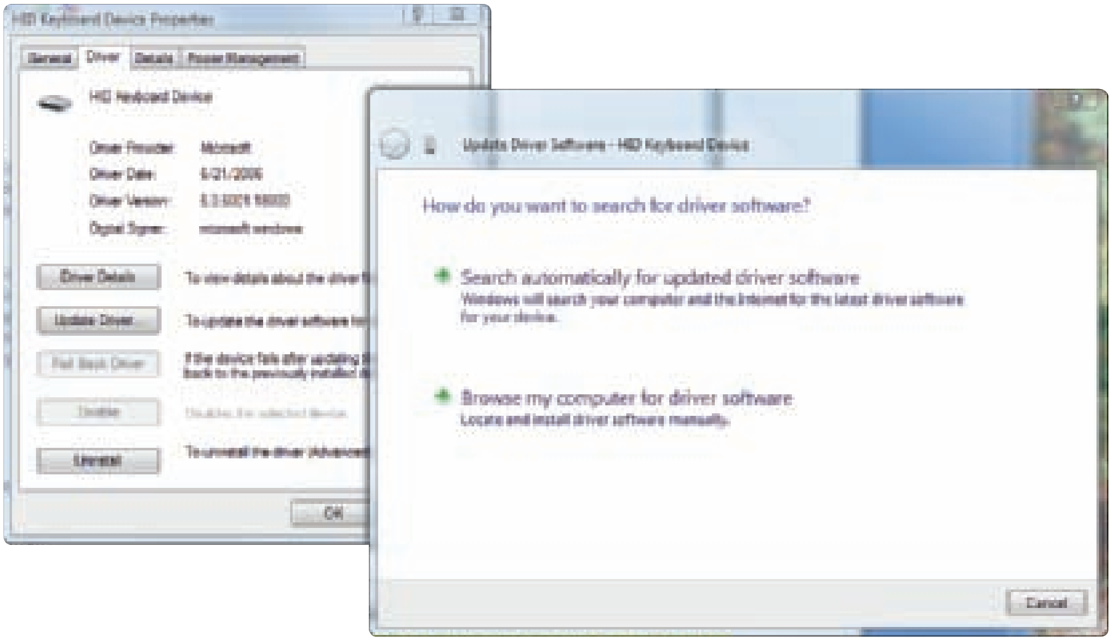
A+
220-701
2.2
2.5

USE DEVICE MANAGER TO UPDATE AND ROLL BACK DRIVERS

Suppose you install a new application on your computer and the function keys on your keyboard don't work the way the application says they should. Or suppose you read that your sound card manufacturer has just released a driver update for your card and you want to try it out. Both of these situations are good reasons to try the Update Driver process. Here's how to use Device Manager to update the drivers for a device:

1. Locate drivers for your device and have the CD handy or download the driver files from the manufacturer's Web site to your hard drive.
2. Using Device Manger, right-click the device and select **Properties** from the shortcut menu. The Properties window for that device appears. Select the **Driver** tab and click **Update Driver**. The Update Driver Software box opens (see Figure 15-18).

A+
220-701
2.2
2.5



HID Keyboard Device Properties

General | Driver | Details | Power Management

HID Keyboard Device

Driver Provider: Microsoft
Driver Date: 6/21/2006
Driver Version: 6.0.6001.18000
Digital Signer: microsoft windows

Driver Details — To view details about the driver f
Update Driver — To update the driver software fo
Roll Back Driver — If the device fails after updating t back to the previously installed d
Disable — Disables the selected device
Uninstall — To uninstall the driver (Advanced

OK

Update Driver Software - HID Keyboard Device

How do you want to search for driver software?

Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device.

Browse my computer for driver software
Locate and install driver software manually.

Cancel

Figure 15-18 Use Device Manager properties box to uninstall, update, and roll back drivers
Courtesy: Course Technology/Cengage Learning

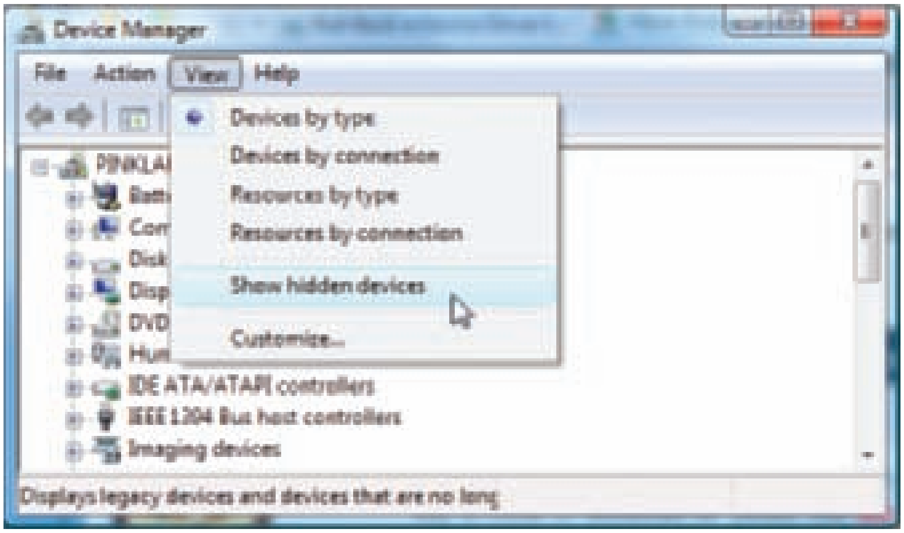
3. To search the Internet for drivers, click **Search automatically for updated driver software**. (Vista searches the Microsoft Web site and the manufacturer's Web site, but XP searches only the Microsoft Web site for drivers.) If you have already downloaded drivers to your PC, click **Browse my computer for driver software,** and point to the downloaded files. Remember, Windows is looking for an .inf file to identify the drivers. Continue to follow the directions on-screen to complete the installation.

Notes Using Windows Vista, you cannot use Device Manager without responding correctly to the UAC box. For Windows XP, you must be logged on with administrator privileges to make changes from Device Manager.

If you update a driver and the new driver does not perform as expected, you can revert to the old driver by using the Driver Rollback feature. To revert to a previous driver, open the Properties window for the device (see the left side of Figure 15-18), and click **Roll Back Driver**. If a previous driver is available, it will be installed. In many cases, when a driver is updated, Windows saves the old driver in case you want to revert to it. Keep in mind that Windows does not save printer drivers when they are updated and also doesn't save drivers that are not functioning properly at the time of an update.

Notes By default, Device Manager hides legacy devices that are not Plug and Play. To view installed legacy devices, click the **View** menu of Device Manager, and check **Show hidden devices** (see Figure 15-19).

A+
220-701
2.2
2.5



Displays legacy devices and devices that are no long

Figure 15-19 By default, Windows does not display legacy devices in Device Manager; you show these hidden devices by using the View menu
Courtesy: Course Technology/Cengage Learning

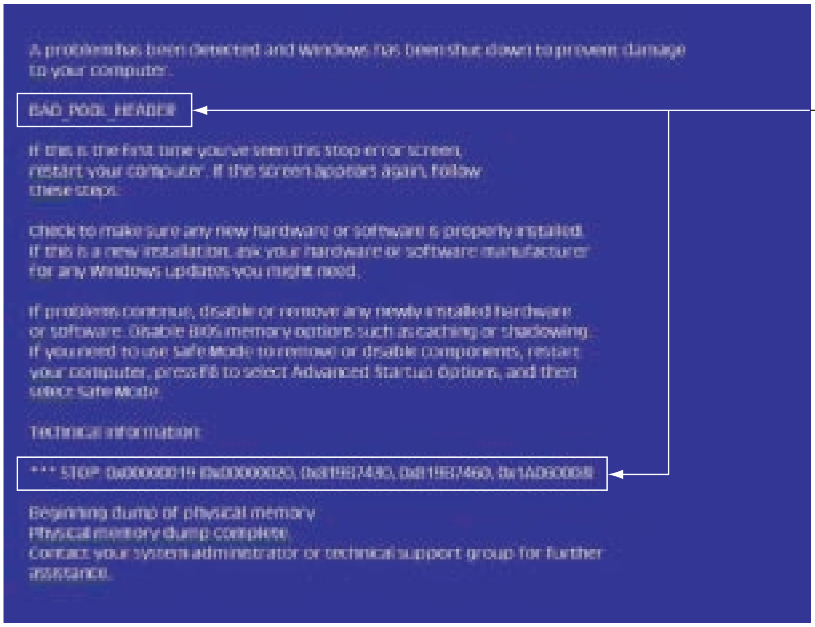
A+
220-701
2.2

UTILITIES BUNDLED WITH A HARDWARE DEVICE

Many devices come with diagnostic utilities included on the setup CD. Sometimes these utilities are installed when you install the device, and sometimes you need to launch the utility from the setup CD. When you have problems with a device, look for this utility either in the Start, All Programs menu or on the setup CD. Use it to test and diagnose problems with the device.

TYPES OF ERRORS AND TOOLS TO USE

Recall that a blue screen error happens when processes running in kernel mode encounter a problem and Windows must stop the system. In such situations, a blue screen appears with a cryptic error message such as the one in Figure 15-20. This particular blue screen appeared a few seconds



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

BAD_POOL_HEADER

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 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: 0x00000019 (0x00000020, 0x81987430, 0x81987460, 0x1A060008)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

For more information, search the Microsoft Web site on these two items

Figure 15-20 A blue screen of death (BSOD) is definitively not a good sign; time to start troubleshooting
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2

after a USB wireless adapter was plugged into a notebook computer. Look on the blue screen for the stop error at the top and the specific number of the error near the bottom of the screen, as labeled in Figure 15-20. For more information about a blue screen, search the Microsoft Web site on these two items. As for the tools useful in solving blue screen errors, put the Internet at the top of your list! (But don't forget that some sites are unreliable and others mean you harm.) Immediately after you restart the system, the Vista Problem Reports and Solutions window might appear with useful information. Event Viewer might also provide events it has logged.

A system lockup means that the computer freezes and must be restarted. These errors are most likely caused by hardware such as memory, the motherboard, CPU, video card, or the system overheating. I/O devices such as the keyboard, mouse, or monitor or application errors don't usually cause a system to lock up. When a system freezes and you must restart it, check Event Viewer to see if it has reported a hardware failure. Other tools that can help are the Reliability and Performance Monitor, Vista Problem Reports and Solutions window, and Vista Memory Diagnostics. When I/O devices give errors, be sure to check Device Manager for warnings and Event Viewer for information it has tracked.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to know the difference between a blue screen error and a system lockup error.

When solving problems with any kind of hardware, it's important that you check for physical damage to the device. If you feel excessive heat coming from the computer case or a peripheral device, immediately unplug the device or power down the system. Don't turn the device or system back on until the problem is solved; you don't want to start a fire! Other symptoms that indicate potential danger are strong electrical odors, unusual noises, liquid spills on a device, and visible damage such as a frayed cable, melted plastic, or smoke. In these situations, turn off the equipment immediately.

As you learn to solve computer problems, see each new problem as the potential to learn something new. Don't forget to search the Internet for information on each problem you face when you don't immediately know the solution. Installation manuals and training materials can also be good sources of information.

VISTA TOOLS FOR SOLVING STARTUP PROBLEMS

A+
220-701
2.2
3.4

Tools that can be used to troubleshoot and solve startup problems with Windows Vista are the Advanced Boot Options menu, the Vista Recovery Environment, and the command prompt window in Windows RE. The Advanced Boot Options menu is also available in Windows 2000/XP, although when using these OSs it is called the **Advanced Options menu**. As you learn to use each tool, keep in mind that you want to use the tool that makes as few changes to the system as possible to fix the problem.

Before we discuss the Windows tools, let's turn our attention to learning about the files that Vista needs to start successfully and the step-by-step process of loading the OS. The better you understand this process, the more likely you will be able to solve a problem when Vista cannot start.

Caution This chapter often refers to the Windows setup CD or DVD. If you have a notebook computer or a brand-name computer such as a Dell, IBM, Lenovo, or Gateway, be sure to use the manufacturer's recovery CDs or DVD instead of a regular Windows setup disc. This recovery disc has drivers specific to your system, and the Windows build might be different from that of an off-the-shelf Windows setup disc. For example, Windows Vista Home Premium installed on a notebook computer might have been built with all kinds of changes made to it by the notebook manufacturer and is, therefore, different from the Windows Vista Home Premium that you can buy in a retail store.

A+
220-701
2.2
3.4

FILES NEEDED TO START WINDOWS VISTA

A Windows Vista system has successfully started when you can log onto Windows and the Windows desktop is loaded. To successfully start, a computer needs the bare-bones minimum of hardware and software. If one of these hardware or software components is missing, corrupted, or broken, the boot fails. To start, a computer needs a CPU, motherboard, memory, power supply, and boot device (hard drive, optical disc, or other boot device).

Table 15-2 lists the files necessary to start Windows Vista. The MBR sector and the OS boot sector are included in the table to complete the list of software components needed to load Vista when Vista loads from the hard drive. Vista startup is managed by two files: the **Windows Boot Manager (BootMgr)** and the **Windows Boot Loader (WinLoad.exe)**. Vista configuration data is stored in the Vista **Boot Configuration Data (BCD) file**. Also notice in Table 15-2 that the BootMgr file and the BCD file are stored in the system partition (the active partition) and the other files are stored in the boot partition. For most installations, the system partition and the boot partition are the same (drive C).

Component or File	Path*	Description
MBR	First sector of the hard drive called the master boot record	Contains the partition table and the master boot program used to locate and start the BootMgr program.
OS boot record	First sector of the system partition (most likely drive C)	Windows XP uses this sector, but Vista does not use it.
BootMgr	Root directory of system partition (C:\)	Windows Boot Manager manages the initial startup of the OS.
BCD	Boot folder of the system partition (C:\Boot)	Boot Configuration Data file contains boot parameters.
WinLoad.exe	C:\Windows\System32	Windows Boot Loader loads and starts essential Windows processes.
Ntoskrnl.exe	C:\Windows\System32	Vista kernel.
Hal.dll	C:\Windows\System32	Dynamic link library handles low-level hardware details.
Smss.exe	C:\Windows\System32	Sessions Manager file responsible for loading user mode graphics components.
Csrss.exe	C:\Windows\System32	Win32 subsystem.
Winlogon.exe	C:\Windows\System32	Logon process.
Services.exe	C:\Windows\System32	Service Control Manager starts and stops services.
Lsass.exe	C:\Windows\System32	Authenticates users.
System registry hive	C:\Windows\System32\Config\System	Holds data for the HKEY_LOCAL_MACHINE key of the registry.
Device drivers	C:\Windows\System32\Drivers	Drivers for required hardware.

*It is assumed that Windows is installed in C:\Windows.

Table 15-2 Software components and files needed to start Windows Vista

A+
220-701
2.2
3.4

Don't be confused with the terminology here. It is really true that, according to the terms used by Microsoft documention, the Windows OS is on the boot partition, and the boot record is on the system partition, although that might seem backward. The PC boots from the system partition and loads the Windows Vista operating system from the boot partition. The system partition contains the files that tell a computer where to look to start Windows. The boot partition contains the \Windows folder where system files are located. Most of the time the boot partition and the system partition are the same partition (drive C). The only time they are different is in a dual-boot configuration. For example, if Vista has been installed in a dual-boot configuration with Windows XP, the system partition is most likely drive C (where Windows XP is installed), and Vista is installed on another drive, such as drive E, which Vista calls the boot partition. The PC boots from drive C and then loads Vista system files stored on drive E in the E:\Windows folder.

The Vista **Boot Configuration Data (BCD) file** is structured the same as a registry file and contains configuration information about how Vista is started. Here is the type of information contained in the BCD file:

- Settings that control BootMgr and WinLoad.exe
- Settings that control WinResume.exe, the program that resumes Vista from hibernation
- Settings that start and control the Windows Memory Diagnostic program (\Boot\MemTest.exe)
- Settings that launch Ntldr to load a previous OS in a dual-boot configuration
- Settings to load a non-Microsoft operating system (such as the Mac OS or Linux)

STEPS TO START A VISTA COMPUTER

Now let's look at the steps to start a Windows Vista computer. Several of these steps are diagrammed in Figures 15-21 and 15-22 to help you visually understand how the steps work.

A+ Exam Tip The A+ 220-701 Essentials exam expects you to recognize symptoms of problems when Windows starts. Understanding the startup process can help you recognize at what point in startup a problem occurs.

Study these steps carefully, because the better you understand startup, the more likely you'll be able to solve startup problems.

