COURSE TECHNOLOGY
CENGAGE Learning

A+ Guide to Software: Managing, Maintaining, and Troubleshooting, 5e

Chapter 6

Tools for Solving Windows Problems

Objectives

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

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors

- Tools for solving Windows problems after startup
  - 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
  - Diagnostic utilities

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Vista Problem Reports and Solutions
  - Use with immediate hardware and software problems
  - Provides a history feature
  - Displays an error screen
  - Problem in Windows kernel mode
    - STOP or blue screen error occurs on next restart
    - User can check for solution
  - Problem in user mode
    - Bubble displays in notification area

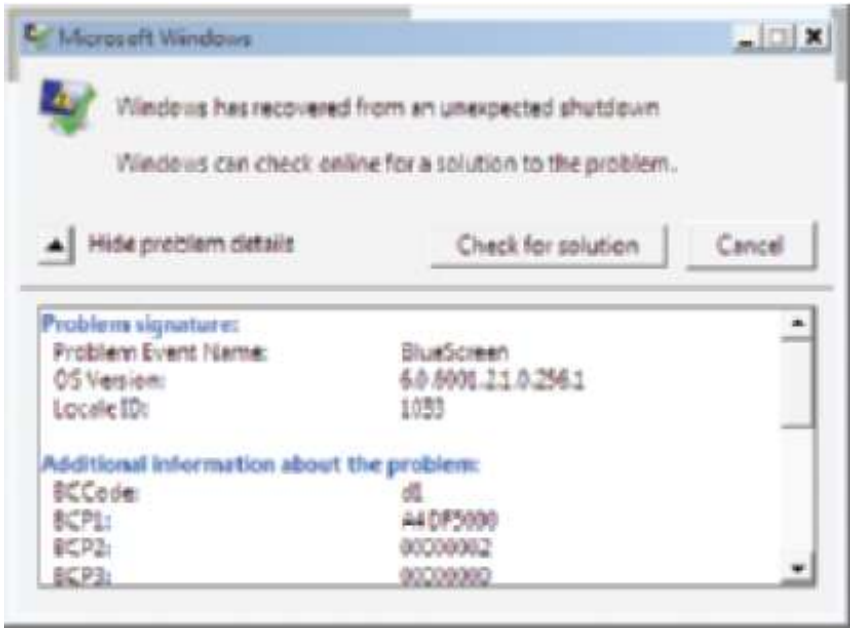

Figure 6-1 Windows reports information about an error
Courtesy: Course Technology/Cengage Learning

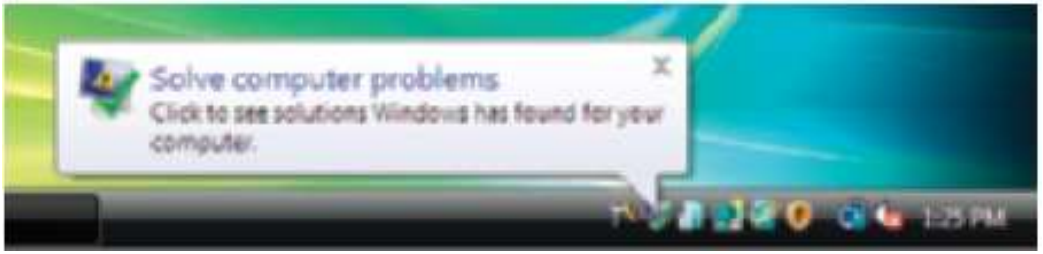

Figure 6-2 Vista error reporting gives an error alert
Courtesy: Course Technology/Cengage Learning

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Vista Problem Reports and Solutions (cont'd.)
  - Viewing a list of solutions not applied
    - Click item for more detail and possibly apply the solution
    - Click Check for new solutions to send information to Microsoft and possibly find new solutions to known problems
  - Viewing past problem history
    - Click View problem history

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Windows XP Error Reporting tool
  - Application error encountered:
    - Problem description message displayed
    - Option to send error report to Microsoft
  - After information sent:
    - Dialogue box appears
    - Provides ability to obtain possible solutions
  - Does not keep a history of previous errors

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Vista Memory Diagnostics tool
  - Identifies problem with memory
  - Eliminates memory as problem source
    - Vista Error Reporting tool prompt to test memory on next reboot
    - Command Prompt window command: mdsched.exe
    - Dual boot: run memory diagnostic test from Windows Vista boot menu
    - Single OS: force Vista boot menu by pressing Spacebar during the boot
    - Use Windows Vista DVD

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- System file checker (SFC) Windows Vista/XP utility
  - Corrupted Windows system file
    - May cause Windows application or hardware problem
  - SFC protects system files and keeps cache current
    - Can refresh a damaged file
  - Run SFC in command prompt window: sfc /scannow
    - Vista requires elevated command prompt

