CHAPTER 17

Troubleshooting Windows Operating Systems

One of the most valuable skills you'll need as a PC technician is the ability to troubleshoot Windows. You need to be able to look at the symptoms, identify the problem, and take steps to get Windows fully operational as quickly as possible. Some problems can be resolved quickly and easily by simply rebooting the system. Other problems can also be quickly resolved if you know what steps to take. This chapter includes many steps that you can use when troubleshooting a system and describes many of the common symptoms that require you to use those steps.

Exam 220-802 objectives in this chapter:

- 1.3 Given a scenario, use appropriate command line tools.
  - Recovery console
    - Fixboot
    - Fixmbr
- 1.4 Given a scenario, use appropriate operating system features and tools.
  - Administrative
    - Windows memory diagnostics
- 1.7 Perform preventive maintenance procedures using appropriate tools.
  - Common symptoms
    - Failure to boot
    - Drive not recognized
    - OS not found
  - Tools
    - Recovery image
- 4.3 Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools.
  - Tools
    - File recovery software

- 4.6 Given a scenario, troubleshoot operating system problems with appropriate tools.
  - Common symptoms
    - BSOD
    - Failure to boot
    - Improper shutdown
    - Spontaneous shutdown/restart
    - Device fails to start
    - Missing dll message
    - Services fails to start
    - Compatibility error
    - Slow system performance
    - Boots to safe mode
    - File fails to open
    - Missing NTLDR
    - Missing Boot.ini
    - Missing operating system
    - Missing Graphical Interface
    - Graphical Interface fails to load
    - Invalid boot disk
  - Tools
    - Fixboot
    - Recovery console
    - Fixmbr
    - Sfc
    - Repair disks
    - Pre-installation environments
    - MSCONFIG
    - DEFRAG
    - REGSVR32
    - REGEDIT
    - Event viewer
    - Safe mode
    - Command prompt
    - Emergency repair disk
    - Automated system recovery

- 4.7 Given a scenario, troubleshoot common security issues with appropriate tools and best practices.
    - Recovery console
    - Event Viewer

Understanding the Boot Process

When a computer starts, it goes through several stages before the Windows logon screen appears. If you understand these stages, you have a better chance of understanding the errors you'll see if any of these stages fail. The following sections describe these steps, including the differences between operating systems.

It's also worth repeating a common troubleshooting step mentioned in Chapter 10, "Working with Customers." Rebooting a system solves many ills, so it's common to try a reboot first. If the problem remains after rebooting, you need to take further steps to troubleshoot it.

Power On Self-Test (POST)

The computer loads information from Basic Input/Output System (BIOS) and completes basic hardware checks on the CPU, RAM, keyboard, and video. If this check fails, use the POST beep codes and displayed errors to identify the faulty hardware.

When POST completes successfully, it starts the bootstrap loader. Computers can boot from different devices, such as a hard drive, an optical disc, or a USB flash drive. The bootstrap loader is the last part of the BIOS programming that identifies where to look for a bootable operating system.

MORE INFO **CHAPTER 2, "UNDERSTANDING MOTHERBOARDS AND BIOS"**

Chapter 2 covers the BIOS and POST in more depth. The BIOS is a firmware program and allows you to configure the boot order of a computer.

Look For Master Boot Record and Boot Sector

The bootstrap loader looks for bootable media by using the boot order in the BIOS. When booting from a hard drive, it looks for a *master boot record (MBR)* and passes control to the MBR. Every MBR-based hard drive has a single MBR, and every partition on the hard drive has a single *boot sector*.

Figure 17-1 shows a single hard drive with three partitions. You might remember from Chapter 16, "Understanding Disks and File Systems," that a hard drive can have up to four primary partitions, with one partition marked as active. The active partition includes code within the boot sector that identifies the location of files used to start the operating system.

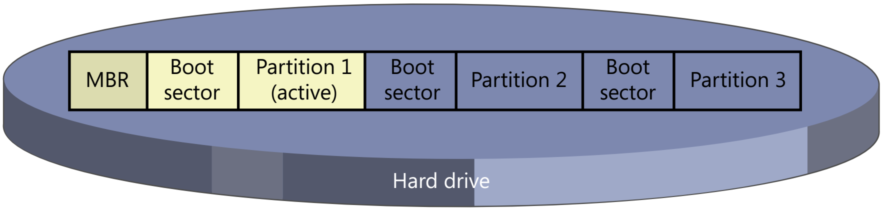


FIGURE 17-1 MBR and boot sectors on a hard disk.

The following steps show the boot process from a hard drive:

1. BIOS loads the master boot code from the MBR into memory.
2. The master boot code scans the partition table on the disk, looking for the active partition.
3. The contents of the active partition's boot sector are loaded into memory by the master boot code.
   - A. On Windows XP, the NTLDR file is loaded.
   - B. On Windows Vista and Windows 7, the boot manager (bootmgr) is loaded.

NOTE **ONLY HARD DISKS HAVE A MBR**

Bootable media other than hard disks have a boot sector but do not have an MBR. For example, a floppy disk has only one partition, so it doesn't need an MBR to locate an active partition. Globally Unique Identifier (GUID) Partition Table (GPT)–based disks are supported on Windows Vista and Windows 7 for systems that use an Extensible Firmware Interface (EFI) instead of a traditional BIOS. The EFI includes an entry to start the bootmgr directly, without looking for an MBR.

Load System Boot Files on Windows XP

On Windows XP, the system boot files are located at the root of the active partition, which is typically C. They are hidden system files, so you won't see them by default. Following is a description of what each file does:

- **NTLDR.** This is a small program that loads the Windows operating system based on the contents of the Boot.ini file.
- **Boot.ini.** This text file identifies the disk, partition, and folder where Windows is located. On multiboot systems, it includes locations of different operating systems and specifies a default operating system.
- **Ntdetect.com.** NTLDR starts this to detect system hardware.

When NTLDR completes the initial load, it runs the ntoskrnl.exe program from the \Windows\System32 folder. This starts Windows XP.

Load Boot Manager on Windows Vista and Windows 7

You might remember from Chapter 12, "Installing and Updating Windows Operating Systems," that Windows Vista and Windows 7 usually create a 100-MB system partition when they are installed. This provides space for BitLocker to be enabled, includes the Windows Recovery Environment (RE), and is also used for system boot files.

The following system boot files are used on Windows Vista and Windows 7:

- **Boot manager (bootmgr) file.** This is a hidden system file located at the root of the system partition.
- **Boot configuration data (BCD).** The BCD is used instead of the Boot.ini file to identify the location of the operating system. On multiboot systems, it includes information for additional operating systems and a default operating system. It is located in the \boot folder of the system partition.

When the bootmgr completes the initial load, it runs Winload.exe from the \Windows \System32 folder. This starts Windows.

EXAM TIP

NTLDR, Ntdetect.com, Boot.ini, and Ntoskrnl.exe files are used only on Windows XP. On Windows Vista and Windows 7, bootmgr, BCD, and Winload.exe are used instead.

Understanding the Registry

The *registry* is a database used by Windows-based systems to store information about the computer's hardware, installed programs, system settings, and user profiles. When you make changes in Control Panel applets or through programs, these changes are often recorded in the registry and accessed by Windows.

Starting the Registry Editor

You can start the registry Editor with the *regedit* or *regedt32* command. In earlier operating systems, these two commands started different programs, but they both start the same registry editor in Windows XP, Windows Vista, and Windows 7.

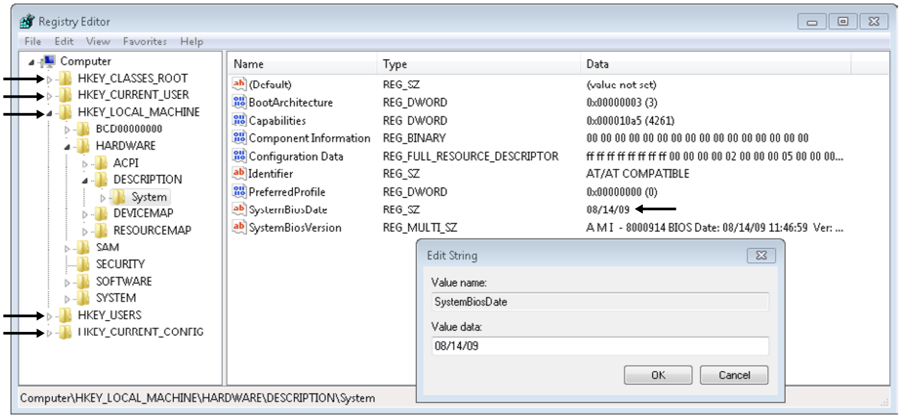
On Windows XP, run the command from the command prompt or the Run line. On Windows Vista or Windows 7, run the command from the command prompt or from the Start, Search text box.

Hives, Keys, and Values

The registry is organized in five groups called *hives*. Each group includes settings called keys and values. The five hives are as follows:

- **HKEY_LOCAL_MACHINE (HKLM).** Settings that apply to the local computer are stored here.
- **HKEY_USERS (HKU).** These settings apply to all users.
- **HKEY_CURRENT_USER (HKCU).** These settings apply only to the user who is currently logged on.
- **HKEY_CURRENT_CONFIG (HKCC).** When the computer starts, it identifies and stores the current configuration here.
- **HKEY_CLASSES_ROOT (HKCR).** Data used by different software applications are stored here. For example, it includes file associations that associate specific file extensions with applications.