1. Startup BIOS first checks all the essential hardware components to make sure they're working and displays its progress on-screen. (The computer is sometimes configured to show a manufacturer's logo or welcome screen instead.) If it has a problem and the video system is working, it displays an error message. If video is not working, BIOS might attempt to communicate an error with a series of beeps (called beep codes) or speech (for speech-enabled BIOS). The process of BIOS checking hardware is called POST (Power-On Self Test).
2. After POST, the BIOS turns to CMOS RAM to find out to which device it should look to find an operating system. One of the settings stored in CMOS is the boot sequence, which is a list of devices such as a DVD drive, floppy drive, USB device,

A+
220-701
2.2
3.4

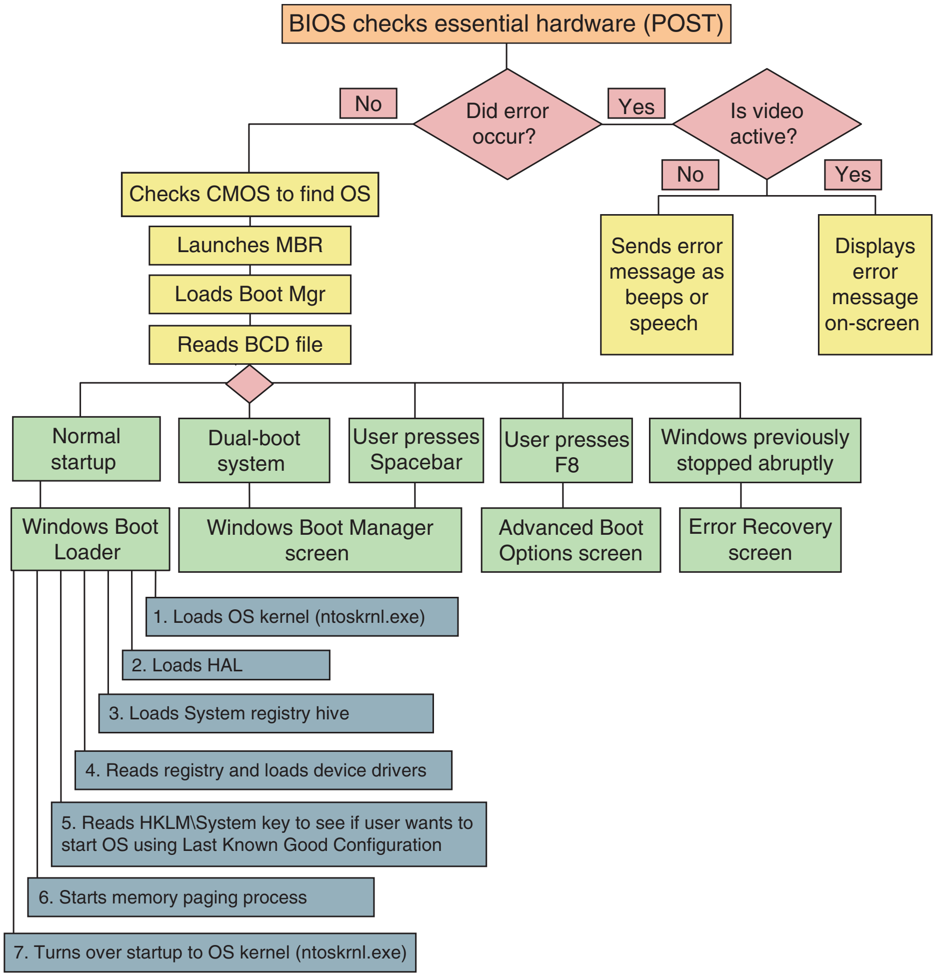

BIOS checks essential hardware (POST)
Did error occur?
No
Yes
Is video active?
No
Yes
Checks CMOS to find OS
Launches MBR
Loads Boot Mgr
Reads BCD file
Sends error message as beeps or speech
Displays error message on-screen
Normal startup
Dual-boot system
User presses Spacebar
User presses F8
Windows previously stopped abruptly
Windows Boot Loader
Windows Boot Manager screen
Advanced Boot Options screen
Error Recovery screen
1. Loads OS kernel (ntoskrnl.exe)
2. Loads HAL
3. Loads System registry hive
4. Reads registry and loads device drivers
5. Reads HKLM\System key to see if user wants to start OS using Last Known Good Configuration
6. Starts memory paging process
7. Turns over startup to OS kernel (ntoskrnl.exe)

Figure 15-21 Steps to booting the computer and loading Vista
Courtesy: Course Technology/Cengage Learning

or hard drive, arranged in the order they should be searched for a bootable OS. The BIOS looks to the first item in the list for storage media that contains an OS to load. If it doesn't find a bootable OS, it moves to the next item in the list. You can change the boot sequence in BIOS setup. Usually the OS is loaded from the hard drive.

3. The BIOS finds and launches the small program in the master boot record (MBR) of the hard drive. This program points to the BootMgr program stored in the root of the system partition. BootMgr is launched.
4. BootMgr starts in 16-bit mode and switches the processor to 32-bit or 64-bit mode. (Starting in 16-bit mode is necessary because all processors start in 16-bit mode, also called real mode.)
5. BootMgr reads the BCD file. The next step, one of five, depends on these factors:

   Option 1: For normal startups that are not dual booting, no menu appears and BootMgr finds and launches Windows Boot Loader (WinLoad.exe).
   Option 2: If the computer is set up for a dual-boot environment, BootMgr displays the Windows Boot Manager screen, as shown in Figure 15-23.

A+
220-701
2.2
3.4

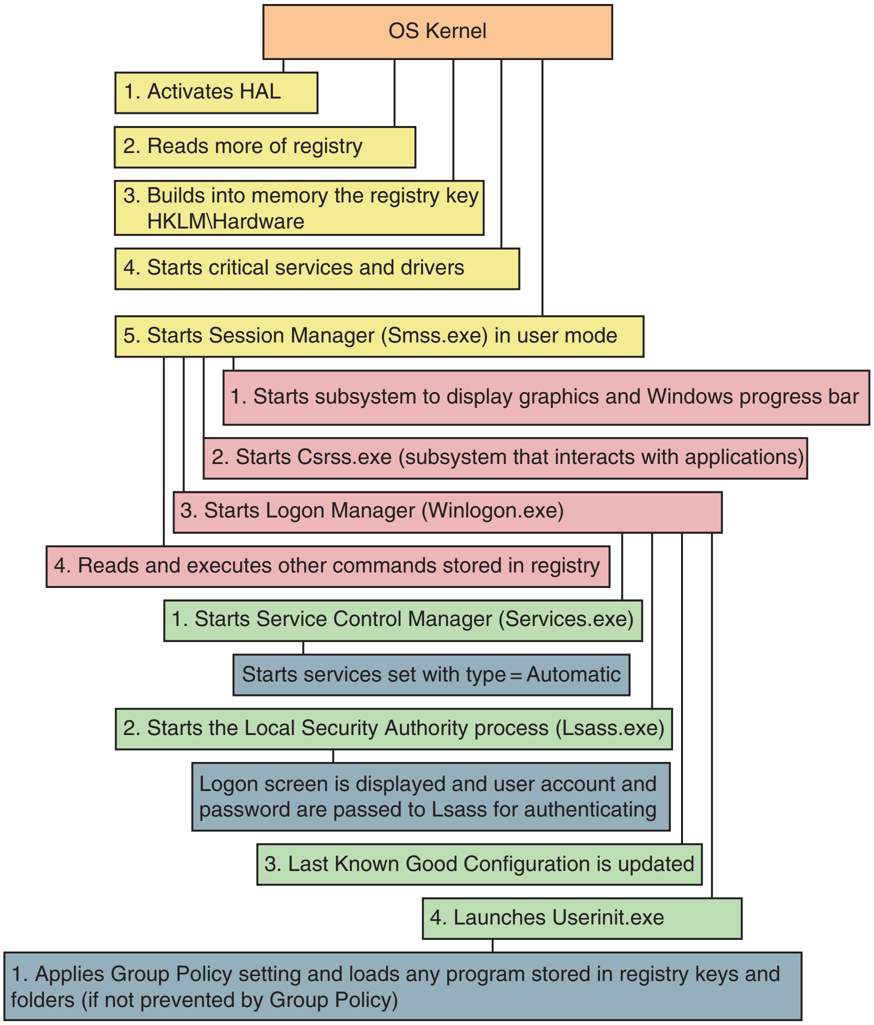
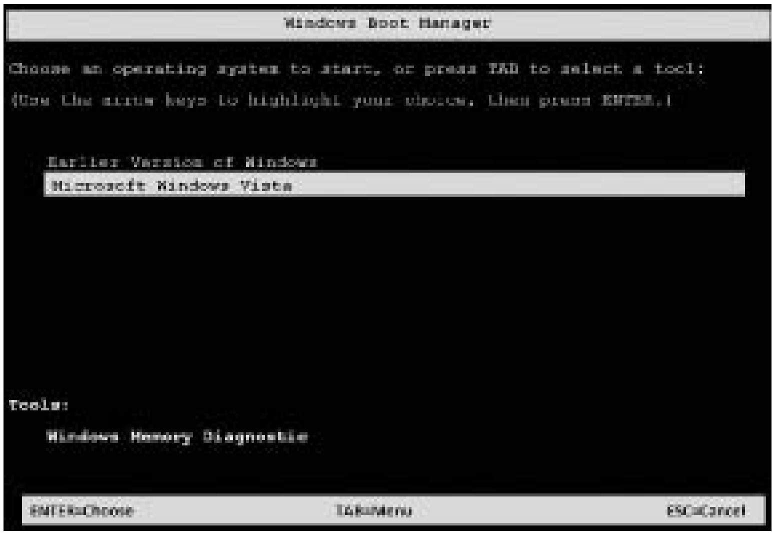

OS Kernel
1. Activates HAL
2. Reads more of registry
3. Builds into memory the registry key HKLM\Hardware
4. Starts critical services and drivers
5. Starts Session Manager (Smss.exe) in user mode
1. Starts subsystem to display graphics and Windows progress bar
2. Starts Csrss.exe (subsystem that interacts with applications)
3. Starts Logon Manager (Winlogon.exe)
4. Reads and executes other commands stored in registry
1. Starts Service Control Manager (Services.exe)
Starts services set with type = Automatic
2. Starts the Local Security Authority process (Lsass.exe)
Logon screen is displayed and user account and password are passed to Lsass for authenticating
3. Last Known Good Configuration is updated
4. Launches Userinit.exe
1. Applies Group Policy setting and loads any program stored in registry keys and folders (if not prevented by Group Policy)

Figure 15-22 Steps to complete loading Vista
Courtesy: Course Technology/Cengage Learning



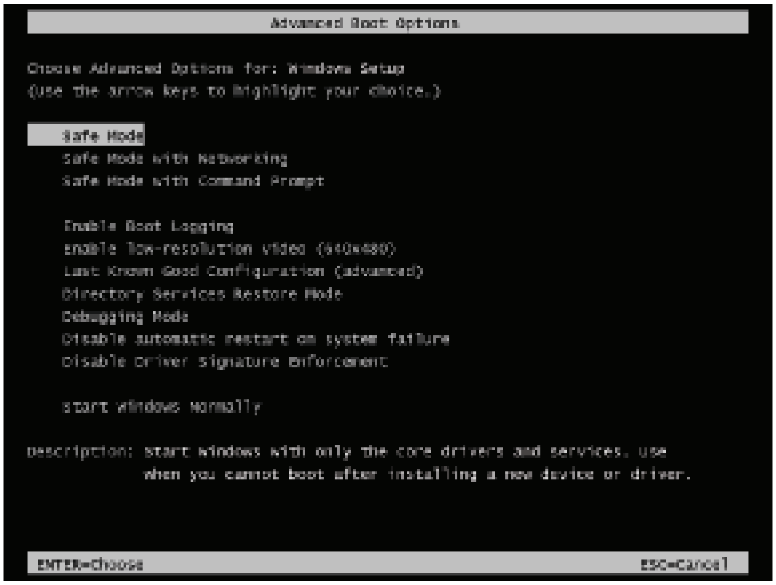
```
                         Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

   Earlier Version of Windows
   Microsoft Windows Vista

Tools:
   Windows Memory Diagnostic

 ENTER=Choose                   TAB=Menu                    ESC=Cancel
```

Figure 15-23 Windows Boot Manager screen appears in a dual-boot environment
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2
3.4

Option 3: If the user presses the Spacebar, the Windows Boot Manager screen appears.

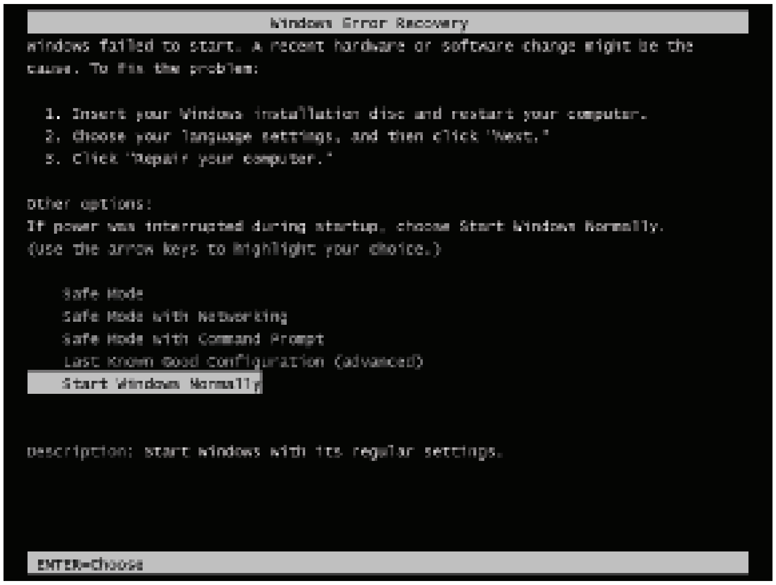
Option 4: If the user presses F8, BootMgr displays the Advanced Boot Options screen, as shown in Figure 15-24.



```
                         Advanced Boot Options

Choose Advanced Options for: Windows Setup
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Start Windows with only the core drivers and services. Use
             when you cannot boot after installing a new device or driver.


ENTER=Choose                                                   ESC=Cancel
```

Figure 15-24 Press F8 to see the Advanced Boot Options menu
Courtesy: Course Technology/Cengage Learning

Option 5: If Windows was previously stopped abruptly, the Windows Error Recovery screen (see Figure 15-25) appears.



```
                         Windows Error Recovery
Windows failed to start. A recent hardware or software change might be the
cause. To fix the problem:

  1. Insert your Windows installation disc and restart your computer.
  2. Choose your language settings, and then click "Next."
  3. Click "Repair your computer."

Other options:
If power was interrupted during startup, choose Start Windows Normally.
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt
    Last Known Good Configuration (advanced)
    Start Windows Normally


Description: Start Windows with its regular settings.




ENTER=Choose
```

Figure 15-25 This window appears if Windows has been abruptly stopped
Courtesy: Course Technology/Cengage Learning

6. For normal startups, WinLoad loads into memory the OS kernel and Ntoskrnl.exe, but does not yet start them. WinLoad also loads into memory the Hardware Abstraction Layer (Hal.dll), which will later be used by the kernel.
7. WinLoad loads into memory the system registry hive (C:\Windows\System32\Config\System).

A+
220-701
2.2
3.4

8. WinLoad then reads the registry key just created, HKEY_LOCAL_ MACHINE\SYSTEM\Services, looking for and loading into memory device drivers that must be launched at startup. The drivers are not yet started.

9. WinLoad reads data from the HKEY_LOCAL_MACHINE\SYSTEM key that tells the OS if the user wants to start the OS using the Last Known Good Configuration.

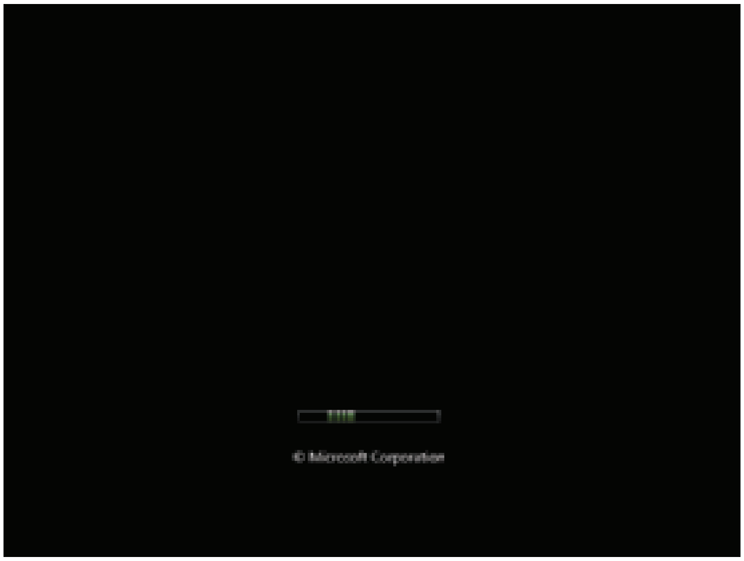
10. WinLoad starts up the memory paging process and then turns over startup to the OS kernel.

11. The kernel (Ntoskrnl.exe) activates the HAL, reads more information from the registry, and builds into memory the registry key HKEY_LOCAL_ MACHINE\HARDWARE, using information that has been collected about the hardware.

12. The kernel then starts critical services and drivers that are configured to be started by the kernel during the boot. Recall that drivers interact directly with hardware and run in kernel mode, while services interact with drivers. Most services and drivers are stored in C:\Windows\System32 or C:\Windows\System32\Drivers and have an .exe, .dll, or .sys file extension.

13. After all services and drivers configured to load during the boot are started, the kernel starts the Session Manager (Smss.exe), which runs in user mode.

14. Smss.exe starts the part of the Win32 subsystem that displays graphics and the Windows **progress bar** is displayed on the screen (see Figure 15-26). When you see the progress bar, you know the Windows kernel has loaded successfully.



© Microsoft Corporation

Figure 15-26 The progress bar indicates that the Windows graphics subsystem is running and the kernel has successfully loaded
Courtesy: Course Technology/Cengage Learning

15. Smss.exe then starts the client/server run-time subsystem (Csrss.exe), which also runs in user mode. Csrss.exe is the Win32 subsystem component that interacts with applications.

16. Smss.exe starts the Logon Manager (Winlogon.exe) and reads and executes other commands stored in the registry, such as a command to replace system files placed there by Windows Update.

A+
220-701
2.2
3.4

17. Winlogon.exe starts the Service Control Manager (Services.exe). Services.exe starts all services listed with the startup type of Automatic in the Services console.

18. Winlogon.exe starts the Local Security Authority process (Lsass.exe). The logon screen appears (see Figure 15-27), and the user account and password are passed to the Lsass.exe process for authenticating. The Last Known Good Configuration information in the registry is updated.

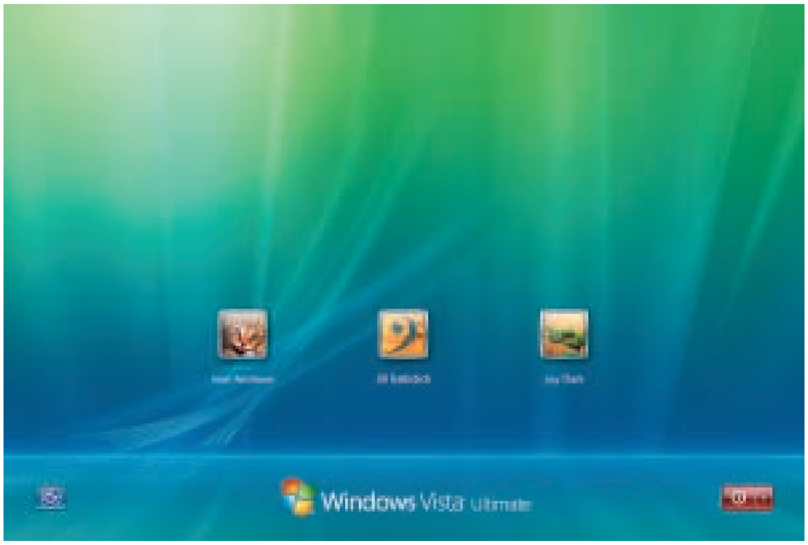


Figure 15-27 Windows Vista logon screen
Courtesy: Course Technology/Cengage Learning

19. Winlogon.exe launches Userinit.exe and the Windows desktop (Explorer.exe).

20. Userinit.exe applies Group Policy settings and any programs not trumped by Group Policy that are stored in these registry keys and folders:
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
    - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - *Systemdrive*\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    - *Systemdrive*\Users*username*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

The Windows startup is officially completed when the Windows desktop appears and the wait circle disappears.