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Driver verifier runs in the background
  - Useful for troubleshooting intermittent problems
  - Puts stress on drivers
  - Problem generates STOP error for problem driver identification
    - Obtain information by looking at file Properties box
  - Run for several days
    - If no problem identified: turn off
  - Be cautious if running on a server

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Tools to verify driver signatures
  - Prevent boot problems, unstable Windows systems, and error messages
  - File Signature Verification tool
    - Displays information about digitally signed file
  - Driver Query tool
    - Directs information about drivers to a file
  - Device Manager
    - Use if problem driver is known
    - Review digital signature information in device's Properties dialog box

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Using Device Manager to update drivers
  - Locate drivers
  - In Device Manger, right-click device, select Properties
  - Select the Driver tab, click Update Driver
    - Update Driver Software box opens
  - Search Internet for drivers or browse computer
- Using Device Manager to roll back drivers
  - In Device Manger, right-click device, select Properties
  - Click Roll Back Driver

Tools to Help with Blue Screen Errors, System Lockups, and I/O Device Errors (cont'd.)

- Device setup CD: use diagnostic utilities
- Tools for blue screen errors
  - Look for stop error and specific error number
    - Search Microsoft Web site
  - Vista Problem Reports and Solutions window
    - Might provide information after reboot
  - Event Viewer might provide events
- Tools for system lockouts
  - Use event viewer, Reliability and Performance Monitor, Vista Problem Reports and Solutions window, and/or Vista Memory Diagnostics

Figure 6-20 A blue screen of death (BSOD) is definitively not a good sign; time to start troubleshooting. Courtesy: Course Technology/Cengage Learning

Vista Tools For Solving Startup Problems

- Vista tools to solve startup problems
  - Advanced Boot Options menu
    - XP/2000: Advanced Options menu
  - Vista Recovery Environment
  - Command prompt window in Windows RE

Files Needed to Start Windows Vista

- Vista system successful start
  - When user can log onto Windows and desktop loads
  - Hardware requirements
    - CPU, motherboard, memory, power supply, boot device
  - Two files managing Vista startup
    - Windows Boot Manager (BootMgr)
    - Windows Boot Loader (WinLoad.exe)
  - Vista configuration data
    - Stored in Vista Boot Configuration Data (BCD) file
  - System partition contains BootMgr and BCD
  - Boot partition contains other files

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 6-2 Software components and files needed to start Windows Vista

Files Needed to Start Windows Vista (cont'd.)

- Vista Boot Configuration Data (BCD) file
  - Structured the same as a registry file
  - Contains configuration information about how Vista started
  - BCD information
    - Settings controlling BootMgr and WinLoad.exe
    - Settings controlling WinResume.exe
    - Settings to start and control Windows Memory Diagnostic program
    - Settings that launch Ntldr to load previous OS in a dual-boot configuration
    - Settings to load a non-Microsoft operating system