You can expand the hives to view the individual keys and subkeys. For example, Figure 17-2 shows the registry editor opened to a specific subkey. The five hives are in the left pane, with the HKEY_LOCAL_MACHINE hive expanded. You can double-click any value to open it, as shown with the SystemBIOSDate value and its data.



Name	Type	Data
(Default)	REG_SZ	(value not set)
BootArchitecture	REG_DWORD	0x00000003 (3)
Capabilities	REG DWORD	0x000010a5 (4261)
Component Information	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Configuration Data	REG_FULL_RESOURCE_DESCRIPTOR	ff ff ff ff ff ff ff ff 00 00 00 00 02 00 00 00 05 00 00 00...
Identifier	REG_SZ	AT/AT COMPATIBLE
PreferredProfile	REG_DWORD	0x00000000 (0)
SystemBiosDate	REG_SZ	08/14/09
SystemBiosVersion	REG_MULTI_SZ	A M I - 8000914 BIOS Date: 08/14/09 11:46:59 Ver: ...

Value name: SystemBiosDate

Value data: 08/14/09

Computer\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System

FIGURE 17-2 Viewing the registry editor.

This figure illustrates the differences between the hives, keys, and values, but you probably realize there are easier ways to identify the date of the BIOS. For example, using the msinfo32 command to start System Information shows this information in a more readable format.

If you want to look for a specific key or value, you can use the Find feature available in the Edit drop-down menu. First, select Computer to search the entire registry, or select a specific hive or key. Next, select Edit, Find, and enter your search term.

NOTE **REGISTRY CLEANERS RARELY NEEDED**

Registry cleaners are often advertised for free on the Internet but are sometimes malicious software (malware). Some are rogueware that trick users into installing it for free and then paying extra to fix nonexistent problems. Chapter 26, "Recognizing Malware and Other Threats," covers rogueware.

Back Up the Registry

You normally won't need to modify the registry directly, but as you advance in your IT career, you might encounter situations when it's necessary. It's important to realize that corruption in Windows can occur with an incorrect change, which can cause a system not to start. If you need to modify the registry back it up first and take your time when making the change.

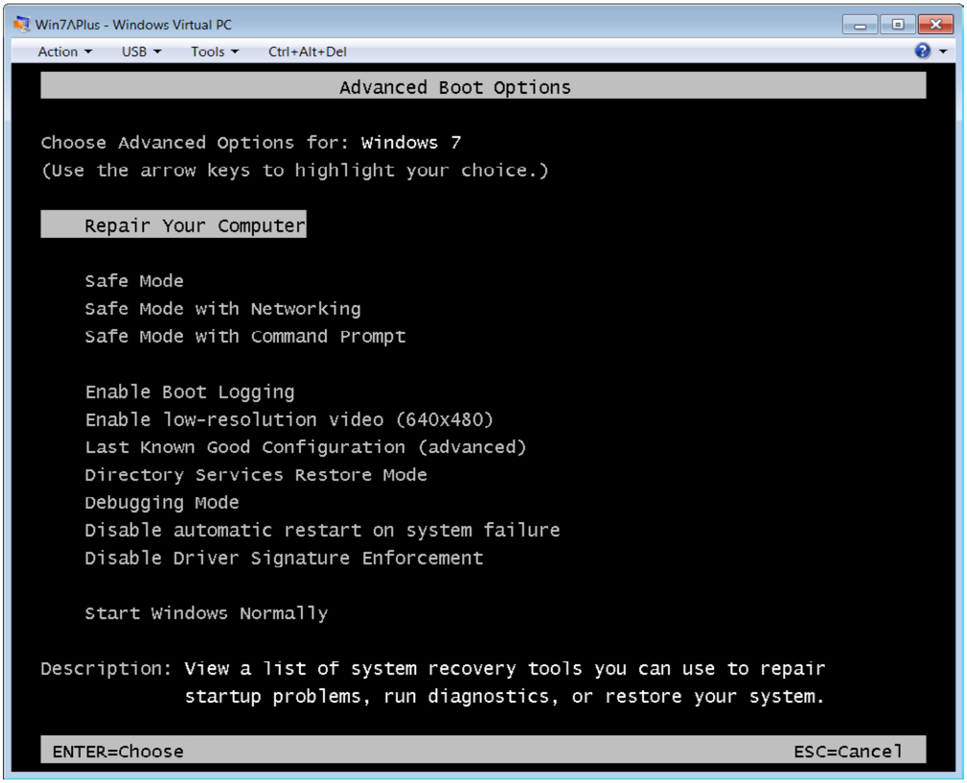
You can use the following steps on Windows XP, Windows Vista, and Windows 7 to back up the registry:

1. Log on to the system by using an account with administrative privileges.
2. Start the registry editor with the regedit or regedt32 command from a command prompt or the Start, Search text box.
3. Right-click Computer and select Export.
4. Browse to the location where you want to store the backup, and type in a name for the backup. For example, you might choose to create a folder named RegBackup on the C drive and name the backup RegComputer. Click Save.
5. You can also back up any portion of the registry. For example, right-click HKEY_LOCAL_MACHINE and select Export.
6. Browse to the location where you want to store the backup, and type in a name for the backup. For example, you might choose to name the backup HKLM_Backup. Click Save.

Advanced Boot Options

Ideally, each time you start Windows, everything will work as planned and you'll be pointing and clicking in no time. Unfortunately, sometimes things go wrong. Windows has several troubleshooting tools available. Many of these tools are started from the Advanced Boot Options menu.

You can access the Advanced Boot Options page by pressing F8 during the boot process. Figure 17-3 shows what this looks like on a Windows 7–based system.



```
                         Advanced Boot Options

Choose Advanced Options for: Windows 7
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    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: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.

 ENTER=Choose                                                  ESC=Cancel
```

FIGURE 17-3 Access Advanced Boot Options page after pressing F8.

NOTE **TAP F8 REPEATEDLY**

Windows monitors the F8 key after BIOS finishes POST. If you aren't pressing the key, the system will boot into Windows and you'll have to restart to try again. There's nothing wrong with tapping the F8 key repeatedly as the computer starts. The worst that can happen is a Keyboard Error if POST interprets your tapping as a stuck key on the keyboard.

The following sections describe the options available from this menu. The options are the same on Windows Vista and Windows 7, but the following menu options do not appear on the Windows XP menu:

- Repair Your Computer
- Disable Automatic Restart On System Failure
- Disable Driver Signature Enforcement

EXAM TIP

You can access the Advanced Boot Options page by pressing F8 as the system boots. It provides access to the Windows Recovery Environment with Repair Your Computer, safe modes, and the Last Known Good Configuration.

Safe Modes

Occasionally, a change to Windows prevents it from starting normally. For example, after installing a hardware driver or updating software, the system might not be able to reboot successfully. You can use one of the safe modes to start Windows with only the basics and avoid loading the faulty driver or software.

There are three different versions of safe mode, as follows:

- **Safe mode.** This is the most basic version.
- **Safe mode with networking.** This mode includes network drivers and services needed to access network resources. Use it if you need to access the Internet from safe mode to download updates or other files.
- **Safe mode with command prompt.** Instead of the normal graphical user interface (GUI) used in Windows, it loads only the command prompt.

NOTE **SAFE MODE HAS A BLACK DESKTOP**

You'll know when you're booted into safe mode because the screen will be black and the words "safe mode" will be in white letters at the four corners of the display.

You can perform most recovery options within safe mode just like during normal operations. These functions include the following:

- Applying restore points by using System Restore.
- Rolling back drivers by using Device Manager.
- Restoring an image by using System Image Recovery, if a system image is available.

MORE INFO **CHAPTER 15, "CONFIGURING WINDOWS OPERATING SYSTEMS"**

Chapter 15 covers System Restore, restore points, Device Manager, and image backups.

Enable Boot Logging

If a system has a corrupted driver or service, it might prevent Windows from starting. You'll see Windows start, but before it finishes, it restarts. One method of identifying the problem is to enable boot logging from the Advanced Boot Options menu. When enabled, it logs activity from the startup process into a file named Ntbtlog.txt, located in the C:\Windows folder.

After enabling boot logging, try to start the system again. It will record the steps in the log, up to where Windows fails. After it fails, press F8 to access the Advanced Boot Options menu and select safe mode. It will append this log with the steps used to boot into safe mode, starting with a time stamp. You can view the log by using one of the following methods:

- Browse to C:\Windows and double-click the Ntbtlog.txt file.
- Open a command prompt and enter the following command:

  ```
  notepad c:\windows\ntbtlog.txt
  ```

Sometimes the problem is related to something that loaded in the regular boot cycle but did not load in safe mode. Look for entries towards the end of the regular boot cycle starting with "Loaded driver" but listed as "Did not load driver" in the safe mode cycle. One of these drivers is likely the reason why Windows is failing.

Enable Low-Resolution Video

This can be useful if the current video driver is configured incorrectly. Imagine the following scenario. You just changed the display settings and clicked Keep Changes to confirm that you want to make the changes permanent. Suddenly, the video card blanks out because it can no longer display the video with these changes.