With this basic knowledge of the boot in hand, let's turn our attention to the Windows tools that can help you solve problems when Vista refuses to load.

ADVANCED BOOT OPTIONS MENU

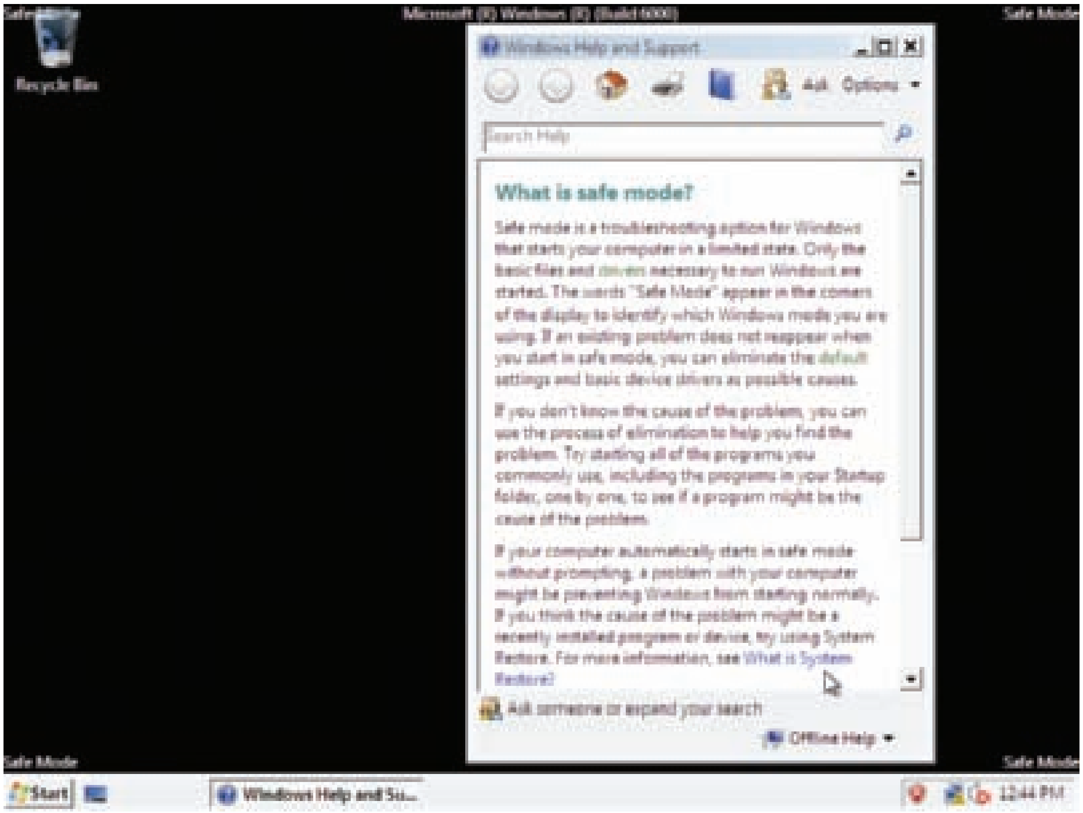
The Vista Advanced Boot Options menu (refer back to Figure 15-24) appears when a user presses F8 as Vista is loading. You need to be familiar with each option on this menu and know how to use it.

A+
220-701
2.2
3.4

SAFE MODE ON THE ADVANCED BOOT OPTIONS MENU

Safe Mode boots the OS with a minimum configuration and can be used to solve problems with a new hardware installation or problems caused by user settings. Safe Mode boots with the mouse, monitor (with basic video), keyboard, and mass storage drivers loaded. It uses the default system services (it does not load any extra services) and does not provide network access. It uses a plain video driver (Vga.sys) instead of the video drivers specific to your video card.

When you boot in Safe Mode, you will see "Safe Mode" in all four corners of your screen. In addition, you have a GUI interface in Safe Mode. The screen resolution is 600 x 800 and the desktop wallpaper (background) is black. Figure 15-28 shows Vista in Safe Mode.



What is safe mode?

Safe mode is a troubleshooting option for Windows that starts your computer in a limited state. Only the basic files and drivers necessary to run Windows are started. The words "Safe Mode" appear in the corners of the display to identify which Windows mode you are using. If an existing problem does not reappear when you start in safe mode, you can eliminate the default settings and basic device drivers as possible causes.

If you don't know the cause of the problem, you can use the process of elimination to help you find the problem. Try starting all of the programs you commonly use, including the programs in your Startup folder, one by one, to see if a program might be the cause of the problem.

If your computer automatically starts in safe mode without prompting, a problem with your computer might be preventing Windows from starting normally. If you think the cause of the problem might be a recently installed program or device, try using System Restore. For more information, see What is System Restore?

Figure 15-28 Safe Mode loads a minimum Vista configuration
Courtesy: Course Technology/Cengage Learning

Here's a list of things you can do in Safe Mode to recover the system:

1. When Safe Mode first loads, if Windows senses the problem is drastic, it gives you the opportunity to go directly to System Restore. Use System Restore unless you know exactly what it is you need to do to solve your problem.
2. If you suspect a virus, scan the system for viruses. You can also use Chkdsk to fix hard drive problems. Your hard drive might be full; if so, make some free space available.
3. Use Device Manager to uninstall or disable a device with problems or to roll back a driver.

A+
220-701
2.2
3.4

4. Use Msconfig to disable unneeded services or startup processes. Recall from Chapter 14 that you can use Msconfig to disable many services and startup processes, and then enable them one group at a time until you discover the one causing the problem.
5. If you suspect a software program you have just installed, use the Programs and Features window to uninstall it.
6. You can also use System Restore from within Safe Mode to restore the system to a previous restore point.
7. If you don't know the source of a problem that prevents a normal startup, but you can launch Safe Mode, you can investigate the problem while in Safe Mode. Use Event Viewer and other detective tools to find information saved during previously failed startups that can help you identify the source of a problem.

Here are some tips about loading Safe Mode that you need to be aware of:

- From the Advanced Boot Options menu, first try Safe Mode with Networking. If that doesn't work, try Safe Mode. And if that doesn't work, try Safe Mode with Command Prompt.
- Know that Safe Mode won't load if core Windows components are corrupted.
- When you load Windows in Safe Mode, all files used for the load are recorded in the Ntbtlog.txt file. Use this file to identify a service, device driver, or application loaded at startup that is causing a problem.

SAFE MODE WITH NETWORKING

Use this option when you are solving a problem with booting and need access to the network to solve the problem. For example, you might need to download updates to your antivirus software. Another example is when you have just attempted to install a printer, which causes the OS to hang when it boots. You can boot into Safe Mode with Networking and download new printer drivers from the network. Uninstall the printer and then install it again from the network. Also use this mode when the Windows installation files are available on the network, rather than the Windows setup CD or DVD, and you need to access those files.

SAFE MODE WITH COMMAND PROMPT

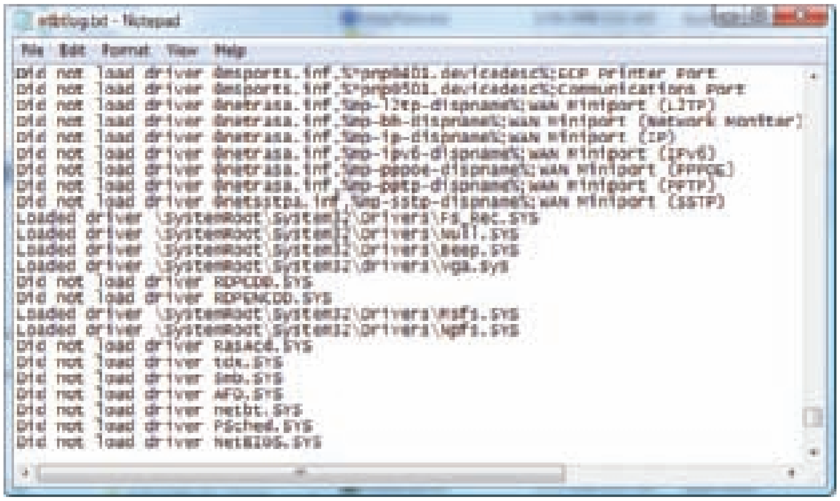
If the first Safe Mode option does not load the OS, then try Safe Mode with command prompt. This Safe Mode option does not load a GUI desktop automatically. You would use it to get a command prompt only. At the command prompt, use the SFC command to verify system files. Also use the Chkdsk command to check for file system errors. If the problem is still not solved, you can use this command to launch System Restore: **C:\Windows\system32\ restore\rstrui.exe**. Then follow the directions on-screen to select a restore point.

ENABLE BOOT LOGGING

When you boot with this option, Windows loads normally and you access the regular desktop. However, all files used during the load process are recorded in a file, C:\Windows\Ntbtlog.txt (see Figure 15-29). Thus, you can use this option to see what did and did not load during the boot. For instance, if you have a problem getting a device to work, check Ntbtlog.txt to see what driver files loaded. Boot logging is much more effective if you have a copy of Ntbtlog.txt that was made when everything worked as it should. Then you can compare the good load to the bad load, looking for differences.

Notes The Ntbtlog.txt file is also generated when you boot into Safe Mode.

A+
220-701
2.2
3.4



```
Did not load driver @msports.inf,%*pnp0401.devicedesc%;ECP Printer Port
Did not load driver @msports.inf,%*pnp0501.devicedesc%;Communications Port
Did not load driver @netrasa.inf,%mp-l2tp-dispname%;WAN Miniport (L2TP)
Did not load driver @netrasa.inf,%mp-bh-dispname%;WAN Miniport (Network Monitor)
Did not load driver @netrasa.inf,%mp-ip-dispname%;WAN Miniport (IP)
Did not load driver @netrasa.inf,%mp-ipv6-dispname%;WAN Miniport (IPv6)
Did not load driver @netrasa.inf,%mp-pppoe-dispname%;WAN Miniport (PPPOE)
Did not load driver @netrasa.inf,%mp-pptp-dispname%;WAN Miniport (PPTP)
Did not load driver @netsstpa.inf,%mp-sstp-dispname%;WAN Miniport (SSTP)
Loaded driver \SystemRoot\System32\Drivers\Fs_Rec.SYS
Loaded driver \SystemRoot\System32\Drivers\Null.SYS
Loaded driver \SystemRoot\System32\Drivers\Beep.SYS
Loaded driver \SystemRoot\System32\drivers\vga.sys
Did not load driver RDPCDD.SYS
Did not load driver RDPENCDD.SYS
Loaded driver \SystemRoot\System32\Drivers\Msfs.SYS
Loaded driver \SystemRoot\System32\Drivers\Npfs.SYS
Did not load driver RasAcd.SYS
Did not load driver tdx.SYS
Did not load driver Smb.SYS
Did not load driver AFD.SYS
Did not load driver netbt.SYS
Did not load driver PSched.SYS
Did not load driver NetBIOS.SYS
```

Figure 15-29 Sample Ntbtlog.txt file
Courtesy: Course Technology/Cengage Learning

> **Notes** If Windows hangs during the boot, try booting using the option Enable Boot Logging. Then look at the last entry in the Ntbtlog.txt file. This entry might be the name of a device driver causing the system to hang.

ENABLE LOW-RESOLUTION VIDEO (640X480)

In Windows XP, this option is called "Enable VGA Mode." Use this option when the video setting does not allow you to see the screen well enough to fix a bad setting. This can happen when a user creates a desktop with black fonts on a black background, or something similar that makes it impossible to see the desktop. Booting in this mode gives you a very plain, standard VGA video. You can then go to the Display settings, correct the problem, and reboot normally. You can also use this option if your video drivers are corrupted and you need to update, roll back, or reinstall your video drivers.

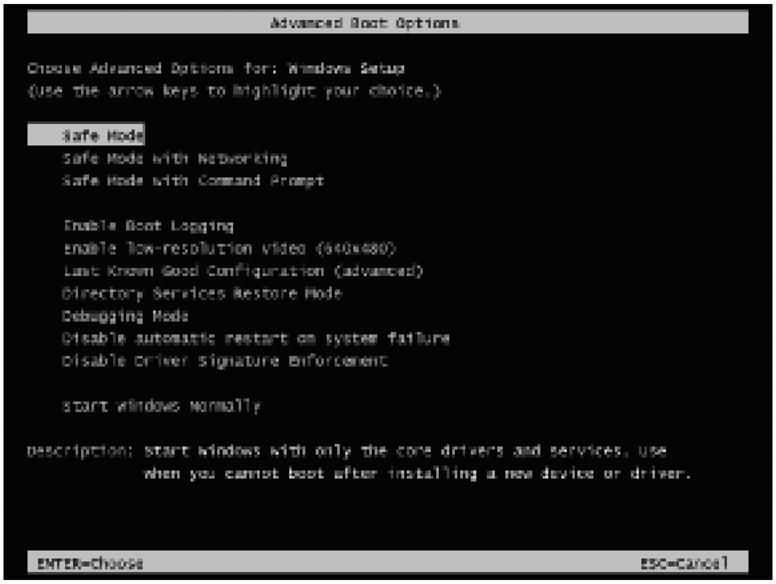
LAST KNOWN GOOD CONFIGURATION

Registry settings collectively called the **Last Known Good Configuration** are saved in the registry each time the user successfully logs onto the system. If your problem is caused by a bad hardware or software installation and you get an error message the first time you restart the system after the installation, using the Last Known Good can, in effect, undo your installation and solve your problem. Do the following:

1. While startup BIOS is finishing up and just before Windows begins to load, press **F8**. The Advanced Boot Options menu appears (see Figure 15-30 for the Vista menu, but the XP menu is similar). If the problem is so severe that this menu does not appear, then the next step is to boot from the Windows setup CD or DVD.
2. Select **Last Known Good Configuration (advanced)** and press **Enter**. The system will reboot.

Remember, the Last Known Good registry settings are saved each time a user logs on to Windows. Therefore, it's important to try the Last Known Good early in the troubleshooting

A+
220-701
2.2
3.4



```
                          Advanced Boot Options

Choose Advanced Options for: Windows Setup
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Start Windows with only the core drivers and services. Use
             when you cannot boot after installing a new device or driver.


 ENTER=Choose                                                  ESC=Cancel
```

Figure 15-30 Press F8 to see the Advanced Boot Options menu
Courtesy: Course Technology/Cengage Learning

session before it's overwritten. (However, know that if you log onto the system in Safe Mode, the Last Known Good is not saved.) For Windows Vista, if the Last Known Good Configuration doesn't work, your next option is the Startup Repair process in the Windows Recovery Environment.

DIRECTORY SERVICES RESTORE MODE (WINDOWS DOMAIN CONTROLLERS ONLY)

This option applies only to domain controllers and is used as one step in the process of recovering from a corrupted Active Directory. Recall that Active Directory is the domain database managed by a domain controller that tracks users and resources on the domain.

DEBUGGING MODE

This mode gives you the opportunity to move system boot logs from the failing computer to another computer for evaluation. To use this mode, both computers must be connected to each other by way of the serial port. Then, you can reboot into this mode and Windows on the failing computer will send all the boot information through the serial port and on to the other computer. For more details, see the *Windows Vista Resource Kit*, the *Windows XP Professional Resource Kit,* or the *Windows 2000 Professional Resource Kit* (Microsoft Press).

DISABLE AUTOMATIC RESTART ON SYSTEM FAILURE

By default, Windows automatically restarts immediately after it encounters a system failure, which is also called a stop error or a blue screen error. This type of error can be especially troublesome if you're trying to shut down a system and it encounters an error. The error can cause the system to continually reboot rather than shut down. For Windows Vista or XP, choose **Disable automatic restart on system failure** to stop the rebooting. (The option is not on the Windows 2000 Advanced Options menu.)

A+
220-701
2.2
3.4

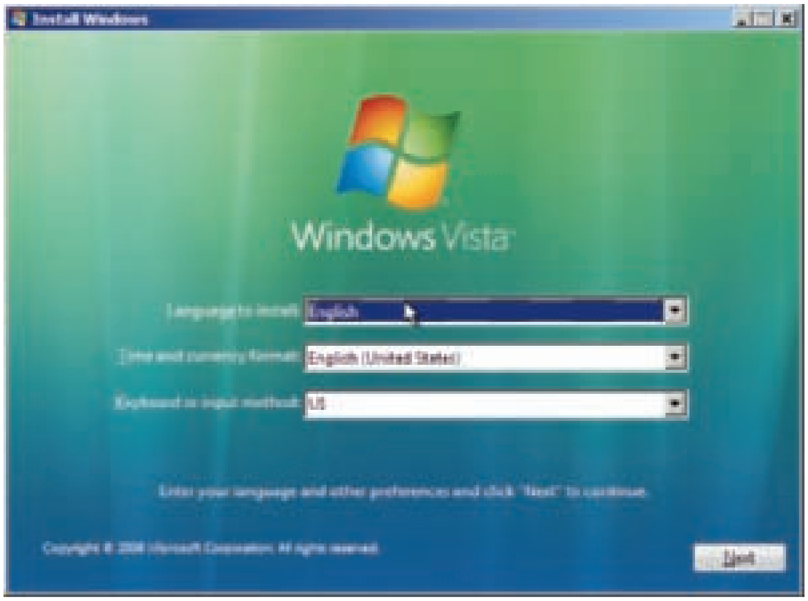
From the Windows desktop, you can modify this same setting using the System Properties window. Click the **Advanced** tab. For Windows Vista and XP, under Startup and Recovery, click **Settings**, and, for Windows 2000, click **Startup and Recovery**. On the Startup and Recovery window, uncheck **Automatically restart**, as shown earlier in Figure 15-17. The next time the system encounters a stop error, it will shut down and not automatically restart.

THE WINDOWS RECOVERY ENVIRONMENT (WINDOWS RE)

The Windows Vista Recovery Environment (RecEnv.exe), also known as Windows RE, is an operating system launched from the Vista DVD that provides a graphical and command-line interface. Our goal in this section is to help you become familiar with Windows RE, and, in Chapter 16, you'll learn to use it to solve startup problems.