The solution is to reconfigure the Display settings, but you can't see the screen to access them. If you boot into safe mode, it uses the basic video driver and you wouldn't be able to modify the settings for the regular video driver, so safe mode won't help.

If you select Enable Low-Resolution Video and restart, it will use the current video driver but with the most basic settings. You can then modify the settings and restart the system.

> ***NOTE*** **ENABLE VGA MODE IN WINDOWS XP**
>
> **The Enable Low-Resolution Video menu choice is named Enable VGA Mode in the Windows XP Advanced Boot Options menu but works the same as Enable Low-Resolution Video.**

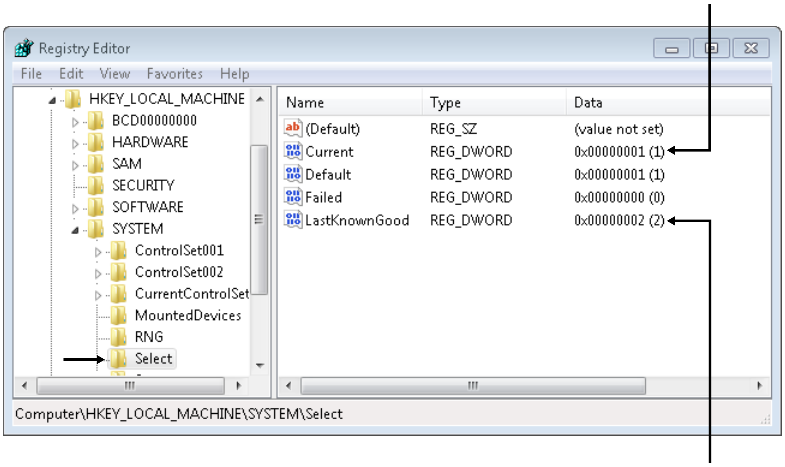
Last Known Good Configuration

The Last Known Good Configuration choice is a valuable option that allows you to easily revert changes from a previously logged on session. It's easier to understand how the last known good configuration can help you if you first understand how Windows records system settings.

Control Sets in the Registry

Windows considers a boot successful when a user logs on. Immediately after a user logs on, it copies the machine's system settings into an area of the registry known as a control set. Figure 17-4 shows the different control sets available in a Windows 7–based system.

Booted using ControlSet001



HKEY_LOCAL_MACHINE
- BCD00000000
- HARDWARE
- SAM
- SECURITY
- SOFTWARE
- SYSTEM
  - ControlSet001
  - ControlSet002
  - CurrentControlSet
  - MountedDevices
  - RNG
  - Select

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

ControlSet002 labeled LastKnownGood

FIGURE 17-4 Viewing control sets in the registry.

The system is started by using the settings from ControlSet001. Immediately after the user logs on, it copies these settings to ControlSet002 and labels ControlSet002 as LastKnownGood. While the user is logged on, system changes are applied to ControlSet001 but the known good settings in ControlSet002 are retained.

Using Last Known Good Configuration

Imagine that a user updated a graphics card driver and restarted the system. When the system starts, the graphics card driver is loaded and it crashes the system. Because the system can't start, the user hasn't logged on and the last known good settings are retained.

You can restart the system and press F8 to access the Advanced Boot Options menu. From this menu, select Last Known Good Configuration. This will restore the settings prior to the addition of the new graphics driver, and the system can now start.

EXAM TIP

The most important point to remember about using Last Known Good Configuration is that it can be used only before a user has logged on. If a user logs on again after making a change, the system creates a new last known good configuration that includes the change.

What if you were able to log on but you were having problems because of a recently updated driver? How could you resolve this problem? You can't use Last Known Good Configuration, but you can boot into safe mode and use Device Manager to roll back the driver. Chapter 15 covers the Device Manager and shows how to do this.

Disable Driver Signature Enforcement

Windows Vista and Windows 7 require drivers to be digitally signed by default. A digital signature provides assurances of who published the driver and that the driver has not been modified.

If you need to bypass this requirement, you can select this option and restart the system. A primary reason that you might choose this option is if you are testing new drivers before they have been finalized.

Disable Automatic Restart on System Failure

You can use this setting if the Windows system is stuck in a restart loop where it fails to start, tries to restart, and fails again over and over. When Windows fails, it will display a stop error on a blue screen, but you might not have time to read it before the system restarts again. If you use this setting, you'll have time to read the error information from the stop error.

Other Advanced Boot Options

The following options on the Advanced Boot Options page are rarely used:

- **Directory Services Restore Mode.** You use this only on Windows Servers that are configured as domain controllers. They run Active Directory Domain Services, but a Windows 7–based system cannot be a domain controller.
- **Debugging Mode.** This is an advanced troubleshooting mode used to troubleshoot advanced software problems.

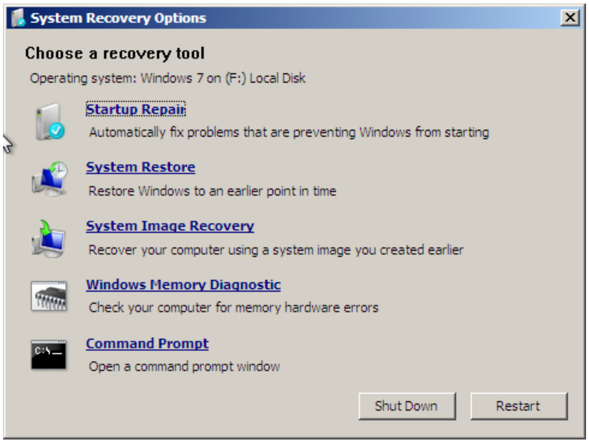
Repair Your Computer

The Repair Your Computer option starts the *Windows Recovery Environment (Windows RE)* and provides you with a list of additional tools you can use to troubleshoot and repair problems. This is especially useful if you find that you can't boot into safe mode.

NOTE **WINDOWS RE FROM WINDOWS INSTALLATION DVD**

The Repair Your Computer option is available only if the tools were installed on your hard disk. By default, these are included in Windows 7 installations but not Windows Vista installations. You can access the same tools from many Windows installation DVDs: boot to the DVD, and select Repair Your Computer. You can also create a system repair disc by using steps later in this chapter to boot directly into the Windows RE from a CD or DVD.

When you select this option, you'll be prompted to select a keyboard language and then you'll need to log on with a local account. If you use an administrative account, the options will include the command prompt, as shown in Figure 17-5.



Choose a recovery tool

Operating system: Windows 7 on (F:) Local Disk

Startup Repair
Automatically fix problems that are preventing Windows from starting

System Restore
Restore Windows to an earlier point in time

System Image Recovery
Recover your computer using a system image you created earlier

Windows Memory Diagnostic
Check your computer for memory hardware errors

Command Prompt
Open a command prompt window

FIGURE 17-5 Using System Recovery Options.

- **Startup Repair.** This option runs a series of checks and attempts to repair problems automatically. If your system is a multiboot system, you'll need to select the operating system you want to repair. It will prompt you for confirmation before it tries to fix problems.
- **System Restore.** This option allows you to apply a restore point, similarly to how you can apply a restore point from within Windows or within safe mode.
- **System Image Recovery.** If you have created a system image, you can use this to restore it. This menu item is called Windows Complete PC Restore on Windows Vista-based systems.
- **Windows Memory Diagnostic.** Use this option to run thorough checks of the random access memory (RAM). It will open the same diagnostic tool that you can start from within Windows.

MORE INFO **CHAPTER 3, "UNDERSTANDING RAM AND CPUS"**

Chapter 3 covers the Windows Memory Diagnostic tool. The Event Viewer section in this chapter shows how to view the results of the Windows Memory Diagnostic in the System log.

- **Command Prompt.** This provides access to a Windows RE Command Prompt. It includes commands such as bootrec and bcdedit, but it doesn't include all normal command prompt commands.

EXAM TIP

The System Repair option will resolve the majority of problems on Windows Vista and Windows 7 with very little user interaction. Other problems affecting the MBR, boot sector, or BCD can be repaired by using the Windows RE Command Prompt.

Recovery Console and Windows RE Command Prompt

The *recovery console* is available in Windows XP and is used to run commands that can repair problems with the MBR, boot sector, and Boot.ini files. It's replaced by the Windows RE Command Prompt in Windows Vista and Windows 7. This section shows how to install and use the recovery console in Windows XP.

Install the Recovery Console in Windows XP

The recovery console is not available by default in Windows XP, but you can install it with the following steps:

1. Boot into Windows XP.
2. Insert the Windows XP installation CD into an optical drive, and identify the drive letter assigned to the drive.
3. Start a command prompt, and enter the following command using the drive letter assigned to the CD. The example assumes the letter D was assigned.

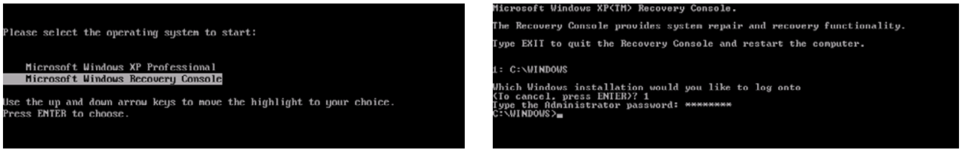
   ```
   d:\i386\winnt32.exe /cmdcons
   ```

4. You'll see a dialog box asking whether you want to install the recovery console. Click Yes.
5. When the installation completes, click OK.