Follow these steps to start up and explore Windows RE:

1. Using a computer that has Windows Vista installed, boot from the Vista setup DVD. (To boot from a DVD, you might have to change the boot sequence in BIOS setup to put the optical drive first above the hard drive.) Select your language preference, as shown in Figure 15-31, and click **Next**.



Language to install: English

Time and currency format: English (United States)

Keyboard or input method: US

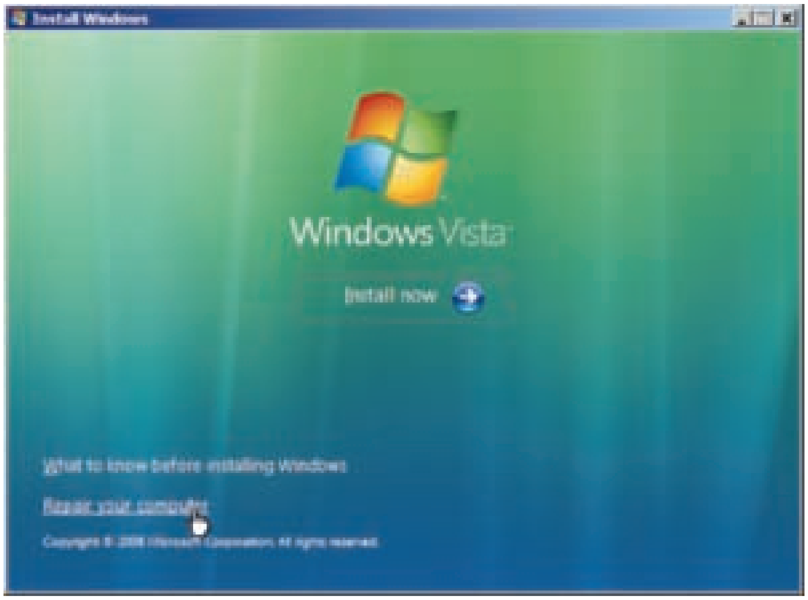
Enter your language and other preferences and click "Next" to continue.

Copyright © 2006 Microsoft Corporation. All rights reserved.

Figure 15-31 Select your language preference
Courtesy: Course Technology/Cengage Learning

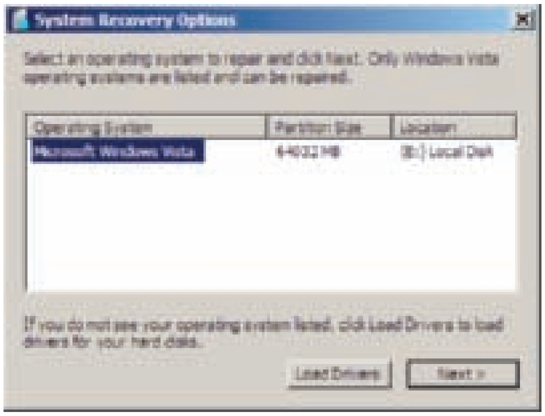
2. The Install Windows screen appears, as shown in Figure 15-32. Click **Repair your computer**. The recovery environment (RecEnv.exe) launches and displays the System Recovery Options dialog box (see Figure 15-33).
3. Select the Vista installation to repair and click **Next**.
4. The System Recovery Options window in Figure 15-34 appears, listing recovery options.
5. The first tool, Startup Repair, can automatically fix many Windows problems, including those caused by corrupted or missing system files. You can't cause any additional problems by using it and it's easy to use. Therefore, it should be your first recovery

A+
220-701
2.2
3.4



Copyright © 2006 Microsoft Corporation. All rights reserved.

Figure 15-32 Launch Windows RE after booting from the Vista DVD
Courtesy: Course Technology/Cengage Learning

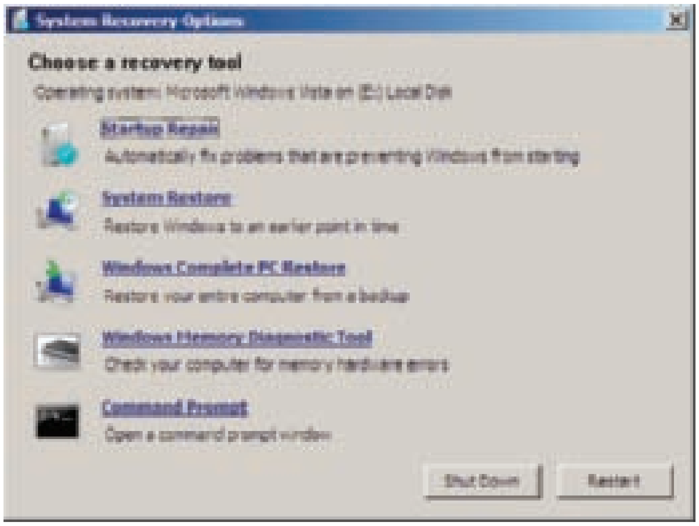


Select an operating system to repair and click Next. Only Windows Vista operating systems are listed and can be repaired.

Operating System	Partition Size	Location
Microsoft Windows Vista	64032 MB	(E:) Local Disk

If you do not see your operating system listed, click Load Drivers to load drivers for your hard disks.

Figure 15-33 Select a Vista installation to repair
Courtesy: Course Technology/Cengage Learning



Choose a recovery tool

Operating system: Microsoft Windows Vista on (E:) Local Disk

Startup Repair
Automatically fix problems that are preventing Windows from starting

System Restore
Restore Windows to an earlier point in time

Windows Complete PC Restore
Restore your entire computer from a backup

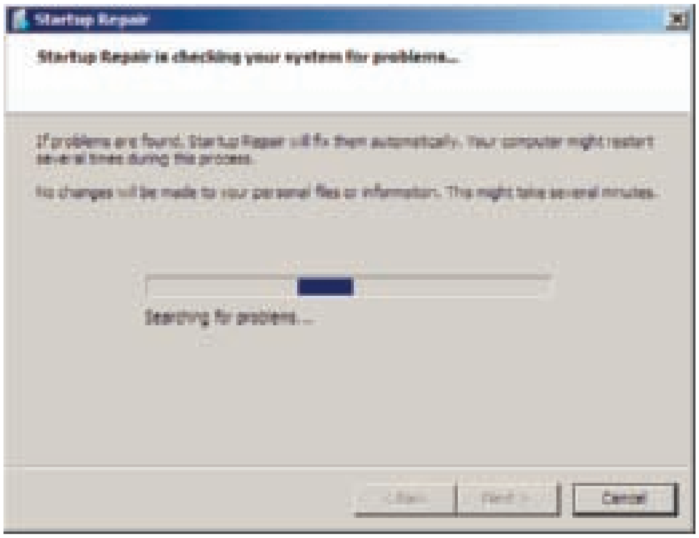
Windows Memory Diagnostic Tool
Check your computer for memory hardware errors

Command Prompt
Open a command prompt window

Figure 15-34 Recovery tools in Windows RE
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2
3.4

option when Vista refuses to load. Click **Startup Repair** and the tool will examine the system for errors (see Figure 15-35).



Startup Repair

Startup Repair is checking your system for problems...

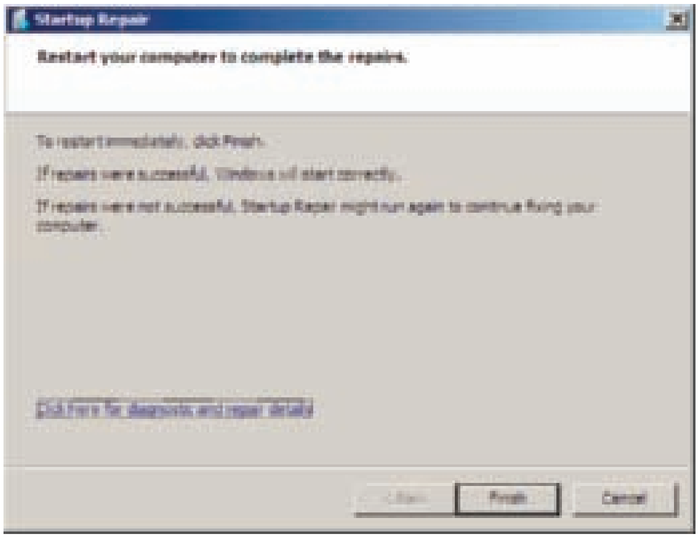
If problems are found, Startup Repair will fix them automatically. Your computer might restart several times during this process.

No changes will be made to your personal files or information. This might take several minutes.

Searching for problems...

Figure 15-35 Startup Repair searches the system for problems it can fix
Courtesy: Course Technology/Cengage Learning

6. Based on what it finds, it will suggest various solutions. For example, it might suggest you use System Restore or suggest you immediately reboot the system to see if the problem has been fixed. For the system in Figure 15-36, a reboot is suggested.



Startup Repair

Restart your computer to complete the repairs.

To restart immediately, click Finish.

If repairs were successful, Windows will start correctly.

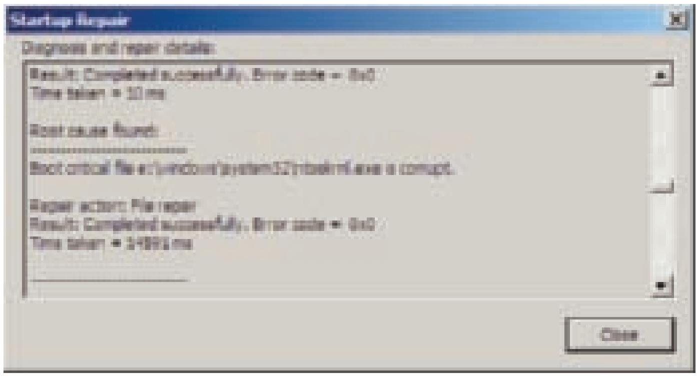
If repairs were not successful, Startup Repair might run again to continue fixing your computer.

Click here for diagnostic and repair details

Figure 15-36 Startup Repair has attempted to fix the problem
Courtesy: Course Technology/Cengage Learning

7. To see a list of items examined and actions taken by Startup Repair, click **Click here for diagnostic and repair details**. The dialog box showing the list of repairs appears, as shown in Figure 15-37. A log file can also be found at C:\Windows\System32\LogFiles\SRT\SRTTrail.txt.

A+
220-701
2.2
3.4

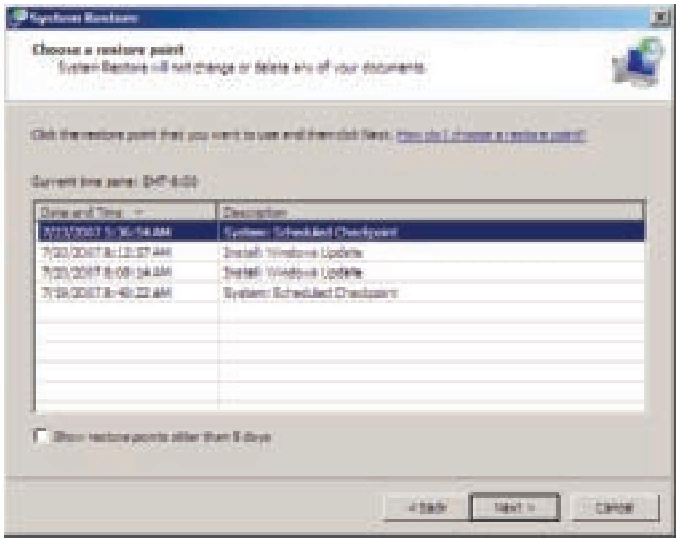


Diagnosis and repair details:

```
Result: Completed successfully. Error code = 0x0
Time taken = 10 ms

Root cause found:
---------------------------
Boot critical file e:\windows\system32\ntoskrnl.exe is corrupt.

Repair action: File repair
Result: Completed successfully. Error code = 0x0
Time taken = 14891 ms

---------------------------
```

Figure 15-37 Details of actions taken by Startup Repair
Courtesy: Course Technology/Cengage Learning

8. System Restore in the System Recovery Options window works the same as Windows System Restore from the desktop to return the system to its state when a restore point was made. Click **System Restore** and then click **Next**; a list of restore points appears (see Figure 15-38). Select the most recent restore point to make the least intrusive changes to the system.



Choose a restore point
System Restore will not change or delete any of your documents.

Click the restore point that you want to use and then click Next. How do I choose a restore point?

Current time zone: GMT-8:00

Date and Time	Description
7/23/2007 5:36:54 AM	System: Scheduled Checkpoint
7/20/2007 8:12:37 AM	Install: Windows Update
7/20/2007 8:08:14 AM	Install: Windows Update
7/19/2007 8:40:22 AM	System: Scheduled Checkpoint

□ Show restore points older than 5 days

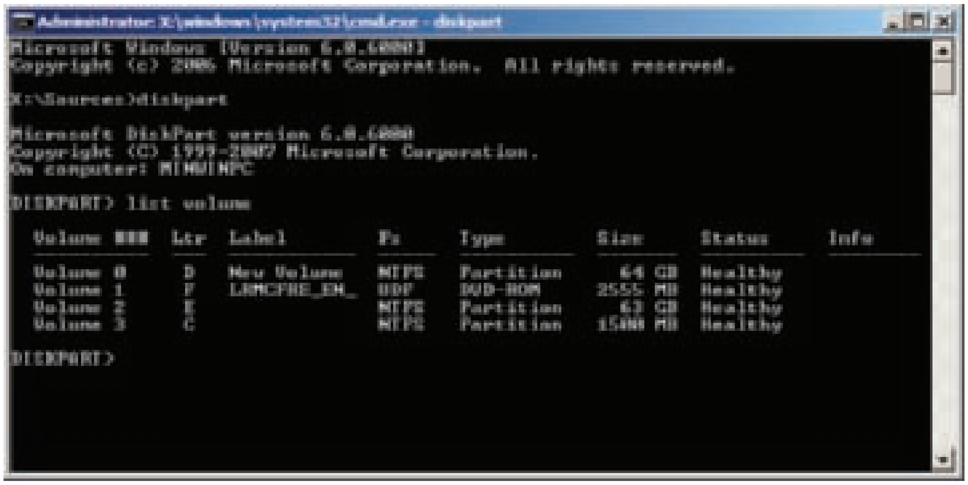
Figure 15-38 Select the most recent restore point to make fewer changes to the system
Courtesy: Course Technology/Cengage Learning

9. Windows Complete PC Restore can be used to completely restore drive C and possibly other drives to their state when the last backups of the drives were made. The backups are made using Complete PC Backup, which you learned about in Chapter 13. When you use Complete PC Restore, everything on the hard drive is lost because the restore process completely erases the drive and restores the OS, user information, applications, and data as they were captured at the time the last Complete PC Backup was made. Therefore, before using Complete PC Restore, consider how old the backup is. Perhaps you can use it to restore drive C and then boot into Windows, reinstall applications installed since the last backup, and use other backups of data more recent than the last Complete PC Backup was made to restore the data.

A+
220-701
2.2
3.4

10. Use the Windows Memory Diagnostic Tool, which you learned to use earlier in the chapter, to test memory.

11. Click **Command Prompt** to open a command prompt window. See Figure 15-39 for an example of this window where the diskpart command is being used. You can use this window to repair a corrupted Vista system or recover data. Commands to use in this window are covered later in the chapter.



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

X:\Sources>diskpart

Microsoft DiskPart version 6.0.6000
Copyright (C) 1999-2007 Microsoft Corporation.
On computer: MINWINPC

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   New Volume   NTFS   Partition     64 GB  Healthy
  Volume 1     F   LRMCFRE_EN_  UDF    DVD-ROM     2555 MB  Healthy
  Volume 2     E                NTFS   Partition     63 GB  Healthy
  Volume 3     C                NTFS   Partition   15000 MB  Healthy