When you restart the system, you'll see Microsoft Windows Recovery Console listed as another boot option. You can select it just as you'd select any operating system in a dual-boot system.

Using the Recovery Console on Windows XP

When you start a system with the Recovery Console installed, it shows a multiboot menu similar to the screen on the left in Figure 17-6. You can also start the recovery console from the installation CD. Boot to the CD and press R when the Welcome screen appears.



```
Please select the operating system to start:


    Microsoft Windows XP Professional
    Microsoft Windows Recovery Console

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

```
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 17-6 Starting the Recovery Console.

The system searches the computer, looking for operating systems, and will prompt you to select the operating system you want to repair. You'll then be prompted to enter the administrator's password for this operating system. You'll end up with a blinking cursor after C:\WINDOWS>, similar to the screen to the left in Figure 17-6, waiting for you to enter a command.

You should understand the following three important commands:

- **fixboot**—Writes a new boot sector on the system partition
- **fixmbr**—Repairs the master boot record (MBR)
- **bootcfg /rebuild**—Rebuilds the Boot.ini file

NOTE **RECOVERY CONSOLE IS DIFFERENT FROM THE COMMAND PROMPT**

The Recovery Console prompt looks similar to the command prompt window, but it's not the same. You can enter the help command to get a list of all supported commands, or you can use the *command* /? format to get help with individual commands.

Bootrec Commands on Windows Vista and Windows 7

The Windows XP Recovery Console and its commands are not available on Windows Vista or Windows 7. However, you can access similar commands from the System Recovery Options command prompt. The most important command for recovery is the *bootrec* (boot recovery) command.

You can execute bootrec with the following key switches:

- **bootrec /fixmbr.** This repairs the MBR.
- **bootrec /fixboot.** This writes a new boot sector onto the system partition. It is useful if an earlier version has been installed after installing Windows Vista or Windows 7. For example, if you install Windows XP after installing Windows 7, it corrupts the Windows 7 boot sector, but this command repairs it.
- **bootrec /rebuildbcd.** This rebuilds the BCD file on the computer. It forces a full scan of disks to locate bootable operating systems and re-creates the BCD file similarly to how bootcfg /rebuild re-creates the Boot.ini file on Windows XP.
- **bootrec /scanos**. This scans a system, looking for operating systems on the computer.

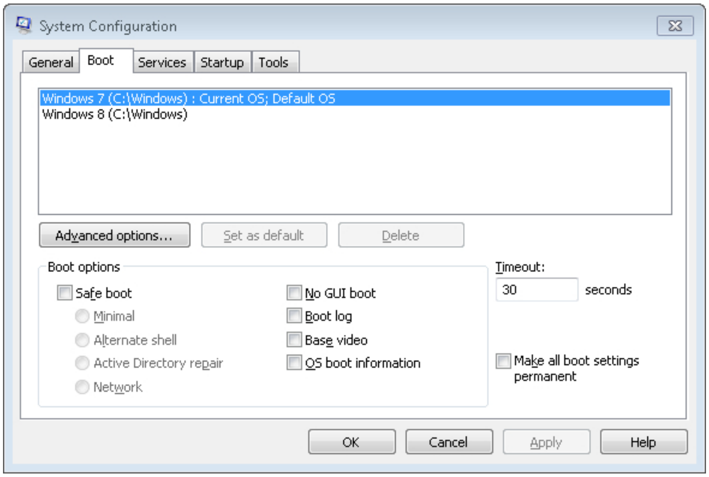
EXAM TIP

The fixboot and fixmbr commands are useful if a virus has damaged the MBR or boot sector on a Windows XP-based system. The bootrec /fixboot and bootrec/ fixmbr commands can repair similar problems on Windows Vista-based and Windows 7–based systems.

Msconfig and Advanced Boot Options

The System Configuration (covered in Chapter 15) is a valuable tool that you can use to identify and troubleshoot problems. It is commonly started with the msconfig command and can also be accessed from the Administrative Tools menu in the Control Panel.

Figure 17-7 shows System Configuration open with the Boot tab selected. You can use this tab to force a system to boot into one of the safe modes without accessing the Advanced Boot Options menu.



Windows 7 (C:\Windows) : Current OS; Default OS
Windows 8 (C:\Windows)

Boot options

□ Safe boot
○ Minimal
○ Alternate shell
○ Active Directory repair
○ Network

□ No GUI boot
□ Boot log
□ Base video
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

FIGURE 17-7 Accessing safe mode options from msconfig.

EXAM TIP

If you use msconfig to boot into one of the safe modes, the system will continue to boot into that safe mode until the setting is changed back. In contrast, if you use F8 and Advanced Boot Options to select a safe mode, it will start normally when you restart the system.

Most of the following selections in the Boot Options area of the Boot tab directly relate to menu items in the Advanced Boot Options menu:

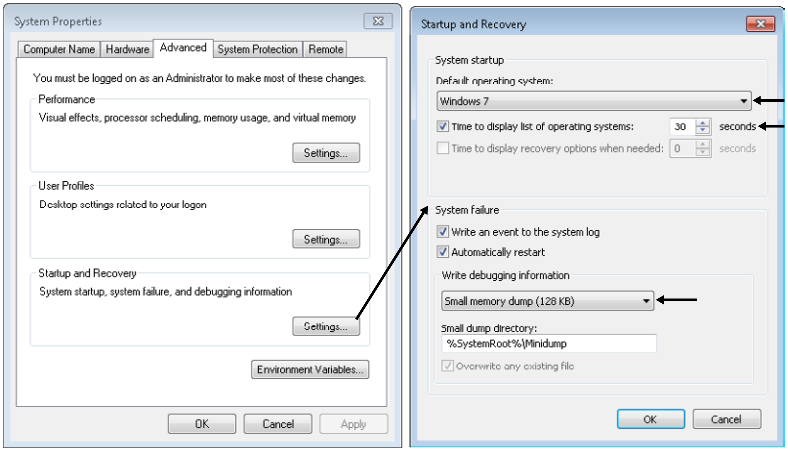
- Safe Boot Minimal is the same as Safe Mode.
- Safe Boot Alternate Shell is the same as Safe Mode With Command Prompt.
- Safe Boot Active Directory Repair is the same as Directory Services Restore Mode.
- Safe Boot Network is the same as Safe Mode With Networking.
- No GUI Boot starts Windows without displaying the Windows Welcome screen. This option is not available from the Advanced Boot Options menu.
- Boot Log is the same as Enable Boot Logging.
- Base Video is the same as Enable Low-Resolution Video.

- OS Boot Information displays driver names as they are being loaded during the startup process. It shows the same information that is logged in the Ntbtlog.txt file if Boot Log or Enable Boot Logging is selected.

Startup and Recovery Options

You can manipulate some startup and recovery settings by using the advanced options available from the System applet. These settings allow you to manipulate how a system boots and to change the default behavior after a system failure.

Figure 17-8 shows the Startup And Recovery page on a Windows 7–based system. The page looks very similar on Windows XP and Windows Vista. Windows 7 is selected as the Default Operating System, and it will boot into Windows 7 after a delay of 30 seconds. If the computer is a multiboot system, you can click the down arrow to the right of Windows 7 and select a different operating system as the default.



You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

Startup and Recovery
System startup, system failure, and debugging information

System startup
Default operating system: Windows 7
☑ Time to display list of operating systems: 30 seconds
☐ Time to display recovery options when needed: 0 seconds

System failure
☑ Write an event to the system log
☑ Automatically restart
Write debugging information
Small memory dump (128 KB)
Small dump directory: %SystemRoot%\Minidump
☑ Overwrite any existing file

FIGURE 17-8 Startup And Recovery Options.

You can access this page by clicking Start, Control Panel, and selecting System. If necessary, change the view in the Control Panel to Classic View or Large icons, depending on the system you're using. On Windows XP, select the Advanced tab. On Windows Vista and Windows 7, select Advanced System Settings. You can then click the Settings button in the Startup And Recovery section.

The System Failure section identifies how Windows responds if Windows encounters a stop failure (also known as a blue screen). By default, it writes an event into the System log and will automatically restart after displaying the error.

It's also configured to write the contents of memory into a file that can be used for advanced troubleshooting. By default, this is set to Kernel Memory Dump, and it will create a large dump file named Memory.dmp. In Figure 17-8, it's changed to Small Memory Dump (256), and it will create a file named Minidump.

The benefit of the Minidump file is that you can read the contents with an advanced utility called Dumpchk.exe. Dumpchk.exe won't work with the large Kernel Memory Dump file, but more advanced forensics tools can read it.

MORE INFO **DUMPCHK AVAILABLE ON MICROSOFT'S TECHNET SITE**

The dumpchk utility is beyond the scope of A+, but if you want to dig into it, you can check out *http://technet.microsoft.com/library/ee424340* for more information.

Startup Options and the Boot.ini File

The Boot.ini text file provides the information needed to locate and start Windows XP. If you modify the Boot Options by using msconfig to force a system to go into safe mode, it modifies the Boot.ini file. Also, if you modify the System Startup settings from the Startup And Recovery page, it modifies the Boot.ini file.

You can also modify the Boot.ini file by using any text editor, such as Notepad, but it is a lot easier to use the GUI tools. Boot.ini is a hidden system file located at the root of the system partition, so you'll need to modify the view to access it. You can also click the Edit button on the Startup And Recovery page for Windows XP.

MORE INFO **CHAPTER 13, "USING WINDOWS OPERATING SYSTEMS"**

The "Folder Options" section in Chapter 13 includes steps you can use to change Windows Explorer views by modifying the Folder Options applet. Microsoft's knowledge base article 289022 includes steps to modify the Boot.ini file and is available at *http://support.microsoft.com/kb/289022*.

Startup Options and Boot Configuration Data

The boot configuration data (BCD) is used instead of the Boot.ini file on Windows Vista and Windows 7, and it is more than a simple text file. However, when you make modifications by using msconfig or the Startup And Recovery options, these changes are written to the BCD similar to how they are written to the Boot.ini file.

You can't access the BCD file with Notepad, but you can modify it with the bcdedit command. The details of the bcdedit command are beyond the scope of the A+ exam, but if you want to dig into it, check out the following page: *http://technet.microsoft.com/library/cc731662*.

The bootrec command and its switches are important for the A+ exam. You should know the key switches of the bootrec command described earlier.

Windows Troubleshooting Tools

The Advanced Boot Options and recovery console tools are effective when a system won't start. However, the system can often start while it still has other problems. The following sections describe some common troubleshooting tools you can use within Windows to resolve these problems.

Event Viewer

Windows regularly logs events into different logs, and you can use the Event Viewer to view them. Event Viewer was significantly enhanced in Windows Vista and Windows 7, but the core functionality available in the Windows XP Event Viewer is the same. For example, you'll find the following three Windows logs in each system:

- **System log.** Contains events logged by the Windows operating system. This includes events when a service is started or stopped or when a driver fails to load. These events are predetermined by the operating system.
- **Application log.** Contains events logged by applications or programs. For example, a third-party antivirus application can log when a virus is discovered or when a virus scan is started or stopped. Application developers choose which events to log.
- **Security log.** Contains security-related events. This includes when someone fails to log on due to an incorrect password or when someone accesses or deletes a file. Administrators choose which events to log.

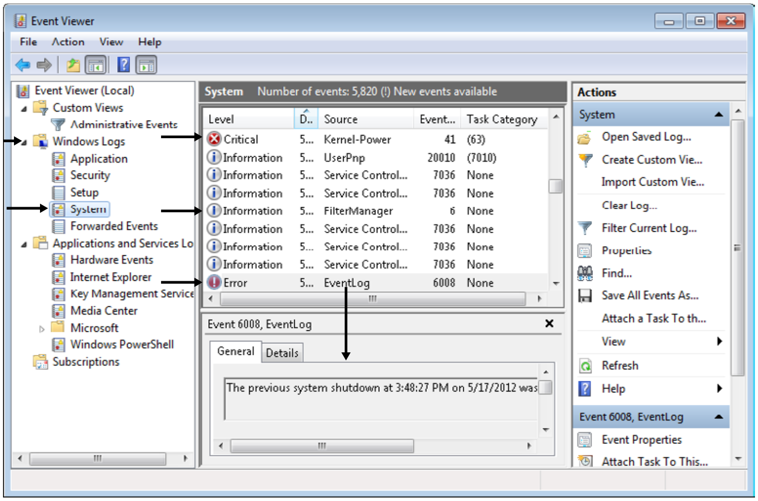
EXAM TIP

Many errors are reported to users via a dialog box or a balloon type message in the bottom-right corner of the screen. If the user reports a message like this but doesn't remember what it says, you can go into the Event Viewer to open the message and get the details.

Starting Event Viewer

You can start the Event Viewer from the Administrative Tools group in the Control Panel or with the eventvwr.msc command. Figure 17-9 shows the Event Viewer in Windows 7 with a few items highlighted. You can see that the Windows Logs are expanded, showing the different logs.

The System log is selected, and the center pane shows the System log events with an error event selected. By default, the events are organized chronologically, but you can reorganize the display with a single click.



System Number of events: 5,820 (!) New events available

Level	D..	Source	Event...	Task Category
Critical	5...	Kernel-Power	41	(63)
Information	5...	UserPnp	20010	(7010)
Information	5...	Service Control...	7036	None
Information	5...	Service Control...	7036	None
Information	5...	FilterManager	6	None
Information	5...	Service Control...	7036	None
Information	5...	Service Control...	7036	None
Information	5...	Service Control...	7036	None
Error	5...	EventLog	6008	None

Event 6008, EventLog

The previous system shutdown at 3:48:27 PM on 5/17/2012 was

FIGURE 17-9 Event Viewer.

For example, if you click the Level heading, it will reorganize the display in alphabetical order, with Critical events first, then Error events, and so on. Click the Level heading again and it organizes them in reverse alphabetical order. Similarly, if you click the Event ID column, it will reorganize the events in Event ID order. This is valuable when you're looking for a specific event.

When you run Windows Memory Diagnostics from the System Recovery Options menu in Windows 7, it runs the diagnostics and then restarts. If you're not sitting in front of the computer when it ends, you won't see the results. However, it logs Event ID 1201 in the System log, with a source of MemoryDiagnostics-Results.

After the system reboots, you can open Event Viewer, select the System log, and find this event. If should be close to the top, but you can click the Event ID column to reorder the display and easily find Event ID 1201.

You can also search for a specific event. With the log selected, click Find on the Action drop-down menu. Enter **1201** or **MemoryDiagnostics-Results** in the text box, and click Find Next.

NOTE **EVENT IDS HAVE CHANGED**

Event IDs have the same number in different operating systems but have different meanings. For example, Event ID 1201 refers to a DNS server configuration issue on Windows Server 2008, but it is used for memory diagnostic results in Windows 7.

Viewing Events in Event Viewer

You can double-click any event to open and see all of the event information. Events are coded with the following error levels so that you can easily identify the serious events:

- **Information** events indicate a change or an activity on the system but do not indicate a problem. They are represented with a small blue *i* within a white circle.
- **Warning** events can impact the operation of the system or result in a more serious problem if action is not taken. They are identified with a black exclamation mark (!) in a yellow triangle.
- **Error** events indicate that a problem has occurred. The problem can impact the functionality of an application or the operating system. They are represented with a white *X* inside a red circle on Windows XP. On Windows Vista and Windows 7, they are represented with a white exclamation mark in a red circle.
- **Critical** events are the most serious and can be seen on Windows Vista-based and Windows 7–based systems. They record failures from an application or the operating system and indicate that the system can't automatically recover from the event. They often result in a stop error or a system reboot. They use a white *X* inside a red circle.
- **Audit** events are recorded in the security log. For example, if someone successfully logs on or fails to log on, the event is logged as a successful audit or a failure audit. These events are identified with a key icon.

Log Properties

Event logs are configured as circular logs by default. That is, they will write data into the log until they reach a maximum size. New events will overwrite older events. You can right-click over any log and select Properties to set the maximum size of the log and select one of the following settings:

- Overwrite Events As Needed (Oldest Events First)
- Archive The Log When Full, Do Not Overwrite Events
- Do Not Overwrite Events (Clear Logs Manually)

EXAM TIP

If the log is configured so that events are not overwritten, it will fill up if it isn't cleared. When full, it will regularly display errors indicating that it is full. You can right-click the log in Event Viewer and select Clear Log to clear it.

Recovery Images

Some Windows tools allow you to create full images of the operating system, all the applications, and the user's data. The following tools are available in Windows:

- Windows Complete PC Backup And Restore, available from the Backup And Restore center on Windows Vista.
- Create A System Image, available from the Backup And Restore applet on Windows 7.

Similarly, there are some third-party tools that provide this capability. If a system fails, you can restore the image and you'll have a fully functioning system with all the applications and the user data up to the moment of the last image save.

This is different than using images to deploy a new installation. A new installation does not include the user's data, but a recovery image from the operating system includes everything. Many computer manufacturers include a recovery partition with the computer. This does not include any data but can be used to restore the system to the state in which it was when the computer was new.

MORE INFO **CHAPTER 15 AND CHAPTER 16**

Chapter 15 shows how to start the backup tools in Windows Vista and Windows 7 and explains the differences between these tools. Chapter 16 discusses recovery partitions.

File Recovery Software

If a computer develops a problem, it's important to consider the user data. If possible, back up the user's data before performing a repair. There are times when you can't easily access the data, but there are some tools available just for this purpose.

For example, if a user accidentally deleted a file, you might be able to restore it from the Recycle Bin. Open the Recycle Bin from the desktop and locate the file. Right-click the file, select Restore, and the file will be restored to the original location.

If the Recycle Bin has been emptied or if the disk is damaged, you might be able to restore data by using third-party recovery tools. Some of these tools are dedicated specifically for file recovery. Other tools are designed for forensic analysis and can often recover more data than regular file recovery tools. Good tools have a cost, but when critical data needs to be recovered, the cost of the tool is minimal.

The best solution is to regularly maintain backups of data. Then, if critical data is lost, it's a simple matter to restore it.