DISKPART>
```

Figure 15-39 The command prompt window resembles the Windows XP Recovery Console
Courtesy: Course Technology/Cengage Learning

12. As you use a tool in the System Recovery Options window, be sure to reboot after each attempt to fix the problem to make sure the problem has not been resolved before you try another tool. To exit the Recovery Environment, click **Shut Down** or **Restart**.

THE COMMAND PROMPT WINDOW IN WINDOWS RE

Use the command prompt window in Windows RE when graphical tools available in Windows RE fail to solve the Vista problem. In the following subsections, we'll look at some commands that are helpful when solving boot problems. In Chapter 13, you learned about other commands, some of which can be used in the Windows RE command prompt window.

COMMANDS TO REPAIR SYSTEM FILES, BOOT RECORDS, AND PARTITIONS

Table 15-3 lists some commands that can help you repair a system. To get helpful information about a command, enter the command followed by /?, such as **bcdedit /?**.

> **Note** For a complete list of Diskpart commands, go to the Microsoft support site (*support.microsoft.com*) and search on "DiskPart Command-Line Options."

COMMANDS TO RESTORE THE REGISTRY

If key registry files are corrupted or deleted, the system will not start. You can use the Windows RE command prompt window to restore registry files using those saved in the C:\Windows\System32\Config\RegBack folder. This RegBack folder contains partial backups of the registry files put there after a successful boot. Use the commands in Table 15-4 to restore the registry files.

A+
220-701
2.2
3.4

Command Line	Description
Bootrec /scanOS	Scans the hard drive for Windows installations not stored in the BCD
Bootrec /rebuildBCD	Scans for Windows installations and rebuilds the BCD
Bcdedit	Manually edits BCD; be sure to make a copy of the file before you edit it
Bootrec /fixboot	Repairs the boot sector of the system partition
Bootrec /fixmbr	Repairs the MBR
Diskpart	Manages partitions and volumes Enter the command to open a DISKPART> command prompt and then use these commands: *Clean*—Removes any partition or volume information from the selected drive. Can be used to remove dynamic disk information or a corrupted partition table *List disk*—Lists installed hard drives *List partition*—Lists partitions on selected drive *Select disk*—Selects a hard drive. For example: *select disk 0* *Select partition*—Selects a partition on the selected drive *Active*—Makes the selected partition the active partition *Inactive*—Makes the selected partition inactive
Bootsect	Repairs problems with dual-booting PCs. You can also use the command to remove Vista from a dual-boot configuration so that you can delete an old operating system used in the dual boot.
Chkdsk c: /r	Repairs errors on drive C

Table 15-3 Commands used in the command prompt window of Windows RE to repair system files and the file system

Command Line	Description
1. c:	Makes drive C the current drive.
2. cd \windows\system32\config	Makes the Windows registry folder the current folder.
3. ren default default.save 4. ren sam sam.save 5. ren security security.save 6. ren software software.save 7. ren system system.save	Renames the five registry files.
8. cd regback	Makes the registry backup folder the current folder.
9. copy system c:\windows\system32\config	For hardware problems, first try copying just the System hive from the backup folder to the registry folder and then reboot.

Table 15-4 Steps to restore the registry files

A+
220-701
2.2
3.4

Command Line	Description
10. copy software c:\windows\system32\config	For software problems, first try copying just the Software hive to the registry folder, and then reboot.
11. copy system c:\windows\system32\config 12. copy software c:\windows\system32\config 13. copy default c:\windows\system32\config 14. copy sam c:\windows\system32\config 15. copy security c:\windows\system32\config	If the problem is still not solved, try copying all five hives to the registry folder and reboot.

Table 15-4 Steps to restore the registry files (continued)

After you try each fix, reboot the system to see if the problem is solved before you do the next fix.

WINDOWS 2000/XP TOOLS FOR SOLVING STARTUP PROBLEMS

To know how to support the Windows 2000/XP boot process, it's not necessary to understand every detail of this process, but it does help to have a general understanding of the more important steps. In this part of the chapter, you learn what happens during the boot process and about the Boot.ini file. Then you'll learn about tools that can help when Windows 2000/XP gives startup problems, including the Advanced Options Menu, the Windows 2000/XP Boot Disk, the Recovery Console, and the Windows 2000 Emergency Repair process.

WHAT HAPPENS WHEN WINDOWS 2000/XP STARTS UP

A Windows 2000/XP system has started up when the user has logged on, the Windows desktop is loaded, and the hourglass associated with the pointer has disappeared. Table 15-5 outlines the steps in the boot sequence for Intel-based computers up to the point that the boot loader program, Ntldr, turns control over to the Windows core component program, Ntoskrnl.exe.

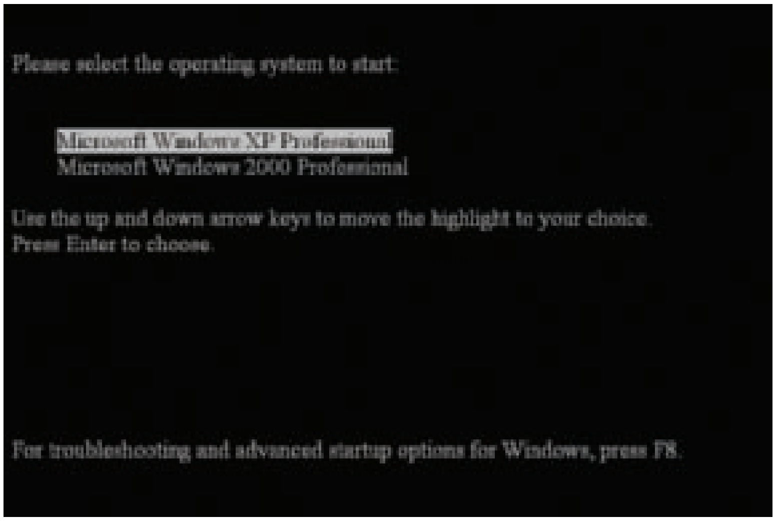
Step	Step Performed By	Description
1.	Startup BIOS	Startup BIOS runs the POST (power-on self test).
2.	Startup BIOS	Startup BIOS turns to the hard drive to find an OS. It first loads the MBR (Master Boot Record) and runs the master boot program within the MBR. (Recall that the master boot program is at the very beginning of the hard drive, before the partition table information.)
3.	MBR program	The MBR program uses partition table information to find the active partition. It then loads the OS boot sector (also called the OS boot record) from the active partition and runs the program in this boot sector.
4.	Boot sector program	This boot sector program launches Ntldr (NT Loader).

Table 15-5 Steps in the Windows 2000/XP boot process for systems with Intel-based processors

A+
220-701
2.2
3.4

Step	Step Performed By	Description
5.	Ntldr, the Windows 2000/XP boot-strap loader program	Ntldr changes the processor from real mode to 32-bit flat memory mode, in which 32-bit code can be executed.
6.	Ntldr	Ntldr launches the minifile system drivers so that files can be read from either a FAT system or an NTFS file system on the hard drive.
7.	Ntldr	Ntldr reads the Boot.ini file, a hidden text file that contains information about installed OSs on the hard drive. Using this information, Ntldr builds the boot loader menu described in the file. The menu is displayed if Ntldr recognizes a dual-boot system or sees a serious problem with the boot (see Figure 15-40). Using the menu, a user can decide which OS to load or accept the default selection by waiting for the preset time to expire.
8.	Ntldr	If the user chooses an OS other than Windows 2000/XP, then Ntldr runs Bootsect.dos and Ntldr is terminated. Bootsect.dos is responsible for loading the other OS.
9.	Ntldr	If the user chooses Windows 2000/XP, then the loader runs Ntdetect.com, a 16-bit real mode program that queries the computer for time and date (taken from CMOS RAM) and surveys hardware (buses, drives, mouse, ports). Ntdetect passes the information back to Ntldr. This information is used later to update the Windows 2000/XP registry concerning the Last Known Good hardware profile used.
10.	Ntldr	Ntldr then loads Ntoskrnl.exe, Hal.dll, and the System hive. Recall that the System hive is a portion of the Windows 2000/XP registry that includes hardware information used to load the proper device drivers for the hardware that's present. Ntldr then loads these device drivers.
11.	Ntldr	Ntldr passes control to Ntoskrnl.exe; Ntoskrnl.exe continues to load the Windows desktop and the supporting Windows environment.

Table 15-5 Steps in The Windows 2000/XP boot process for systems with Intel-based processors (continued)



```
Please select the operating system to start:

     Microsoft Windows XP Professional
     Microsoft Windows 2000 Professional

Use the up and down arrow keys to move the highlight to your choice.
Press Enter to choose.




For troubleshooting and advanced startup options for Windows, press F8.
```

Figure 15-40 The Windows 2000/XP boot loader menu allows the user to choose which OS to load
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2
3.4

FILES NEEDED TO START WINDOWS 2000/XP

The files needed to boot Windows 2000/XP successfully are listed in Table 15-6. Several of these system files form the core components of Windows 2000/XP.

File	Location and Description
Ntldr	◢ Located in the root folder of the system partition (usually C:\) ◢ Boot-strap loader program
Boot.ini	◢ Located in the root folder of the system partition (usually C:\) ◢ Text file contains boot parameters
Bootsect.dos	◢ Located in the root folder of the system partition (usually C:\) ◢ Used to load another OS in a dual-boot environment
Ntdetect.com	◢ Located in the root folder of the system partition (usually C:\) ◢ Real-mode program detects hardware present
Ntbootdd.sys	◢ Located in the root folder of the system partition (usually C:\) ◢ Required only if a SCSI boot device is used
Ntoskrnl.exe	◢ Located in \*%SystemRoot%*\system32 folder of the boot partition (usually C:\Windows\system32) ◢ Core component of the OS executive and kernel services
Hal.dll	◢ Located in \*%SystemRoot%*\system32 folder of the boot partition (usually C:\Windows\system32) ◢ Hardware abstraction layer
Ntdll.dll	◢ Located in \*%SystemRoot%*\system32 folder of the boot partition (usually C:\Windows\system32) ◢ Intermediating service to executive services; provides many support functions
Win32k.sys Kernel32.dll Advapi32.dll User32.dll Gdi32.dll	◢ Located in \*%SystemRoot%*\system32 folder of the boot partition (usually C:\Windows\system32) ◢ Core components of the Win32 subsystem
System	◢ Located in \*%SystemRoot%*\system32\config folder of the boot partition (usually C:\Windows\system32\config) ◢ Registry hive that holds hardware configuration data, including which device drivers need loading at startup
Device drivers	◢ Located in \*%SystemRoot%*\system32\drivers folder of the boot partition (usually C:\Windows\system32\drivers) ◢ Windows and third-party drivers needed for startup
Pagefile.sys	◢ Located in the root folder of the system partition (usually C:\) ◢ Virtual memory swap file

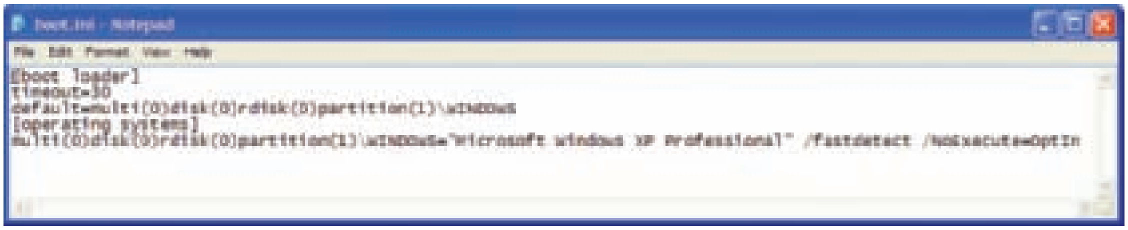
Table 15-6 Files needed to boot Windows 2000/XP successfully

Notes When repairing a corrupted hard drive, a support person often copies files from one PC to another. However, the Bootsect.dos file contains information from the partition table for a particular hard drive and cannot be successfully copied from another PC.

A+
220-701
2.2
3.4

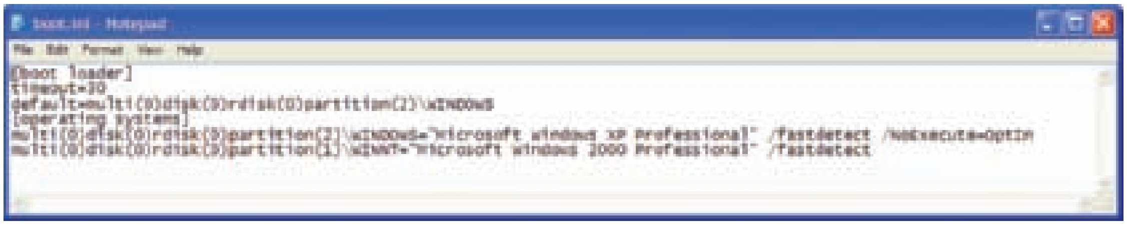
THE BOOT.INI FILE

One key file used by Windows 2000/XP startup is Boot.ini. Recall that the Boot.ini file is a hidden text file stored in the root directory of the active partition that Ntldr reads to see what operating systems are available and how to set up the boot. You can view and edit the Boot.ini file, which might be necessary when you are trying to solve a difficult boot problem. Figure 15-41 shows an example of a Boot.ini file for Windows XP. Figure 15-42 shows a similar file for a system that uses a Windows 2000 and Windows XP dual boot.



```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect /NoExecute=OptIn
```

Figure 15-41 A sample Windows XP Boot.ini file
Courtesy: Course Technology/Cengage Learning



```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Microsoft Windows XP Professional" /fastdetect /NoExecute=OptIn
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Professional" /fastdetect
```

Figure 15-42 A sample Boot.ini file on a dual-boot system
Courtesy: Course Technology/Cengage Learning

Before you can view or edit the Boot.ini file using a text editor such as Notepad, you must first change the folder options to view hidden system files. To do so, open **Windows Explorer**, select the root directory, click **Tools** on the menu bar, click **Folder Options**, and then select the **View** tab. Uncheck the option to **Hide protected operating system files**.

There are two main sections in Boot.ini: the [boot loader] section and the [operating systems] section. The [boot loader] section contains the number of seconds the system gives the user to select an operating system before it loads the default operating system; this is called a timeout. In Figure 15-41, the timeout is set to 30 seconds, the default value. If the system is set for a dual boot, the path to the default operating system is also listed in the [boot loader] section. In Figure 15-42, you can see the default OS is loaded from the \Windows folder in the second partition.

The [operating systems] section of the Boot.ini file provides a list of operating systems that can be loaded, including the path to the boot partition of each operating system. Here is the meaning of each entry in Figure 15-42:

- *Multi(0)*. Use the first hard drive controller.
- *Disk(0)*. Use only when booting from a SCSI hard drive.
- *Rdisk(0)*. Use the first hard drive.
- *Partition(1)*. Use the first partition on the drive.

A+
220-701
2.2
3.4

Switches are sometimes used in the [operating systems] section. In Figure 15-41, the first switch used in this Boot.ini file is /fastdetect, which causes the OS not to attempt to inspect any peripherals connected to a COM port (serial port) at startup.

The second switch is /NoExecute=OptIn. This switch is new with Windows XP Service Pack 2 and is used to configure Data Execution Prevention (DEP). DEP stops a program if it tries to use a protected area of memory, which some viruses attempt to do.

Although you can change the Boot.ini file by editing it, a better way to make changes is by using the System Properties box. To access it, right-click My Computer and select Properties from the shortcut menu. Several of the startup and recovery options that you can change in this box are recorded as changes to Boot.ini.

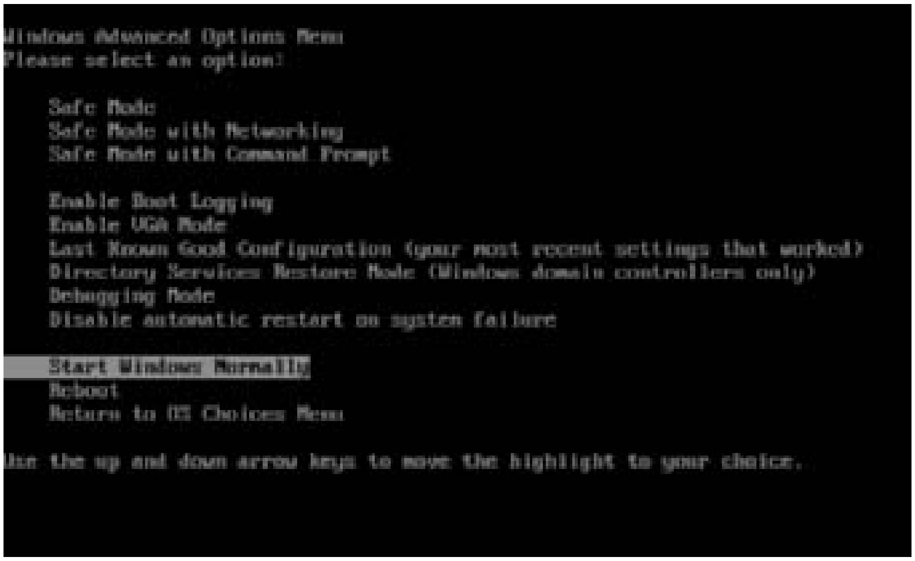
Notes Many technical people use the terms "boot" and "startup" interchangeably. However, in general, the term "boot" refers to the hardware phase of starting up a computer. Microsoft consistently uses the term "startup" to refer to how its operating systems are booted, well, started, I mean.

ADVANCED OPTIONS MENU

As a PC boots and the "Starting Windows" message appears at the bottom of the screen, press the F8 key to display the Windows XP **Advanced Options menu,** which is shown in Figure 15-43, or the Windows 2000 Advanced Options menu, which is shown in Figure 15-44. This menu can be used to diagnose and fix problems when booting Windows 2000/XP. The purpose of each menu option is outlined earlier in the chapter.

WINDOWS 2000/XP BOOT DISK

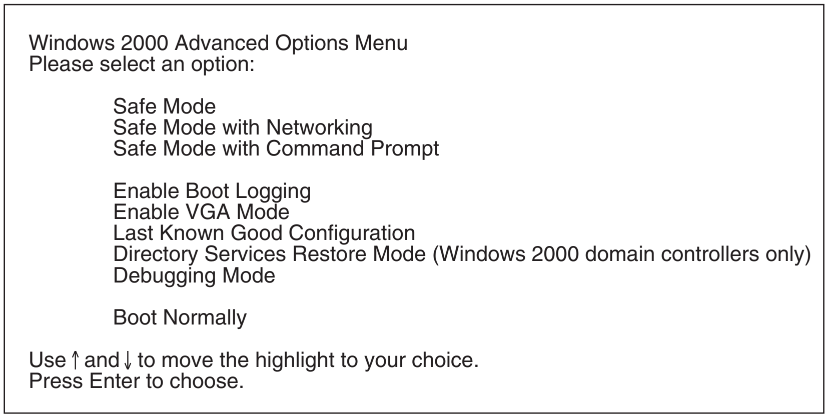
A Windows 2000/XP boot disk can be used to boot the system bypassing the boot files stored in the root directory of drive C. If you boot from the disk and the Windows 2000/XP desktop loads successfully, then the problem is associated with damaged sectors or missing or damaged files in the root directory of drive C that are required to boot the OS. These sectors



```
Windows Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration (your most recent settings that worked)
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode
    Disable automatic restart on system failure

    Start Windows Normally
    Reboot
    Return to OS Choices Menu

Use the up and down arrow keys to move the highlight to your choice.
```

Figure 15-43 Press the F8 key at startup to display the Windows XP Advanced Options menu
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2
3.4



```
Windows 2000 Advanced Options Menu
Please select an option:

        Safe Mode
        Safe Mode with Networking
        Safe Mode with Command Prompt

        Enable Boot Logging
        Enable VGA Mode
        Last Known Good Configuration
        Directory Services Restore Mode (Windows 2000 domain controllers only)
        Debugging Mode

        Boot Normally

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.
```

Figure 15-44 The Windows 2000 Advanced Options menu
Courtesy: Course Technology/Cengage Learning

and files include the master boot program; the partition table; the OS boot record; the boot files Ntldr file, Ntdetect.com file, and Ntbootdd.sys (if it exists); and the Boot.ini file. In addition, the problem can be caused by a boot sector virus. However, a boot disk cannot be used to troubleshoot problems associated with unstable device drivers or any other system files stored in the \Windows folder or its subfolders.

You first create the boot disk by formatting the disk using a working Windows 2000/XP computer and then copying files to the disk. These files can be copied from a Windows 2000/XP setup CD, or a Windows 2000/XP computer that is using the same version of Windows XP or Windows 2000 as the problem PC. Do the following to create the disk:

1. Obtain a floppy disk and format it on a Windows 2000/XP computer.
2. Using Explorer, copy Ntldr and Ntdetect.com from the \i386 folder on the Windows 2000/XP setup CD or a Windows 2000/XP computer to the root of the floppy disk.
3. If your computer boots from a SCSI hard drive, then obtain a device driver (*.sys) for your SCSI hard drive, rename it **Ntbootdd.sys**, and copy it to the root of the floppy disk. (If you used an incorrect device driver, then you will receive an error after booting from the floppy disk. The error will mention a “computer disk hardware configuration problem” and that it “could not read from the selected boot disk.” If this occurs, contact your computer manufacturer or hard drive manufacturer for the correct version of the SCSI hard drive device driver for your computer.)
4. Look at Boot.ini on the problem computer, and then obtain an identical copy from another known good computer (or create your own) and copy it to the root of the floppy disk.
5. If you can’t find a good Boot.ini file to copy, you can use the lines listed below to create a Boot.ini file. These lines work for a Boot.ini file if the problem computer is booting from an IDE hard drive:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=”Microsoft Windows
XP Professional” /fastdetect
```

A+
220-701
2.2
3.4

6. Write-protect the floppy disk so that it cannot become infected with a virus.
7. You have now created the Windows 2000/XP boot disk. Check BIOS setup to make sure the first boot device is set to the floppy disk, and then insert the boot disk and reboot your computer.