Automated System Recovery

Automated System Recovery (ASR) is a recovery option available in Windows XP. It is intended as a last resort after trying Last Known Good Configuration, rolling back drivers, reverting to previous restore points, and troubleshooting in safe mode.

ASR includes two steps: ASR backup and ASR restore. ASR backup creates a copy of key files, and if you have an ASR backup, you can use ASR restore to recover from a catastrophic failure.

You can create an ASR backup from the Windows XP backup utility. Start Backup by clicking Start, Accessories, System Tools, and selecting Backup. When the Welcome screen appears, click Advanced Mode, and select Automated System Recovery Wizard.

When you create an ASR backup, it backs up operating system files on the system partition along with system information from other partitions that include operating system components. It does not back up user data. The primary backup is large, but ASR backup also creates an ASR floppy disk that holds a small file identifying information on the ASR backup.

If you need to use the backup, ensure that you have the original ASR backup file available, the ASR floppy, and the Windows XP installation CD. Insert the Windows XP installation CD, and reboot the system. When it starts the text mode section of startup, press F2. You'll be prompted to insert the ASR floppy disk, and a wizard will lead you through the process.

MORE INFO **KB ARTICLE 818903 AND MICROSOFT TECHNET**

You can read more about ASR in Microsoft Knowledge Base article 818903 (*http://support.microsoft.com/kb/818903*) and in the Microsoft TechNet article at *http://technet.microsoft.com/library/bb456980*. It isn't used very often on desktop systems due to the amount of work required to keep the backup up-to-date.

Emergency Repair Disk

The CompTIA objectives specifically mention the emergency repair disk (ERD) as an available tool. This was used with Windows 2000 and earlier operating systems for recovery, but Windows XP uses Automated System Recovery instead.

System Repair Disc

An important tool you'll use to repair Windows Vista-based and Windows 7–based systems is the Windows RE. Normally, you would access the Windows RE by selecting Repair Your Computer from the Advanced Boot Options on Windows 7 and Windows Vista, but what do you do if you can't access this menu?

One solution is to create a System Repair disk. This is a bootable CD or DVD that will boot you directly into the Windows RE.

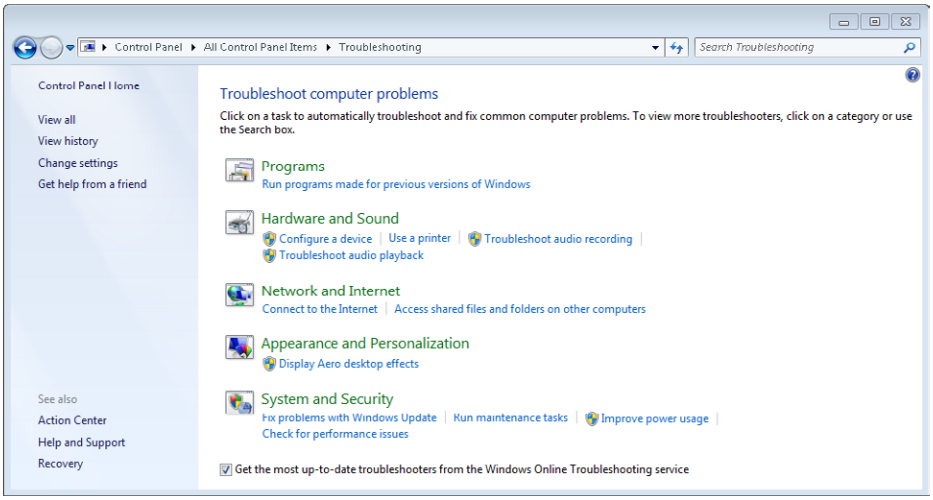
If you have a working Windows 7–based system, you can create it from the Backup And Restore Center in the Control Panel. Insert a blank disc into a CD or DVD burner, and click Create A System Repair Disc. It's a short wizard, and you'll then have a system repair disc that you can use on both Windows Vista-based and Windows 7–based systems.

Another option is to boot using an installation DVD and select Repair Your Computer. This option is available on Windows Vista installation DVDs, but it is not available on all Windows 7 DVDs.

Troubleshooting Applet

The Troubleshooting applet is available in Windows 7–based systems from the Control Panel. You can access it by changing the Control Panel display to Large icons and selecting Troubleshooting.

This applet includes links to several different troubleshooters available in Windows 7, as shown in Figure 17-10. Each troubleshooter is a software wizard that checks for common issues and can often resolve them with little user interaction.



Control Panel ▸ All Control Panel Items ▸ Troubleshooting

Search Troubleshooting

Control Panel Home

View all

View history

Change settings

Get help from a friend

See also

Action Center

Help and Support

Recovery

Troubleshoot computer problems

Click on a task to automatically troubleshoot and fix common computer problems. To view more troubleshooters, click on a category or use the Search box.

Programs

Run programs made for previous versions of Windows

Hardware and Sound

Configure a device | Use a printer | Troubleshoot audio recording | Troubleshoot audio playback

Network and Internet

Connect to the Internet | Access shared files and folders on other computers

Appearance and Personalization

Display Aero desktop effects

System and Security

Fix problems with Windows Update | Run maintenance tasks | Improve power usage | Check for performance issues

☑ Get the most up-to-date troubleshooters from the Windows Online Troubleshooting service

FIGURE 17-10 Troubleshooting applet in Control Panel.

Click any of the links to start the troubleshooter, read the information, and click Next to run it. After a moment, it will usually display a screen indicating that troubleshooting has completed. Occasionally, it will prompt you with information about a problem it has discovered and ask for confirmation to repair it.

The Troubleshooter completion screen includes a View Detailed Information link. If you click it, it opens a report showing all the items that were checked and the results of the check.

Common Symptoms and Their Solutions

This section lists many of the symptoms you might see when troubleshooting Windows. It also includes steps that you can take to resolve many of these common problems.

BSOD

BSOD is short for *blue screen of death,* but the name is much more dramatic than the reality. The computer is not dead. If Windows encounters a critical problem that it can't resolve, it stops and shows a blue screen with the error. If you read the error, you'll get some insight into the problem and be able to resolve it.

Stop errors start with 0x (read as hex or hexadecimal) followed by a string of zeros and a number. For example, the stop error of 0x0000007B (read as hex 7B) includes the text "inaccessible boot device" and indicates a problem with a hard drive.

There are many reasons why you'd get a 7B error, but the important point is that you now have information you can use to troubleshoot the system. An end user might say, "My system crashed," and never read the error. The problem could be due to just about anything.

A knowledgeable PC technician reads the error and investigates from there. For example, you could use Bing.com and search "0x0000007B" or "inaccessible boot device." You might find that a knowledge base article describes your problem perfectly and includes an easy-to-follow solution.

EXAM TIP

Often a stop error is displayed very briefly and then Windows restarts before you can read it. On Windows Vista and Windows 7, you can select the Disable Automatic Restart On System Failure option from the Advanced Boot Options menu to prevent a reboot. The stop error message will remain on the screen until you reboot the system.

Failure to Boot

If you're unable to boot a system, you can use the following task list to help you repair it:

- **Restart.** Sometimes the failure is a fluke, and restarting resolves the problem.
- **Read the error.** If an error message is displayed, read it. It has some important clues.
- **Last Known Good Configuration.** If you recently changed hardware or hardware drivers and you haven't logged on since, try Last Known Good Configuration from the Advanced Boot Options menu.
- **Startup Repair.** On Windows Vista and Windows 7, try the Startup Repair option from the System Recovery Options.
- **Safe mode.** Boot into safe mode, and perform different repairs:
  - Run antivirus software from within safe mode.
  - Run System Restore to apply a previous restore point.
  - Verify system files with the sfc /scannow tool.
- **Fix the boot sector or MBR.** Use the appropriate Windows tools to repair potential boot sector or MBR problems.

- **Restore the system from an image.** If you have an image, restore the system with the image after recovering user data.

MORE INFO **CHAPTER 26**

Some problems are caused by viruses or other types of malware. A solution is to run up-to-date antivirus software on the system to remove it. You can do so while booted normally or in safe mode. Chapter 26 provides more details about how to detect and remove malware.

Fix Boot Sector and MBR on Windows XP

If you need to repair the boot sector and/or the MBR on a Windows XP-based system, use the following steps:

1. Start the recovery console.
2. Enter the following command to repair the boot sector:

   ```
   fixboot
   ```

3. Enter the following command to repair the MBR:

   ```
   fixmbr
   ```

Fix Boot Sector and MBR on Windows Vista and Windows 7

If you need to repair the boot sector and/or the MBR on a Windows Vista-based or Windows 7–based system, use the following steps:

1. Start the Windows RE Command Prompt.
   A. Start the computer, and press F8 to access the Advanced Boot Options.
   B. Select Repair Your Computer to access the System Recovery Options.
   C. Select Command Prompt to access the Windows RE Command Prompt.
2. Enter the following command to repair the boot sector:

   ```
   bootrec /fixboot
   ```

3. Enter the following command to repair the MBR:

   ```
   bootrec /fixmbr
   ```

Rebuild BCD in Windows Vista and Windows 7

If you need to rebuild the BCD on a Windows Vista-based or Windows 7–based system, you can use the following steps:

1. Start the Windows RE Command Prompt.
2. **Enter the following commands to rebuild the BCD:**

```
bcdedit /export C:\backup_bcd
c:
cd boot
attrib bcd -s -h -r
ren c:\boot\bcd bcd.old
bootrec /rebuildbcd
```

The Windows RE boots you into the hidden 100-MB system partition, and it is identified as C within Windows RE. The BCD file is in the boot folder of this partition. Following is a description of what each of the preceding commands does:

- bcdedit /export creates a backup of the current BCD. This is useful if you later need to import data from it.
- attrib removes the system, hidden, and read-only attributes of the BCD file so that it can be renamed.
- ren renames the file as Bcd.old. This is useful if you need the original file later.
- bootrec /rebuildbcd creates a new BCD for the system.

MORE INFO **KB ARTICLE 927392 AND CHAPTER 14, "USING THE COMMAND PROMPT"**

For more information about the bootrec tool, check out knowledge base article 927392 at *http://support.microsoft.com/kb/927392*. Chapter 14 covers command prompt commands such as cd, attrib, and ren.

Improper Shutdown

Ideally, Windows should be shut down logically by clicking Start, Turn Off Your Computer, or by clicking Start, Shut Down, depending on the operating system. This gives Windows time to logically close files and processes. However, if the system suddenly loses power, Windows doesn't have time to clean things up.

When the system is restarted from an improper shutdown, you'll see an error message. You can often ignore the error and continue to restart the system. However, if it won't restart, follow the procedures in the "Failure to Boot" section.

Spontaneous Shutdown or Restart

There are a few reasons why Windows might stop or restart without giving you any warning. If it happens once, you can ignore it. However, if it happens more than once, you need to do some troubleshooting. The following are possible causes and solutions:

- **Infected computer.** Run antivirus software to check it. You might need to run sfc /scannow to repair system files.
- **Faulty RAM.** Run memory diagnostics to check the RAM.
- **Faulty power supply.** Check the voltages on the power supply to ensure that they are within tolerance, as mentioned in Chapter 1, "Introduction to Computers."

Device Fails to Start

If a single device fails to start, it's almost always due to a problem with the device driver. You can check the System log in Event Viewer to see whether it provides you with any error messages and use the Device Manager to check or update the driver. Chapter 15 provides details about how to resolve problems with device drivers by using the Device Manager.

Missing DLL Message

Windows systems use *dynamic link libraries (DLLs)* as reusable code. A DLL includes code for multiple programming tasks and can be used in different applications. All DLLs have an extension of .dll.

For example, a programmer can create code to identify the square root of a number. The code accepts a number as an input and provides the square root of the number as an output. The programmer could use the code in 50 different applications, but instead of re-creating the code each time, it is placed in a DLL and referenced from there. Each of these 50 applications can reference the same DLL.

Windows includes a wealth of DLLs, and third-party applications also use them. If Windows or an application tries to access a DLL and it is corrupted or missing, you might see a missing DLL error. These errors include the phrase "A required .DLL file (name.dll) could not be found." If this is due to a missing system DLL, you can use the system file checker (sfc) tool to scan and repair the system.

> ***MORE INFO*** **CHAPTER 14, "USING THE COMMAND PROMPT"**
>
> **Chapter 14 includes information about sfc, including steps to run it. The sfc /scannow command will scan all protected system files, including system DLLs, and attempt to repair them. You can also use the sfc /scanfile command to repair a specific DLL.**

If you see the error when you run an application, it's possible that the DLL is specific to the application. In this case, reinstall the application or use System Restore to revert your system to a restore point before the problem occurred.

Registering a DLL with Regsvr32

Sometimes you might need to register a DLL with the operating system so that it can use it. This is normally done automatically when an application is installed, but there are times when it is done manually. You can use the *regsvr32.exe* command to register and unregister DLLs manually. For example, if the DLL is named Success.dll, you can use the following commands to register or unregister it:

```
regsvr32 success.dll

regsvr32 /u success.dll
```

NOTE **REGSVR32 IS NOT THE SAME AS REGSRV3**

This command is frequently misspelled, so if you find the command isn't working, double-check the spelling. It is spelled as regsvr32.

Beware of Malware

A common response to a missing DLL error is to search on the Internet for a solution, but this can be dangerous. Many sites have infected files with the same or similar file name as a legitimate file. Criminals then use a variety of different methods to trick you into installing them. Users who download and install them might be giving up control of their computers or granting access to their bank accounts.

For example, users visiting a website could see an error pop up saying, "A required .DLL file (regsvr32.dll) could not be found." It could include a link to download the file and repair the problem. The truth is that there is no file named Regsvr32.dll (although there is a file named Regsvr32.exe). When users download and install this bogus file, they install malware and give a criminal access to their computers.

Similarly, the Kernel32.dll file is a legitimate Windows-based system file. Malware files named Kernel32.exe or Kernell32.exe (with an extra "L") are known malware, mimicking the legitimate file.

Some criminals host websites advertised as free DLL download sites where you can easily find missing DLLs. They actually host malware programs that look like legitimate DLLs. From a criminal's perspective, advertising a site as a free DLL download site is more successful than advertising it as a location hosting malware.

EXAM TIP

If you need to restore system DLLs, use the sfc /scannow command. Downloading and installing system DLLs from the Internet is not recommended.

Service Fails to Start

If a service fails to start, it will affect all the functions of the service. A good place to check is the System log in the Event Viewer. It will include log entries stating that the service failed to start and often includes hints about why.

Another good place to check is the Services applet covered in Chapter 13. Verify that the Startup Type is not set to Disabled, preventing the service from starting. Additionally, check the Dependencies tab of the service to identify any service dependencies. The service might not be starting due to a problem with another service.

Compatibility Error

Compatibility errors are most commonly associated with programs. If you're lucky, the program will fail and give an error saying directly that it's incompatible with the current operating system or with another application. More often, it will just fail to start.

You can check the Application log in the Event Viewer to see whether the error message gives you an indication of the problem. The best solution is to use the Compatibility tab of the application or to use the Compatibility Wizard as described in Chapter 11, "Introducing Windows Operating Systems," and in Chapter 15. You can use these tools to configure the application to run with settings that mimic a previous operating system.

Slow System Performance

If your system is running slowly, it could be because you're running more applications than it can manage, a process or application is causing a problem, or the system could be infected. Excessive paging is described in Chapter 16 and occurs if a system doesn't have enough memory. If that's the case, you can close some applications and it might return to normal.

Task Manager, described in Chapter 13, is a great tool to help you identify the source of the problem. You can open it by pressing Ctrl+Shift+Esc. If an application is hung up, it will be listed as Not Responding on the Application tab, and you can select it and click End Task to close it.

Check the Performance tab of Task Manager to see whether the CPU Usage is high. If it is, check the Processes tab to identify what process is consuming the CPU's time. It could be that antivirus software or some other application is running and consuming the system's resources.

One option is to right-click the offending application in the Processes tab and select Set Priority to set it to a lower priority, such as Below Normal. Don't do this with a system process; it could crash your system.

You might find that an unknown process is consuming your system resources. This could be malware, or it could be a legitimate process that you don't recognize. Sometimes a quick search on Bing.com will let you know the purpose of the processor.

Boots to Safe Mode

If a system consistently boots into safe mode, the most likely reason is that it is configured to do so. Normally, the only way you can access safe mode is by pressing F8 at startup and starting safe mode from the Advanced Boot Options menu. However, if the System Configuration (msconfig) tool is configured to boot into safe mode, it retains this configuration until you change it back.

The "Msconfig and Advanced Boot Options" section earlier in this chapter described the Boot tab of msconfig. If a system is rebooting into one of the safe modes, check the settings on this tab.

Another possibility is that the system is infected with malware. Malware can corrupt key system files, causing the system to go into safe mode automatically. The solution is to run up-to-date antivirus software from safe mode to clean the system.

File Fails to Open

Normally when you double-click a file, the associated application will start and the file will open within that application. For example, if you double-click a file named A+StudyNotes.docx, Microsoft Word 2010 will start and open the file. However, if the file has an unknown extension, such as .a+pass, the computer won't know what application to start and won't open the file.

On Windows XP, you can see and modify associations from the Folder Options applet by selecting the File Types tab. On Windows Vista and Windows 7, start the Default Programs applet in Control Panel and click Associate A File Type or Protocol With A Program. You can use the *assoc* | *more* command from the command prompt to see a list of extensions and the applications associated with each extension.

If you want to change an association from Windows Explorer, you can right-click the file and select Open With, Choose Default Program. Browse to the correct application, and select it.

Missing NTLDR and Missing Boot.ini

Windows XP-based systems use the NTLDR and Boot.ini files, and if they cannot be located, you might see one of the following errors:

- NTLDR is missing
- Invalid Boot.ini
- Windows could not start

These errors indicate that the system is trying to boot from a non-bootable disk. They indicate that there is a problem with either the NTLDR file or the Boot.ini file, or that the BIOS is not configured correctly. The following list identifies common fixes for these errors and steps for most of these fixes were provided earlier in this chapter. Chapter 2 includes information about working with BIOS.