Tip If you are creating your own Boot.ini file, be sure to enter a hard return after the /fastdetect switch in the last line of the file.

Notes To learn more about the Windows XP boot disk, see the Microsoft Knowledge Base Articles 305595 and 314503 at the Microsoft Web site *support.microsoft.com*. To learn more about the Windows 2000 boot disk, see the Microsoft Knowledge Base Article 301680.

If the Windows 2000/XP desktop loads successfully, then do the following to attempt to repair the Windows 2000/XP installation:

1. Load the Recovery Console and use the Fixmbr and Fixboot commands to repair the MBR and the OS boot sector.
2. Run antivirus software.
3. Use Disk Management to verify that the hard drive partition table is correct.
4. Defragment your hard drive.
5. Copy Ntldr, Ntdetect.com, and Boot.ini from your floppy disk to the root of the hard drive.
6. If you're using a SCSI hard drive, copy Ntbootdd.sys from your floppy disk to the root of the hard drive.

If the Windows 2000/XP desktop did not load by booting from the boot disk, then the next tool to try is the Recovery Console.

RECOVERY CONSOLE

The Advanced Options Menu can help if the problem is a faulty device driver or system service. However, if the problem goes deeper than that, the next tool to use is the **Recovery Console**. Use it when Windows 2000/XP does not start properly or hangs during the load. It works even when core Windows system files are corrupted. The Recovery Console is a command-driven operating system that does not use a GUI. With it, you can access the FAT16, FAT32, and NTFS file systems.

Using the Recovery Console, you can:

- Repair a damaged registry, system files, or file system on the hard drive.
- Enable or disable a service or device driver.
- Repair the master boot program on the hard drive or the boot sector on the system partition.

A+
220-701
2.2
3.4

- Repair a damaged Boot.ini file.
- Recover data when the Windows installation is beyond repair.

The Recovery Console is designed so that someone can't maliciously use it to gain unauthorized access. You must enter the Administrator password in order to use the Recovery Console and access an NTFS volume. Unless you first set certain parameters, you are not allowed into all folders, and you cannot copy files from the hard drive to a removable media. If the registry is so corrupted that the Recovery Console cannot read the password in order to validate it, you are not asked for the password, but you are limited in what you can do at the Recovery Console.

Now let's look at a list of Recovery Console commands, how to access the Recovery Console, how to use it to perform several troubleshooting tasks, and how to install the Recovery Console on the boot loader menu.

LIST OF RECOVERY CONSOLE COMMANDS

As a summary reference, Table 15-7 lists Recovery Console commands and their descriptions.

Command	Description	Examples
Attrib	Changes the attributes of a file or folder.	To remove the read-only, hidden, and system attributes from the file: `C:\> Attrib -r -h -s filename`

Batch	Carries out commands stored in a batch file.	To execute the commands in File1:
		`C:\> Batch File1.bat`
		To execute the commands in File1 and store the results of the commands to File2:
		`C:\> Batch File1.bat File2.txt`

Cd	Displays or changes the current folder. It cannot be used to change drives.	To change folders to the C:\Windows\system folder:
		`C:\> Cd C:\windows\system`
		`C:\windows\system>`

Chkdsk	Checks a disk and repairs or recovers the data.	To check drive C: and repair it: `C:\> Chkdsk C: /r`
Cls	Clears the screen.	`C:\> Cls`
Copy	Copies a single file. Use the command to replace corrupted system files or save data files to another media when the hard drive is failing.	To copy the file File1 on the CD to the hard drive's Winnt folder, naming the file File2: `C:\> Copy D:\File1 C:\Winnt\File2`
Del	Deletes a file.	To delete File2: `C:\Winnt> Del File2`
Dir	Lists files and folders. Wildcard characters are allowed.	To list all files with an .exe file extension: `C:\> Dir *.exe`

Table 15-7 Commands available from the Recovery Console

A+
220-701
2.2
3.4

Command	Description	Examples
Disable	Disables a service or driver. Use it to disable a service or driver that starts and prevents the system from booting properly. After you disable the service, restart the system to see if your problem is solved.	To disable the Event Log service: `C:\> Disable eventlog`
Diskpart	Creates and deletes partitions on the hard drive.	Enter the command with no arguments to display a user interface: `C:\> Diskpart`
Enable	Displays the status and enables a Windows system service or driver.	To display the status of the Event Log service: `C:\> Enable eventlog`
Exit	Quits the Recovery Console and restarts the computer.	`C:\> Exit`

Expand	Expands compressed files and extracts files from cabinet files and copies the files to the destination folder.	To extract File1 from the Drivers.cab file:
		`C:\> Expand D:\i386\Drivers.cab -f:File1`
		To expand the compressed file, File1.cp_:
		`C:\> Expand File1.cp_`

Fixboot	Rewrites the OS boot sector on the hard drive. If a drive letter is not specified, the system drive is assumed.	To repair the OS boot sector of drive C: `C:\> Fixboot C:`
Fixmbr	Rewrites the Master Boot Record boot program.	To repair the Master Boot Record boot program: `C:\> Fixmbr`

Format	Formats a logical drive. If no file system is specified, NTFS is assumed.	To format using the NTFS file system:
		`C:\> Format D:`
		To format using the FAT32 file system:
		`C:\> Format D:/fs:FAT32`

Help	Help utility appears for the given command.	To get help with the Fixboot command: `C:\> Help fixboot`
Listsvc	Lists all available services. This command has no parameters.	`C:\> Listsvc`
Logon	Allows you to log onto an installation with the Administrator password. Use it to log onto a second installation of Windows in a dual-boot environment.	When logged onto the first Windows installation, use this command to log onto the second installation: `C:\> logon 2` If you don't enter the password correctly after three tries, the system automatically reboots.
Map	Lists all drive letters and file system types.	`C:\> Map`

Table 15-7 Commands available from the Recovery Console (continued)

A+
220-701
2.2
3.4

Command	Description	Examples
Md or Mkdir	Creates a folder.	`C:\> MD C:\TEMP`
More or Type	Displays a text file on-screen.	`C:\> Type filename.txt`
Rd or Rmdir	Deletes a directory.	`C:\> RD C:\TEMP`
Rename or Ren	Renames a file.	`C:\> Rename File1.txt File2.txt`
Set	Displays or sets Recovery Console environmental variables.	To turn off the prompt when you are overwriting files: `C:\> Set nocopyprompt=true`

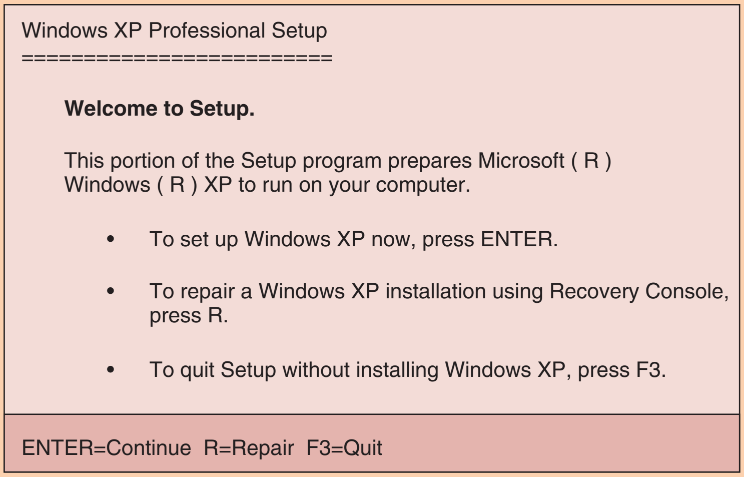
Systemroot	Sets the current directory to the directory where Windows 2000/XP is installed.	`C:\> Systemroot`
		`C:\WINDOWS>`

Table 15-7 Commands available from the Recovery Console (continued)

APPLYING CONCEPTS — HOW TO ACCESS THE RECOVERY CONSOLE

The Recovery Console software is on the Windows 2000/XP setup CD and the four Windows 2000 setup disks. You can launch the Recovery Console from the CD or four disks, or manually install the Recovery Console on the hard drive and launch it from there.

How to access the Recovery Console using Windows XP. For Windows XP, to use the Recovery Console, insert the Windows XP setup CD in the CD drive and restart the system. When the Windows XP Setup opening menu appears (see Figure 15-45), press **R** to load the Recovery Console.



```
Windows XP Professional Setup
=========================

     Welcome to Setup.

     This portion of the Setup program prepares Microsoft ( R )
     Windows ( R ) XP to run on your computer.

          •    To set up Windows XP now, press ENTER.

          •    To repair a Windows XP installation using Recovery Console,
               press R.

          •    To quit Setup without installing Windows XP, press F3.

ENTER=Continue  R=Repair  F3=Quit
```

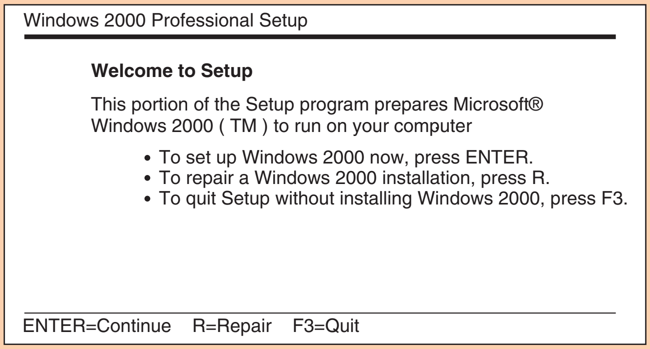
Figure 15-45 Windows XP Setup opening menu
Courtesy: Course Technology/Cengage Learning

Access the Recovery Console using Windows 2000. For Windows 2000, you can boot from the Windows 2000 setup CD or you can boot from the four setup disks. Use the four setup disks if the computer will not boot from a CD drive. If you have not already created the Windows 2000 setup

A+
220-701
2.2
3.4

disks, you can go to a working Windows 2000 PC and create the disks by following the directions given in Chapter 12. Follow these steps to load Windows 2000 from the disks or from the setup CD and access the Recovery Console:

1. Insert the first of the four setup disks, and restart the PC. You are directed to insert each of the four disks in turn, and then the Setup screen appears, as shown in Figure 15-46. If you boot from the Windows 2000 setup CD, the same screen appears.



Windows 2000 Professional Setup

Welcome to Setup

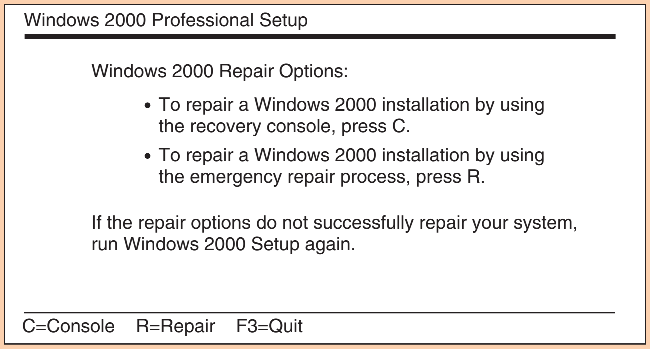
This portion of the Setup program prepares Microsoft®
Windows 2000 (TM) to run on your computer

- To set up Windows 2000 now, press ENTER.
- To repair a Windows 2000 installation, press R.
- To quit Setup without installing Windows 2000, press F3.

ENTER=Continue R=Repair F3=Quit

Figure 15-46 Use this Windows 2000 Setup screen to access the Recovery Console
Courtesy: Course Technology/Cengage Learning

2. Type **R** to select the "To repair a Windows 2000 installation" option. The Windows 2000 Repair Options window opens (see Figure 15-47). Type **C** to select the Recovery Console.



Windows 2000 Professional Setup

Windows 2000 Repair Options:

- To repair a Windows 2000 installation by using the recovery console, press C.
- To repair a Windows 2000 installation by using the emergency repair process, press R.

If the repair options do not successfully repair your system, run Windows 2000 Setup again.

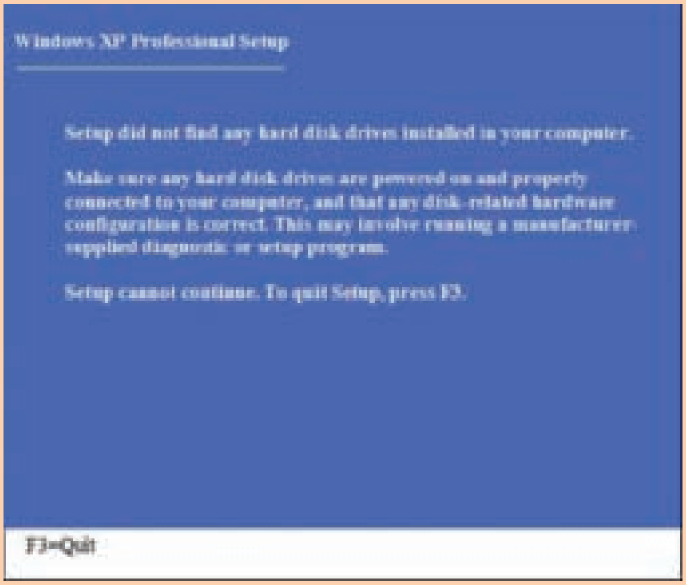
C=Console R=Repair F3=Quit

Figure 15-47 Windows 2000 offers two repair options
Courtesy: Course Technology/Cengage Learning

3. Note that as the Recovery Console attempts to load and give you access to the hard drive, it will display one of the following screens depending on the severity of the problem with the drive:

   - If the Recovery Console cannot find the drive, the window in Figure 15-48 appears. Consider the problem hardware related. You might have a totally dead drive.

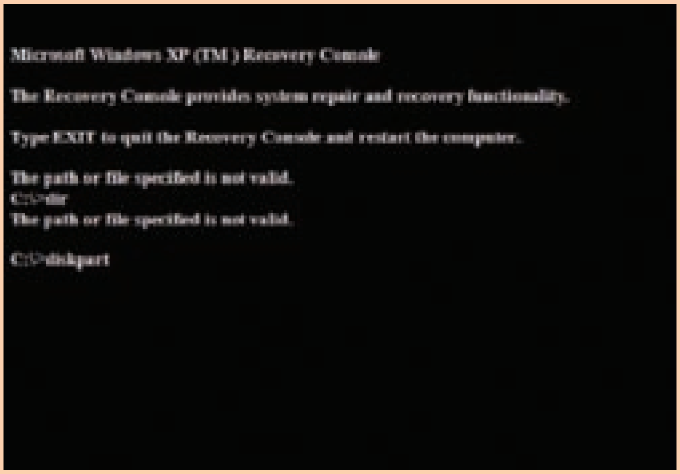
A+
220-701
2.2
3.4



```
Windows XP Professional Setup

   Setup did not find any hard disk drives installed in your computer.

   Make sure any hard disk drives are powered on and properly
   connected to your computer, and that any disk-related hardware
   configuration is correct. This may involve running a manufacturer-
   supplied diagnostic or setup program.

   Setup cannot continue. To quit Setup, press F3.

F3=Quit
```

Figure 15-48 Windows setup cannot find a hard drive
Courtesy: Course Technology/Cengage Learning

- If the Console can find the hard drive, but cannot read from it, the window in Figure 15-49 appears. Notice in the window the C prompt (C:\>), which seems to indicate that the Recovery Console can access the hard drive, but the message above the C prompt says otherwise. When you try the DIR command, as shown in Figure 15-49, you find out that drive C: is not available. The Diskpart, Fixmbr, and Fixboot commands might help.

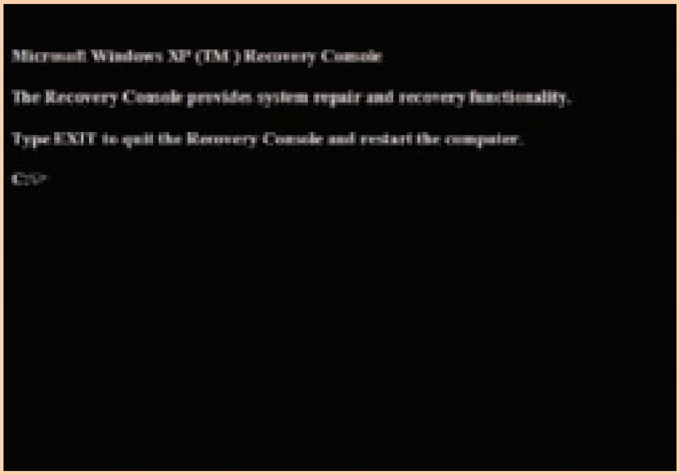


```
Microsoft Windows XP (TM) Recovery Console

The Recovery Console provides system repair and recovery functionality.

Type EXIT to quit the Recovery Console and restart the computer.

The path or file specified is not valid.
C:\>dir
The path or file specified is not valid.

C:\>diskpart
```

Figure 15-49 The Recovery Console cannot read from the hard drive
Courtesy: Course Technology/Cengage Learning

- If the Console is able to read drive C, but Windows is seriously corrupted, the window in Figure 15-50 appears. Use the DIR command to see what files or folders are still on the drive. Is the \Windows folder present? If not, then you might need to reformat the drive and reinstall Windows. But first try to find any important data that is not backed up.

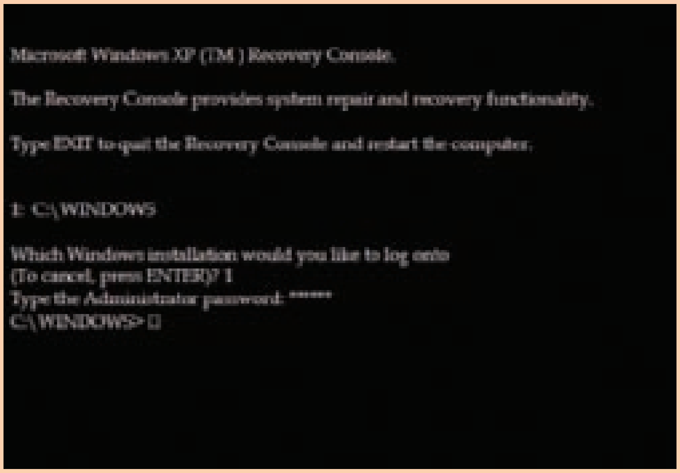
A+
220-701
2.2
3.4



```
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.

C:\>
```

Figure 15-50 The Recovery Console can read drive C, but cannot find a Windows installation
Courtesy: Course Technology/Cengage Learning

- If the Console is able to determine that one or more Windows installations is on the drive, it gives you a choice of with which installation you want to work. If only one installation is showing, as in Figure 15-51, type **1** and press **Enter**. Next, you will be asked for the Administrator password. Enter the password and press **Enter**. The command prompt shows the Windows folder is the current working directory. You can now use the Recovery Console to try to find the problem and fix it. How to do that is coming up next.



```
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 installation would you like to log onto
(To cancel, press ENTER)? 1
Type the Administrator password: ******
C:\WINDOWS>
```

Figure 15-51 The Recovery Console has found a Windows installation
Courtesy: Course Technology/Cengage Learning

4. To exit the Recovery Console, type **Exit** and press **Enter**. The system will attempt to boot to the Windows desktop.

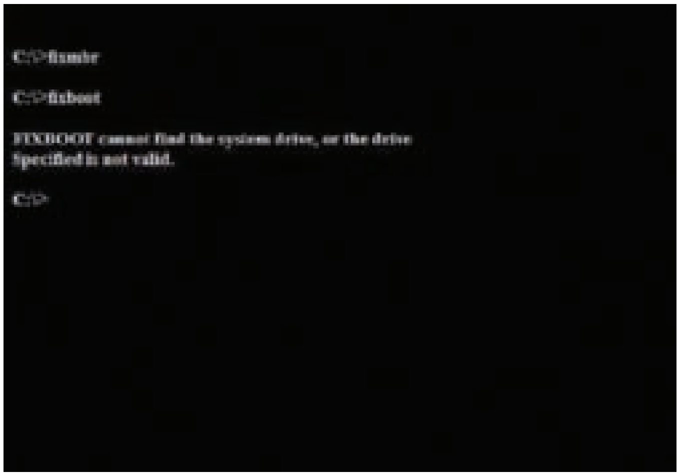
A+
220-701
2.2
3.4

USE THE RECOVERY CONSOLE TO FIX HARD DRIVE PROBLEMS

Here are the commands you can use to examine the hard drive structure for errors and possibly fix them:

> **Notes** Here are two useful tips to help you when using the Recovery Console: To retrieve the last command entered, press **F3** at the command prompt. To retrieve the command one character at a time, press the **F1** key.

- ***Fixmbr and Fixboot.*** The Fixmbr command restores the master boot program in the MBR, and the Fixboot command repairs the OS boot record. As you enter each command, you're looking for clues that might indicate at what point the drive has failed. For example, Figure 15-52 shows the results of using the Fixmbr command, which appears to have worked without errors, but the Fixboot command has actually failed. This tells us that most likely the master boot program is healthy, but drive C is not accessible. After using these commands, if you don't see any errors, exit the Recovery Console and try to boot from the hard drive.



```
C:\>fixmbr

C:\>fixboot

FIXBOOT cannot find the system drive, or the drive
Specified is not valid.

C:\>
```

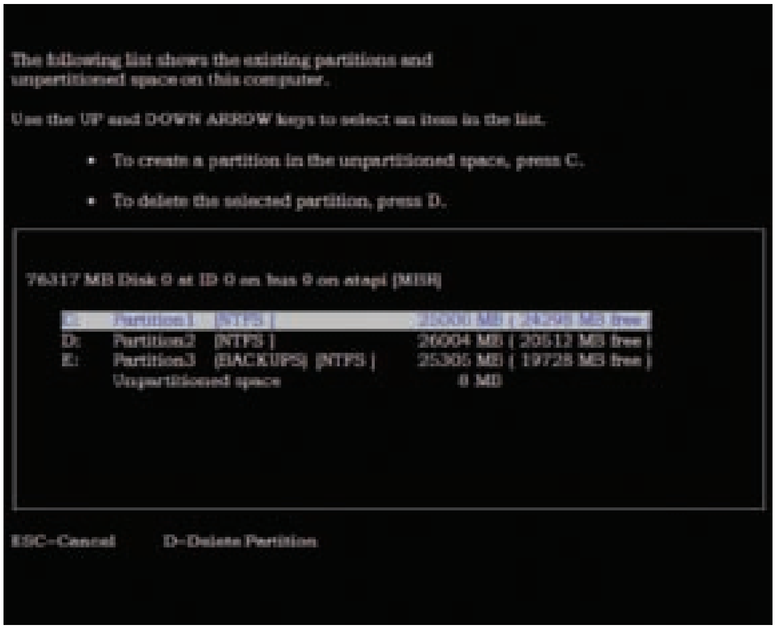
Figure 15-52 Results of using the Fixmbr and Fixboot commands in the Recovery Console
Courtesy: Course Technology/Cengage Learning

- ***Diskpart.*** Use the Diskpart command to view, create, and delete partitions on the drive. Type **Diskpart** and press **Enter** and a full screen appears, listing the partitions the Console sees on the drive. See Figure 15-53.
- ***Chkdsk.*** Use this command to repair the file system and recover data from bad sectors: **chkdsk C: /r**.

USE THE RECOVERY CONSOLE TO RESTORE THE REGISTRY

Earlier in the chapter, you learned how to use commands in the command prompt window of the Vista Recovery Environment to restore the registry files from backup. These backup hive files are located in the C:\Windows\System32\config\regback folder. You can use a similar group of commands to restore the Windows XP or Windows 2000 registry hive files

A+
220-701
2.2
3.4



```
The following list shows the existing partitions and
unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

     •  To create a partition in the unpartitioned space, press C.

     •  To delete the selected partition, press D.

  76317 MB Disk 0 at ID 0 on bus 0 on atapi [MBR]

     C:   Partition1  [NTFS]                  25000 MB ( 24290 MB free )
     D:   Partition2  [NTFS]                  26004 MB ( 20512 MB free )
     E:   Partition3  [BACKUPS] [NTFS]        25305 MB ( 19728 MB free )
          Unpartitioned space                     8 MB

ESC=Cancel     D=Delete Partition
```

Figure 15-53 Using the Diskpart screen, you can view, delete, and create partitions
Courtesy: Course Technology/Cengage Learning

from backups. The Windows XP backup files are stored in C:\Windows\System32\config\repair, and the Windows 2000 backup files are stored in C:\Windows\System32\config\repair\regback. See Table 15-3 for the commands to use.

USE THE RECOVERY CONSOLE TO DISABLE A SERVICE OR DEVICE DRIVER

Sometimes when Windows fails, it first displays a stop error (blue screen error). The stop error might give the name of a service or device driver that caused the problem. If the service or driver is critical to Windows operation, booting into Safe Mode won't help because the service or driver will be attempted in Safe Mode. The solution is to boot the system using the Recovery Console and copy a replacement program file from the Windows 2000/XP setup CD to the hard drive.

In order to know what program file to replace, you'll need to know the name or description of the service or driver causing the problem. If an error message doesn't give you the clue you need, you might try to boot to the Advanced Options Menu (press **F8** while booting) and then select **Enable Boot Logging**. Then compare the Ntbtlog.txt file to one generated on a healthy system. You might be able to find the driver or service that caused the boot to halt.

If you know the service causing the problem, use these commands to list services and disable and enable a service:

- *Listsvc*. Enter the command Listsvc to see a list of all services currently installed, which includes device drivers. The list scrolls on and on, showing the name of each service, a brief one-line description, and its status (disabled, manual, or auto). To find the service giving the problem, you'll have to have more information than what this list shows.
- *Disable*. Use the Disable command to disable a service. For example, to disable the service SharedAccess, which is the Windows Firewall service, use this command: **disable**

A+
220-701
2.2
3.4

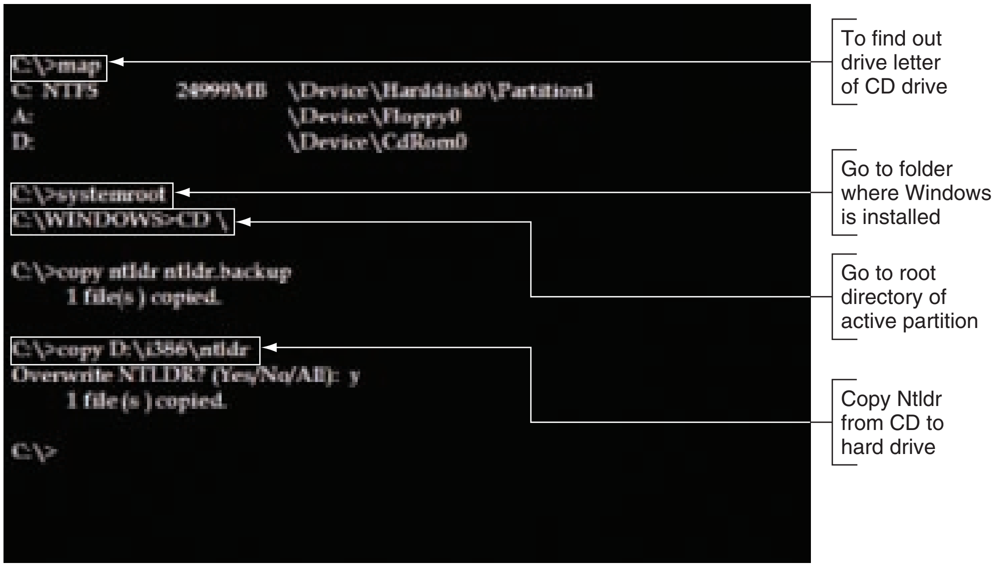
sharedaccess. Before you enter the command, be sure to write down the current startup type that is displayed so that you'll know how to enable the service later. For services that are auto-started like this one, the startup type is service_auto_start.

- *Enable*. Use the Enable command followed by the name of the service to show the current status of a service. To enable the service, use the startup type in the command line. For example, to reinstate the Firewall service, use this command: **enable sharedaccess service_auto-start.**

If you think you've found the service that is causing the problem, disable it and reboot the system. If the problem disappears or the error message changes, you might have found the right service to replace. The next step is to replace the program file with a fresh copy from the Windows setup CD.

USE THE RECOVERY CONSOLE TO RESTORE SYSTEM FILES

Based on error messages and your research about them, if you think you know which Windows system file is corrupted or missing, you can use the Recovery Console to copy a new set of system files from the Windows setup CD to the hard drive. For example, suppose you get an error message that Ntldr is corrupted or missing. To replace the file, you could execute the commands in Figure 15-54.



```
C:\>map
C: NTFS          24999MB   \Device\Harddisk0\Partition1
A:                         \Device\Floppy0
D:                         \Device\CdRom0

C:\>systemroot
C:\WINDOWS>CD \

C:\>copy ntldr ntldr.backup
        1 file(s ) copied.

C:\>copy D:\i386\ntldr
Overwrite NTLDR? (Yes/No/All): y
        1 file (s ) copied.

C:\>
```

To find out drive letter of CD drive
Go to folder where Windows is installed
Go to root directory of active partition
Copy Ntldr from CD to hard drive

Figure 15-54 Recovery Console command to repair Ntldr
Courtesy: Course Technology/Cengage Learning

Here are other commands to use to restore system files:

- *Map*. Displays the current drive letters. This command is useful to find your way around the system, such as when you need to know the drive letter for the CD drive.
- *Systemroot*. Use this command to make the Windows directory the default directory (refer to Figure 15-54 for an example of its use).
- *CD*. Change directory. For example, to move to the root directory, use **CD \**.
- *Delete*. Deletes a file. For example, to delete Ntldr in the Temp directory, use this command: **Delete C:\temp\ntldr**.

A+
220-701
2.2
3.4

- *Copy*. To make a backup of the current Ntldr file, use this command:

  ```
  copy ntldr ntldr.backup
  ```

  To copy the Ntldr file from the Windows setup CD to the root directory of the hard drive, use this command:

  ```
  copy D:\i386\ntldr C:\
  ```

Substitute the drive letter for the CD drive in the command line.

A compressed file uses an underscore as the last character in the file extension; for example, Netapi32.dl_. When you use the Copy command, the file will automatically uncompress. For example, use this command to copy Netapi32.dl_ from the setup CD:

```
copy D:\i386\netapi32.dl_ netapi32.dll
```

- *Bootcfg*. This command lets you view and edit the Boot.ini file. Here are useful parameters:

• **bootcfg /list**	Lists entries in Boot.ini
• **bootcfg /copy**	Makes a copy of Boot.ini before you rebuild it
• **bootcfg /rebuild**	Rebuilds the Boot.ini file

- *Expand*. When you're looking for a certain file on the Windows 2000/XP setup CD, you'll find cabinet files that hold groups of compressed files (cabinet files have a .cab file extension). Use the Expand command to extract these files. Here are some useful parameters of the Expand command:

  To list all files in the driver.cab cabinet file:

  ```
  expand D:\i386\driver.cab -f:* /d
  ```

  To extract a file, first use the Cd command to change the default folder to the location where you want the extracted file to go. Then use the Expand command to extract the file. For example, to extract the Splitter.sys file from the Driver.cab file and copy it from the setup CD to the hard drive, use these two commands:

  ```
  cd C:\windows\system32\drivers
  expand D:\i386\driver.cab /f:splitter.sys
  ```

  You can also use the Expand command to uncompress a compressed file. For example, to expand a file and copy it to the current folder, use this command:

  ```
  expand D:\i386\netapi32.dl_
  ```

USE THE RECOVERY CONSOLE TO RECOVER DATA

If your hard drive is corrupted, you still might be able to recover data. The problem with using the Recovery Console to do the job is that, by default, it will not allow you to go into folders other than the system folders or to copy data onto removable media. To do these tasks, you first need to change some Recovery Console settings. Then you can use the Copy command to copy data from the hard drive to other media.

A+
220-701
2.2
3.4

Here are the commands you'll need to change the settings:

- To allow access to all files and folders on all drives:

```
set allowallpaths=true
```

- To allow you to copy any file to another media such as a USB drive or floppy disk:

```
set allowremovablemedia=true
```

- To allow the use of wildcard characters * and ?:

```
set allowwildcards=true
```

OPTIONAL INSTALLATION OF THE RECOVERY CONSOLE

Although the Recovery Console can be launched from the Windows setup CD to recover from system failure, you can also install it on your working system so that it appears on the OS boot loader menu. You can then use it to address less drastic problems that occur when you can boot from the hard drive.

To install the Recovery Console:

1. Open a command window.
2. Change from the current directory to the \i386 folder on the Windows 2000/XP CD.
3. Enter the command **winnt32 /cmdcons**. The Recovery Console is installed.
4. Restart your computer. Recovery Console should now be shown with the list of available operating systems on the OS boot loader menu.

WINDOWS 2000 EMERGENCY REPAIR PROCESS

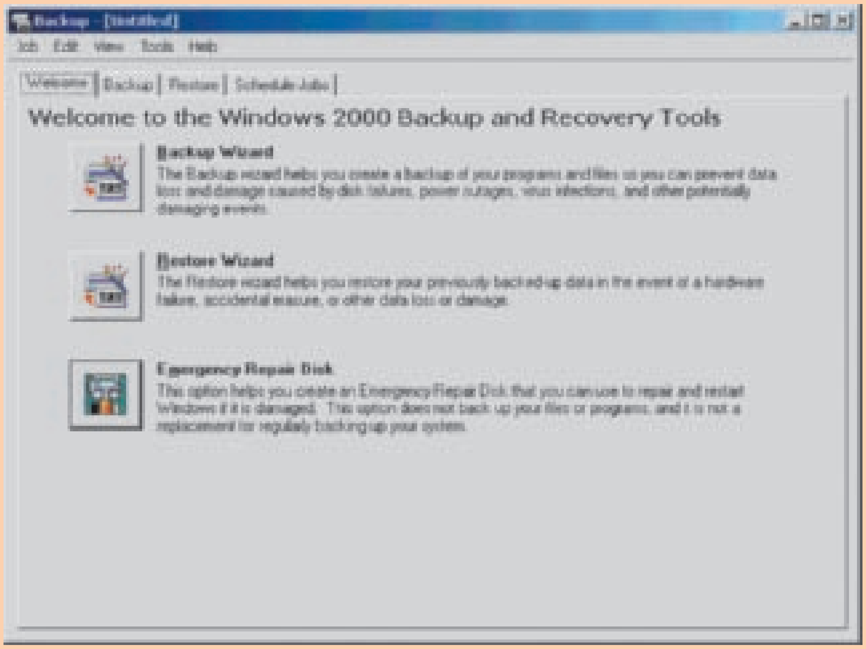
The Windows 2000 Emergency Repair Process should be used only as a last resort because it restores the system to the state it was in immediately after the Windows 2000 installation. All changes made since the installation are lost. The process uses an Emergency Repair Disk (ERD), which contains information about your current installation. The Windows 2000 ERD points to a folder on the hard drive where the registry was backed up when Windows 2000 was installed. This folder is *%SystemRoot%*\repair, which, in most systems, is C:\Winnt\repair.

APPLYING CONCEPTS

Using the Windows 2000 ERD to recover from a corrupted registry returns you to the installation version of the registry, and you lose all changes to the registry since that time. Because of the way the ERD works, you do not need to update the disk once you've created it. Before a problem occurs, follow these directions to create the disk:

1. Click **Start**, point to **Programs**, **Accessories**, and **System Tools**, and then click **Backup**. The Backup window appears with the Welcome tab selected (see Figure 15-55). Select **Emergency Repair Disk**.