- **Verify the boot order in BIOS.** Ensure that the system is not trying to boot to media without an operating system (such as a CD or DVD). You can also remove any CDs or DVDs from the drives.
- **Repair or replace the Boot.ini file.** It could be that the Boot.ini file is corrupt and pointing to the wrong location.
- **Fix the boot sector.** If the active partition has a corrupted boot sector, it might not be able to locate the NTLDR file.
- **Fix the MBR.** The MBR might be corrupted, causing this error.
- **Manually copy the file.** It's also possible that the NTLDR file is missing or corrupted, so you can manually copy it.

Manually Copy System Files in Windows XP

Some errors indicate that key files used in the Windows XP boot process have failed. One way to resolve the problem is to manually copy the files from the Windows XP installation CD. The two files you might need to copy are NTLDR and Ntdetect.com.

Both of these files are available in the i386 folder of the installation CD. They are normally in the root of the C drive, and you can copy them from the CD to the C drive with the following steps:

1. Start the Recovery Console.
2. Insert the installation CD and identify the drive letter. For these examples, assume it is assigned the letter D.
3. Use the following commands to copy the NTLDR and Ntdetect.com files from the installation CD to the C drive. If the system partition is something other than C, use that letter instead.

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

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

Rebuild Boot.ini File in Windows XP

The Boot.ini file is used only with Windows XP. There might be times when the Boot.ini file used in Windows XP needs to be modified or re-created. You can modify it with Notepad if you know the correct settings, or you can rebuild it with the following steps:

1. Start the Recovery Console.
2. Enter the following command to rebuild the Boot.ini file:

```
bootcfg /rebuild
```

This command scans the system for bootable operating systems and automatically creates the Boot.ini file with the proper settings.

Boot Sector and MBR Errors

Many other errors are caused by problems with the boot sector or MBR. For example, if boot sector information is missing, a disk doesn't have an active partition, or there is a problem with the MBR, you might see one of the following errors:

- Missing operating system
- Error loading operating system
- Invalid partition table

EXAM TIP

These errors can also be described generically as the graphical interface fails to load or the graphical interface is missing. If Windows won't start at all, it's often a problem with the hard drive holding the boot sector or MBR or with the BIOS boot order.

Some errors indicate a problem with the boot sector (or that the system is trying to boot from the wrong disk). These include the following:

- Non-system disk or disk error
- Invalid boot disk
- Disk boot failure

On Windows Vista and Windows 7, a problem with the MBR can give you one of the following errors:

- Bootmgr not found
- Bootmgr is missing

The solution to all of these errors is summarized in the following three tasks:

- **Verify boot order in BIOS.** Check BIOS to ensure that you're booting from the correct media.
- **Repair or replace the BCD.** It could be that the BCD is corrupt and needs to repaired with the bootrec /rebuildbcd command.
- **Fix the boot sector.** Use fixboot on Windows XP and bootrec /fixboot on Windows Vista and Windows 7.
- **Fix the MBR.** Use fixmbr on Windows XP and bootrec /fixmbr on Windows Vista and Windows 7.

EXAM TIP

On Windows Vista and Windows 7, the Startup Repair option from the System Recovery Options menu will often check and repair boot sector and MBR problems without requiring user interaction. This is a simple step to take and resolves many problems.

✓ **Quick Check**

1. **What are common reasons for slow system performance?**
2. **How can you restore system DLLs?**

Quick Check Answers

1. **Fix the boot sector and MBR.**
2. **Run sfc /scannow.**

Chapter Summary

- The boot process starts with POST and loads code from the MBR. The MBR identifies the active partition and loads code from its boot sector. On Windows XP, it uses NTLDR, Boot.ini, Ntdetect.com, and Ntoskrnl.exe. On Windows Vista and Windows 7, it uses the bootmgr, BCD, and Winload.exe.
- Windows stores systems settings in the registry. You can use the registry editor (regedit or regedt32) to view, modify, and back up the registry.
- Press F8 on startup to access the Advanced Boot Options. It provides access to Repair Your Computer, safe modes, last known good configuration, and other troubleshooting tools.
- Safe modes load only basic drivers and services. Use safe mode with networking if you need to access the Internet. Last Known Good Configuration can be used to restore the settings from the last successful boot. It's useful only if the user hasn't logged on after making changes.
- Windows XP supports the recovery console and commands such as fixboot, fixmbr, and bootcfg /rebuild. Windows Vista and Windows 7 use the Windows RE and commands such as bootrec /fixboot, bootrec /fixmbr, and bootrec /rebuildbcd.
- The Event Viewer is used to view logs. System logs record system events, such as when a driver or service fails to load. Application logs record applications events, such as when a third-party virus application detects malware.
- You can create a system repair disc in Windows 7 and use it to boot directly into the Windows RE from a bootable CD.
- When troubleshooting problems, try a restart first. If the restart doesn't solve the problem, pay close attention to error messages for clues.
- Repair system DLLs with the sfc /scannow tool.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter: The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the “Answers” section at the end of this chapter.

1. You need to start Windows 7 in safe mode. What should you do?

   A. Reconfigure the Boot.ini file.

   B. Restart it, and press F8 as it starts.

   C. Run bootrec /safemode.

   D. Select Safe Mode from Task Manager.

2. After installing a new driver, a user’s system is caught in a reboot loop. Which of the following choices would be the easiest way to restore the system?

   A. Perform an image recovery.

   B. Start safe mode and roll back the driver.

   C. Start safe mode and revert to a previous restore point.

   D. Use Last Known Good Configuration.

3. A Windows 7–based system fails, showing a blue screen, but restarts before you can view the error. What should you do?

   A. Modify the Startup and Recovery boot options.

   B. Modify the options from the Advanced Boot Options menu.

   C. Boot into safe mode, and view the Ntbtlog.txt file.

   D. Reboot the system by using the System Repair disc.

4. A user complained that he saw an error message and then his system failed. He doesn’t remember what the message said. How can you identify the contents of the error message?

   A. Use Task Manager.

   B. Use Performance Monitor.

   C. Use Event Viewer.

   D. Use Device Manager.

5. After booting a Windows XP-based system, you see an error indicating that NTLDR is missing. Of the following choices, which has the best possibility of resolving this problem?

   A. Run the fixmbr command from the recovery console.

   B. Run the System Repair utility.

   C. Format the disk with diskpart.

   D. Run the bootrec /fixmbr command from the Windows RE.

6. A Windows 7–based system fails to boot and gives a "Missing Operating System" message. Of the following choices, which has the best chance of resolving this problem?

   A. Run the fixboot command from Windows RE.

   B. Run the bootrec /fixboot command from Windows RE.

   C. Rebuild the Boot.ini file.

   D. Download a replacement Regsvr32.dll file.

Answers

This section contains the answers to the chapter review questions in this chapter.

1. **Correct Answer:** B

   A. **Incorrect:** Windows 7 does not use boot.ini.

   B. **Correct:** Safe mode is started from the Advanced Boot Options menu, which is shown by pressing F8 when a computer starts.

   C. **Incorrect:** Bootrec does not include a /safemode switch.

   D. **Incorrect:** Safe Mode cannot be started from Task Manager

2. **Correct Answer:** D

   A. **Incorrect:** Performing an image recovery would take the longest time of the given choices.

   B. **Incorrect:** Rolling back a driver from Safe Mode is possible, but it requires more steps than using Last Known Good Configuration.

   C. **Incorrect:** Reverting to a previous restore point is possible, but it requires more steps than Last Known Good Configuration.

   D. **Correct:** Last Known Good Configuration is possible because the user has not logged on yet. It is accessed after pressing F8 on boot to access the Advanced Boot Options menu.

3. **Correct Answer:** B

   A. **Incorrect:** If the system started, you could modify the Startup And Recovery boot options, but it won't start.

   B. **Correct:** You can select Disable Automatic Restart on System Failure from the Advanced Boot Options menu. This stops an automatic reboot so that you can view the error.

   C. **Incorrect:** Ntbtlog.txt isn't available unless Enable Boot Logging is enabled from the Advanced Boot Options menu.

   D. **Incorrect:** The System Repair Disc can be useful to help you repair the system but not to view the error.

4. **Correct Answer:** C

   A. **Incorrect:** The Task Manager is used to view current activity and end tasks that are not responding.

   B. **Incorrect:** Performance Monitor provides extended capabilities to monitor system resources.

   C. **Correct:** Event Viewer is used to view logs. Error messages are logged in the System or Application logs.

   D. **Incorrect:** The Device Manager is used to manage devices and their drivers.

5. **Correct Answer:** A

   A. **Correct:** The recovery console fixmbr command will repair many problems, including this error in some situations.

   B. **Incorrect:** The System Repair utility in Windows Vista and Windows 7 is not available on Windows XP.

   C. **Incorrect:** Formatting the disk causes you to start all over, but this problem can usually be repaired.

   D. **Incorrect:** The bootrec /fixmbr command is available in Windows Vista and Windows 7, but not in Windows XP.

6. **Correct Answer:** B

   A. **Incorrect:** The fixboot command is not available in the Windows Recovery Environment (Windows RE).

   B. **Correct:** The bootrec /fixboot command in the Windows RE will fix the boot sector and might resolve this problem.

   C. **Incorrect:** Windows 7 does not use boot.ini.

   D. **Incorrect:** Windows uses a regsvr32.exe file to register DLLs, but regsvr32.dll might be malware.