A+
220-701
2.2
3.4



Backup - [Untitled]

Welcome to the Windows 2000 Backup and Recovery Tools

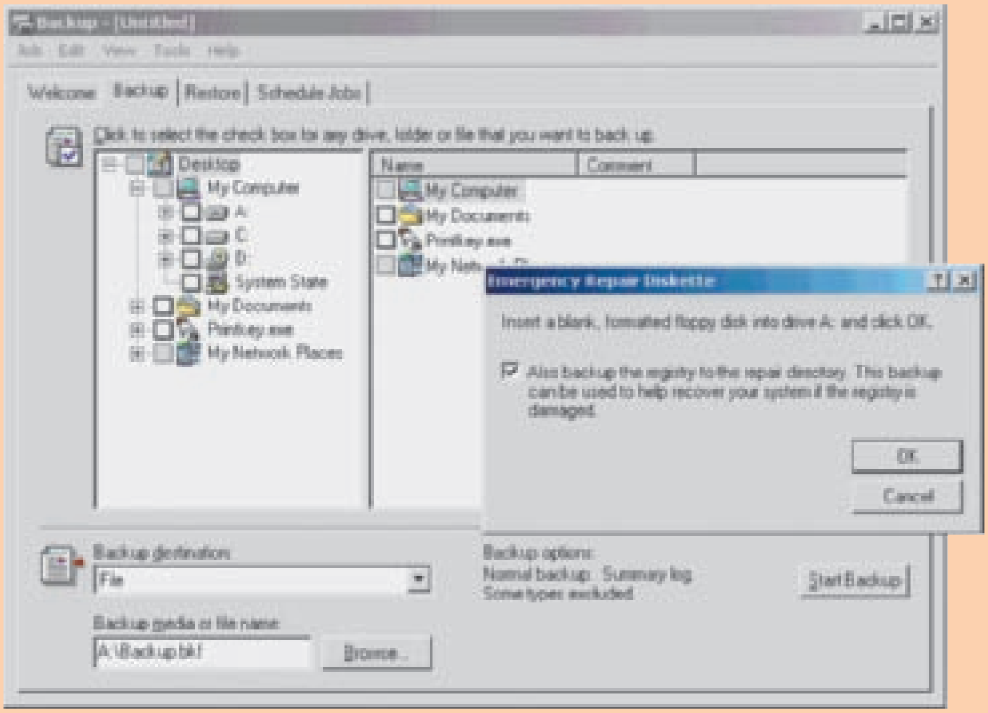
Backup Wizard
The Backup wizard helps you create a backup of your programs and files so you can prevent data loss and damage caused by disk failures, power outages, virus infections, and other potentially damaging events.

Restore Wizard
The Restore wizard helps you restore your previously backed-up data in the event of a hardware failure, accidental erasure, or other data loss or damage.

Emergency Repair Disk
This option helps you create an Emergency Repair Disk that you can use to repair and restart Windows if it is damaged. This option does not back up your files or programs, and it is not a replacement for regularly backing up your system.

Figure 15-55 Use the Backup window to back up the registry and create an emergency repair disk
Courtesy: Course Technology/Cengage Learning

2. The Backup tab and the Emergency Repair Diskette dialog box open. If you check the box shown in Figure 15-56, the system backs up your registry to a folder under the Repair folder, *%SystemRoot%*\repair\RegBack.



Backup - [Untitled]

Click to select the check box for any drive, folder or file that you want to back up.

Emergency Repair Diskette

Insert a blank, formatted floppy disk into drive A: and click OK.

☑ Also backup the registry to the repair directory. This backup can be used to help recover your system if the registry is damaged.

Backup destination: File

Backup media or file name: A:\Backup.bkf

Backup options:
Normal backup. Summary log.
Some types excluded.

Figure 15-56 Create an ERD and back up the registry to the hard drive
Courtesy: Course Technology/Cengage Learning

A+
220-701
2.2
3.4

3. Click **OK** to create the disk. Label the disk "Windows 2000 Emergency Repair Disk," and keep it in a safe place.

If your hard drive fails, you can use the ERD to restore the system, including system files, boot files, and the registry, to its state at the end of the Windows 2000 installation. Follow these steps:

1. Check BIOS setup to make sure the floppy drive appears before the hard drive in the OS boot order.
2. Boot the PC from the four Windows 2000 setup disks. The Setup menu appears (refer back to Figure 15-46). Select option **R**.
3. When the Windows 2000 Repair Options window opens (refer back to Figure 15-47), select option **R**.
4. You are instructed to insert the Emergency Repair Disk. Follow the instructions on the screen to repair the installation.
5. If this process does not work, then your next option is to reinstall Windows 2000. If you don't plan to reformat the drive, you need to scan the drive for errors before you reinstall Windows. To do that, you can boot to the Recovery Console and use the Chkdsk command to scan the drive for errors. If you suspect that a virus damaged the file system, also use the Fixmbr command to replace the master boot program in case it has been corrupted by the virus.

>> CHAPTER SUMMARY

- The Vista Problem Reports and Solution tool and the XP Error Reporting tool can report errors about hardware, applications, and Windows and suggest a solution. In addition, the Vista tool keeps a history of past problems and solutions.
- Use the Vista Memory Diagnostics tool to test memory during the boot.
- Use the System File Checker (SFC) tool to verify and restore system files.
- The Driver Verifier (verifier.exe) tool puts stress on device drivers so that a driver with a problem can be identified. Don't use the tool on a computer unless you understand the potential problems it might cause by degraded performance and STOP errors.
- Use the Startup and Recovery section in the System Properties box to keep Windows from automatically restarting after a STOP error. Automatic restarts can put the boot into an endless loop.
- Tools to verify that drivers are digitally signed are the File Signature Verification tool (sigverif.exe), the Driver Query tool (driverquery), and the driver Properties box of Device Manager.
- Use Device Manager to enable and disable devices and to update and roll back drivers.
- The hardware components required for a successful boot are the CPU, motherboard, power supply, memory, and a boot device such as a hard drive or CD drive.
- When you first turn on a system, startup BIOS on the motherboard takes control to examine hardware components and find an operating system to load.

- Vista startup is managed by the Windows Boot Manager (BootMgr) and the Windows Boot Loader (WinLoad.exe).
- The Vista Boot Configuration Data (BCD) file contains information about settings that control BootMgr, WinLoad.exe, WinResume.exe, and the Windows Memory Diagnostic program, settings that launch Ntldr for loading a previous OS in a dual-boot configuration, and settings to load a non-Microsoft operating system.
- The Advanced Boot Options menu offers Safe Mode, Safe Mode with networking, Safe Mode with command prompt, enable boot logging, enable low-resolution video (enable VGA mode in Windows XP/2000), Last Known Good Configuration, directory services restore mode, debugging mode, and disable automatic restart on system failure. This last option is not available in Windows 2000.
- Windows Vista Recovery Environment can be started from the Vista setup DVD.
- The boot process for Windows 2000/XP uses files stored in the root directory of the hard drive and the C:\Windows\system32 folder.
- The boot process can be customized with entries in Boot.ini. The Boot.ini file can be edited with a text editor, but it is best to change the file using the System Properties dialog box.
- Tools to use to troubleshoot problems with loading Windows 2000/XP are the Advanced Options menu, the boot disk, and the Recovery Console.
- The Recovery Console is a command interface with a limited number of commands available to troubleshoot a failing Windows 2000/XP load. The console requires that you enter the Administrator password.

>> KEY TERMS

Advanced Options menu
Boot Configuration Data (BCD) file
Boot.ini
Driver Query
Driver Verifier (verifier.exe)
Emergency Repair Disk (ERD)
Emergency Repair Process
File Signature Verification
Last Known Good Configuration
Memory Diagnostics
progress bar
Recovery Console
System File Checker (SFC)
Windows Boot Loader (WinLoad.exe)
Windows Boot Manager (BootMgr)
Windows RE
Windows Vista Recovery Environment (RecEnv.exe)

>> REVIEWING THE BASICS

1. Blue screen errors happen when which type of processes encounter an error?
2. Which Vista tool keeps a record of STOP errors and allows you to view a history of these errors?
3. When you allow Windows XP Error Reporting to send a report to Microsoft of an error, what does Microsoft give in return?
4. What is the command to use the Vista Memory Diagnostics tool?
5. What method can you use to test memory on a Windows XP system by using the Vista Memory Diagnostics tool without having to install Vista on the system?

6. What is the command to use the System File Checker to immediately verify system files? To verify system files on the next restart?
7. Why might it not be wise to use the Driver Verifier tool on a computer that serves up files to an office of 10 people?
8. A blue screen error halts the system while it is booting, and the booting starts over in an endless loop of restarts. How can you solve this problem?
9. What three Windows tools can be used to verify that a driver is digitally signed?
10. What does Windows call the process of undoing a driver update?
11. Is the BootMgr file stored in the boot partition or the system partition?
12. Where is the master boot record (MBR) located?
13. What is the name of the Windows Vista boot loader program? Where is the program located?
14. What is the name of the Vista kernel program?
15. What is the name of the program that manages Windows logon?
16. Which registry hive is loaded first during Windows startup?
17. Where does Windows store device driver files?
18. What is the first thing that BIOS checks?
19. Which key do you press to launch the Advanced Boot Options window during Windows startup?
20. What can you assume about the Vista startup when you see the progress bar on-screen?
21. When is the Windows startup process completed?
22. At what point in Windows startup are the settings that are called the Last Known Good Configuration saved?
23. What command in Windows RE can you use to rebuild the BCD file?
24. What command in Windows RE gives you an opportunity to manage partitions and volumes installed on the system?
25. What is the name and path of the log file created by Vista Startup Repair?
26. If you are having a problem with a driver, which of the following is the least invasive solution: update the driver or use System Restore?
27. What tool can you use to stop a program that is hung?
28. If an application works when the system is loaded in Safe Mode, but does not work when Windows is loaded normally, what can you assume?
29. What are the three stages of the Vista startup process?
30. What is the name of the log file and its location that is created when you enabled boot logging from the Advanced Boot Options startup menu?
31. In the Windows 2000/XP boot process, what is the name of the program file that reads and loads the boot menu?
32. Where is the Boot.ini file stored?
33. What two subfolders in the C:\Windows\system32 folder contain files needed for Windows startup?

>>THINKING CRITICALLY

1. When the Windows Vista registry is corrupted and you cannot boot from the hard drive, what tool or method is the best option to fix the problem?.
   a. Boot into Safe Mode and use System Restore to repair the registry.
   b. Use the Last Known Good Configuration on the Advanced Boot Options menu.
   c. Use commands from the Windows Recovery Environment to recover the registry from backup.
   d. Reinstall Windows Vista using the Complete PC Restore process.
2. Your Windows XP system boots to a blue screen and no desktop. What do you do first?
   a. Reinstall Windows XP.
   b. Attempt to boot into the Advanced Options menu.
   c. Attempt to boot into the Recovery Console.
   d. Attempt to use the Automated System Recovery.
3. You have important data on your hard drive that is not backed up and your Windows installation is so corrupted you know that you must repair the entire installation. What do you do first? Why?
   a. Use System Restore.
   b. Make every attempt to recover the data.
   c. Perform an in-place upgrade of Windows Vista.
   d. Reformat the hard drive and reinstall Windows Vista.
4. As a helpdesk technician, list four good detective questions to ask if a user calls to say, "My PC won't boot."
5. Reword the following questions that might be asked when interviewing a user over the telephone. Your new questions should reflect a more positive attitude toward the user.
   a. Did you drop your laptop?
   b. Did you forget to recharge the laptop battery?
   c. You say the problem is that Microsoft Word is giving an error, but do you really know how to use that application?

>> HANDS-ON PROJECTS

PROJECT 15-1: Support for Your Installed Hardware and Software

Do the following to find out what kind of support and replacement parts are available for your computer:

1. Make a list of all the installed hardware components on your computer that are considered field replaceable components needed to boot the system, including the motherboard, processor, power supply, optical drive, hard drive, and memory.

2. Search the Web for the device manufacturer Web pages that show what support is available for the devices, including any diagnostic software, technical support, and device driver updates.
3. Print a Web page showing a replacement part for each device that fits your system. If possible, show the exact match for a replacement part.
4. Make a list of all installed applications on your computer.
5. For each application, print a Web page showing the support available on the software manufacturer's Web site for the application.

PROJECT 15-2: Practicing Solving Boot Problems

This project is best done on a lab computer rather than your personal computer. Unplug the computer, open the case, and disconnect the data cable to your hard drive. Turn the computer back on and boot the system. What error message did you see? Now reboot using your Windows Vista setup DVD. Try to load the Recovery Environment. What error messages did you receive, if any? Power down your computer, unplug it, and reconnect your hard drive. Reboot and verify that Windows Vista loads successfully.

PROJECT 15-3: Practicing Using the Recovery Environment

Boot from the Vista DVD and launch the Recovery Environment. Then do the following:

1. Execute the Startup Repair Process. What were the results?
2. Execute System Restore. What is the most recent restore point? (Do not apply the restore point.)
3. Using the command prompt window, open the Registry Editor. What command did you use? Close the editor.
4. Using the command prompt window, copy a file from your Documents folder to a flash drive. Were you able to copy the file successfully? If not, what error message(s) did you receive?

PROJECT 15-4: Using Ntbtlog.txt

Compare an Ntbtlog.txt file created during a normal boot to one created when booting into Safe Mode. Note any differences you find.

PROJECT 15-5: More Practice with Windows RE

Using Windows Explorer, rename the BootMgr file in the root directory of drive C. Reboot the system. What error message do you see? Now use Windows RE to restore the BootMgr file. List the steps taken to complete the repair.

PROJECT 15-6: Problem-Solving Using the Microsoft Knowledge Base

You are trying to clean up a hard drive to free some disk space. You notice the hard drive has a C:\Windows.Old folder that uses 10 GB. However, in the Disk Cleanup dialog box, you don't see the option to delete Previous Windows Installations. Using the Microsoft support site (*support.microsoft.com*), find the Knowledge Base Article that allows you to manually delete the folder. Answer these questions:

1. What is the Article ID for this article?
2. What are the three command lines needed to delete the folder?
3. Explain the purpose of each of the three commands, and explain the purpose of each parameter in the command line.

PROJECT 15-7: Using Boot Logs and System Information to Research Startup

Boot logs can be used to generate a list of drivers that were loaded during a normal startup and during the Safe Mode startup. By comparing the two lists, you can determine which drivers are not essential to startup. Also, the System Information utility (msinfo32.exe) can help you find out information about a driver or service. Do the following to research startup:

1. To turn on boot logging, boot to the Advanced Boot Options menu and choose Enable Boot Logging. Then boot to the normal Windows desktop. Print the file C:\Windows\ntbtlog.txt and save the file to a different location on the hard drive.
2. Reboot the system in Safe Mode. Print the file C:\Windows\ntbtlog.txt and save the file to a different location on the hard drive. Using the two lists, identify the drivers that were loaded normally but not loaded during Safe Mode.
3. The next step is to identify each hardware component that uses the device drivers you identified in Step 2. These are the drivers that were loaded normally, but not loaded during Safe Mode. Use the System Information utility (msinfo32.exe) to drill down to each hardware component or use the search feature at the bottom of the System Information window. When you find the hardware component, look for the device drivers that are associated with the component.

As you identify the drivers not loaded during Safe Mode, it might be helpful to know that these registry keys list the drivers and services that are loaded during Safe Mode:

- Lists drivers and services loaded during Safe Mode:
  HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal
- Lists drivers and services loaded during Safe Mode with Networking:
  HKLM\System\CurrentControlSet\Control\SafeBoot\Network

PROJECT 15-8: Researching Software to Compare Text Files

Comparing boot log files manually can be tedious work, and a utility that compares text files looking for differences can be a great help. Finding the best utility can, however, be a challenge. Vista offers the Comp command, and Windows XP support tools include Windiff.exe. Alternately, you can find and download another file comparison program from the Internet. Do the following to research file comparison programs:

1. In a command prompt window, use the Vista Comp command to compare the two log files you saved in Project 15-7.

2. Locate a file comparison program on the Internet, copy it to your Vista computer, and install it. Be sure to verify that the site you are using is reliable before you download a file from it—you don't want to download malware to your PC. Use the program to compare the two log files.
3. If you have access to a Windows XP computer that has the system tools installed, copy the Windiff.exe program to your Vista computer and use it to compare the two log files.
4. Which file comparison program do you like best? Why?

>> REAL PROBLEMS, REAL SOLUTIONS

REAL PROBLEM 15-1: Finding an Unknown Device (Challenging Real Problem)

Someone has come to you for help with their computer. They are unable to connect to the Internet and are not sure why. After some investigation, you realize that they have just replaced the network adapter, but have lost the driver CD for the adapter and its documentation. Windows does not recognize the device type and there is no model information on the device itself. To find the correct drivers, you need to know the exact brand and model of the device. Use the following steps to retrieve this information. By following these steps, you'll learn to use the Ultimate Boot CD, which can be a valuable utility to add to your PC repair kit.

1. Go to the Ultimate Boot CD download page at *www.ultimatebootcd.com/download.html* and read the directions about creating the Ultimate Boot CD. The CD is created using an ISO image. An ISO image is a file that contains all the files that were burned to an original CD or DVD. This ISO image is then used to create copies of the original CD or DVD. The process has three steps: (1) Download the ISO image as a compressed, self-extracting .exe file, (2) Decompress the compressed file to extract the ISO file having an .iso file extension, (3) Use CD burning software to burn the CD from the ISO image.
2. Now that you understand the process, follow directions to download to your hard drive a compressed and self-extracting executable (.exe) file containing the ISO image. The current version of the Ultimate Boot CD as of the printing of this book is Version 4.1.1 and the file to download is ubcd411.exe.
3. Double-click the downloaded file to execute it and extract the ISO image. (For Version 4.1.1, the new file will be named ubcd411.iso.)
4. You'll need software to burn the ISO image to the CD. (Do not just burn the .iso file to the CD. The software extracts the files inside the ISO image and burns these files to the CD to create a bootable CD holding many files.) The Ultimate Boot CD Web site suggests some free CD burning software that supports ISO images. Download and execute one of these products to burn the ISO image to the CD. Using a permanent marker, label the CD "Ultimate Boot CD" and include the version number that you downloaded.
5. Boot the computer from the CD and find a tool that will retrieve the brand and model number of the NIC (network adapter). What software on the CD did you decide to use?
6. Use the program to find the make and model number of the NIC installed in your system and write down this information.
7. Using the acquired information, search the Internet for the correct driver.

8. Does this driver match the driver installed on your system?

9. Answer the following questions about other programs on the Ultimate Boot CD:

   a. Some antivirus software reports that some programs on the Ultimate Boot CD are viruses. Search the Ultimate Boot CD Web site for the name of one of these programs. What is its name and what is the purpose of the program? Is the program truly a virus?

   b. Name one other program on the Ultimate Boot CD that you believe will be useful when troubleshooting. Describe what the program does.

This page intentionally left blank