Steps to Start a Vista Computer

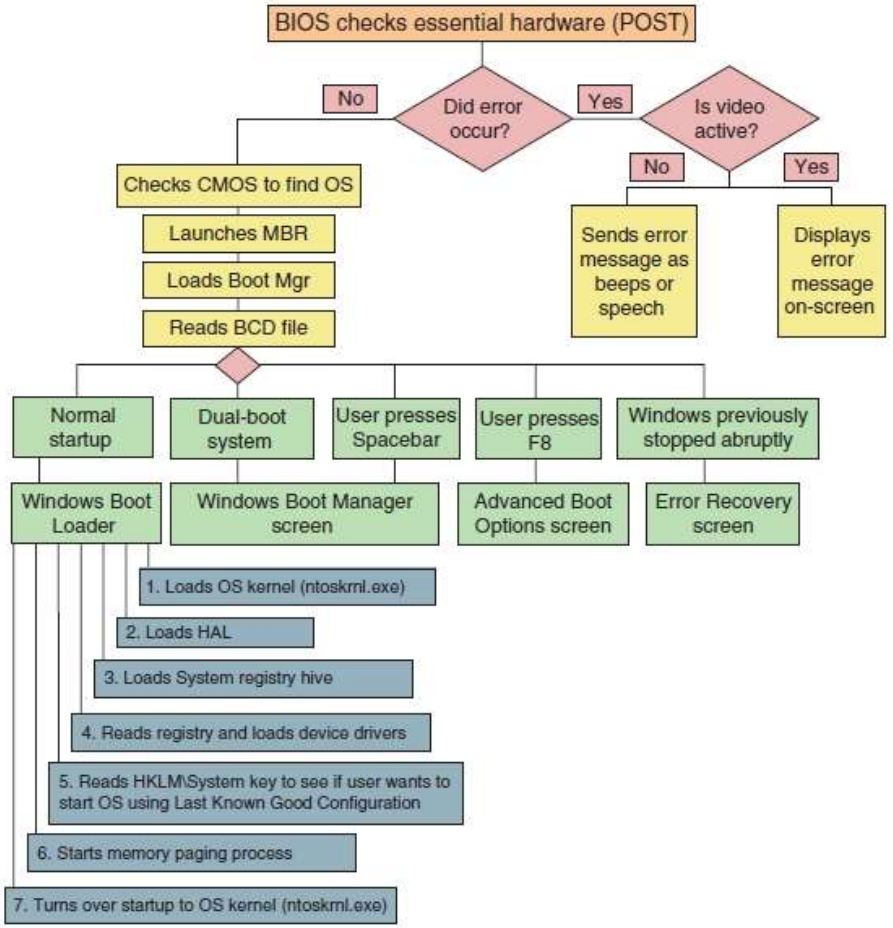

Figure 6-21 Steps to booting the computer and loading Vista
Courtesy: Course Technology/Cengage Learning

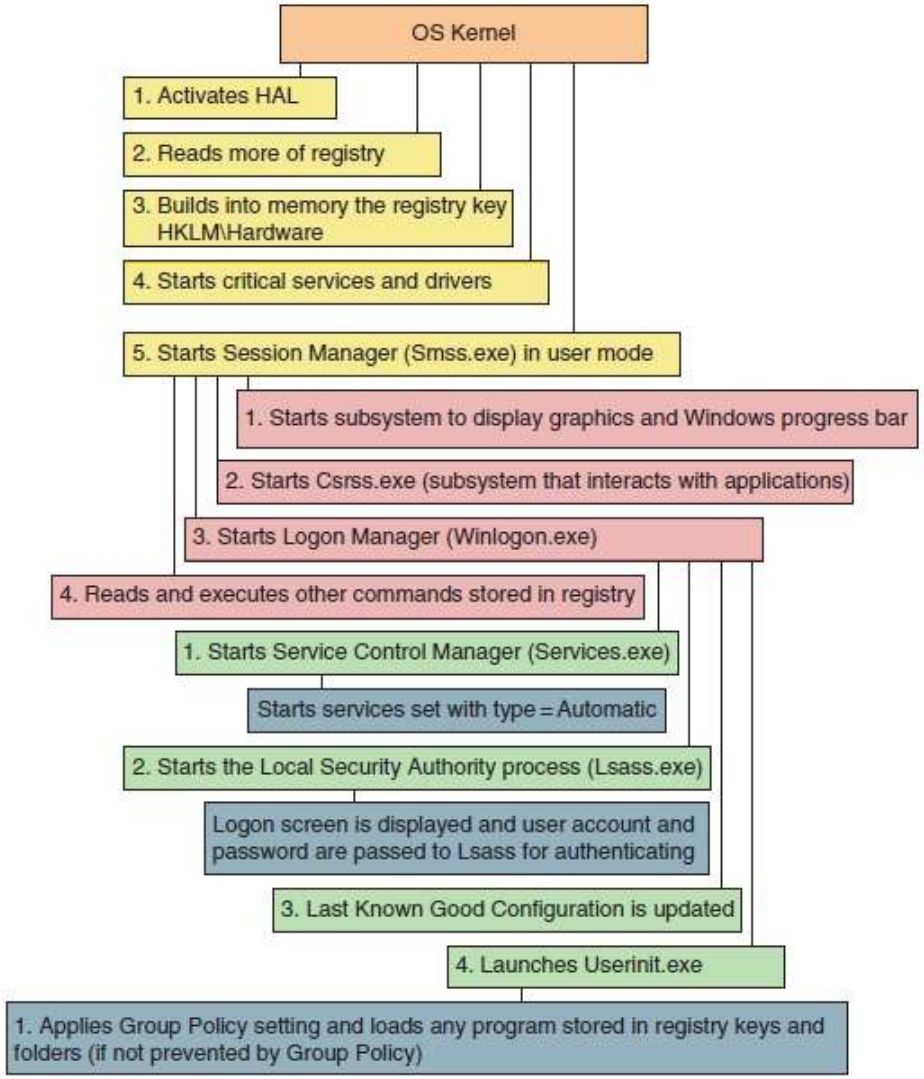

Figure 6-22 Steps to complete loading Vista
Courtesy: Course Technology/Cengage Learning

Steps to Start a Vista Computer (cont'd.)

- Windows startup is officially completed when Windows desktop appears and wait circle disappears

Figure 6-27 Windows Vista logon screen
Courtesy: Course Technology/Cengage Learning

Advanced Boot Options Menu

- Press F8 as Vista loads
- Safe Mode boots a minimum configuration OS
  - Uses default system services
  - No networking
  - Uses a plain video driver
  - “Safe Mode” appears in four corners of the screen
  - GUI interface
  - Screen resolution: 600 x 800
  - Desktop wallpaper (background): black

Advanced Boot Options Menu (cont'd.)

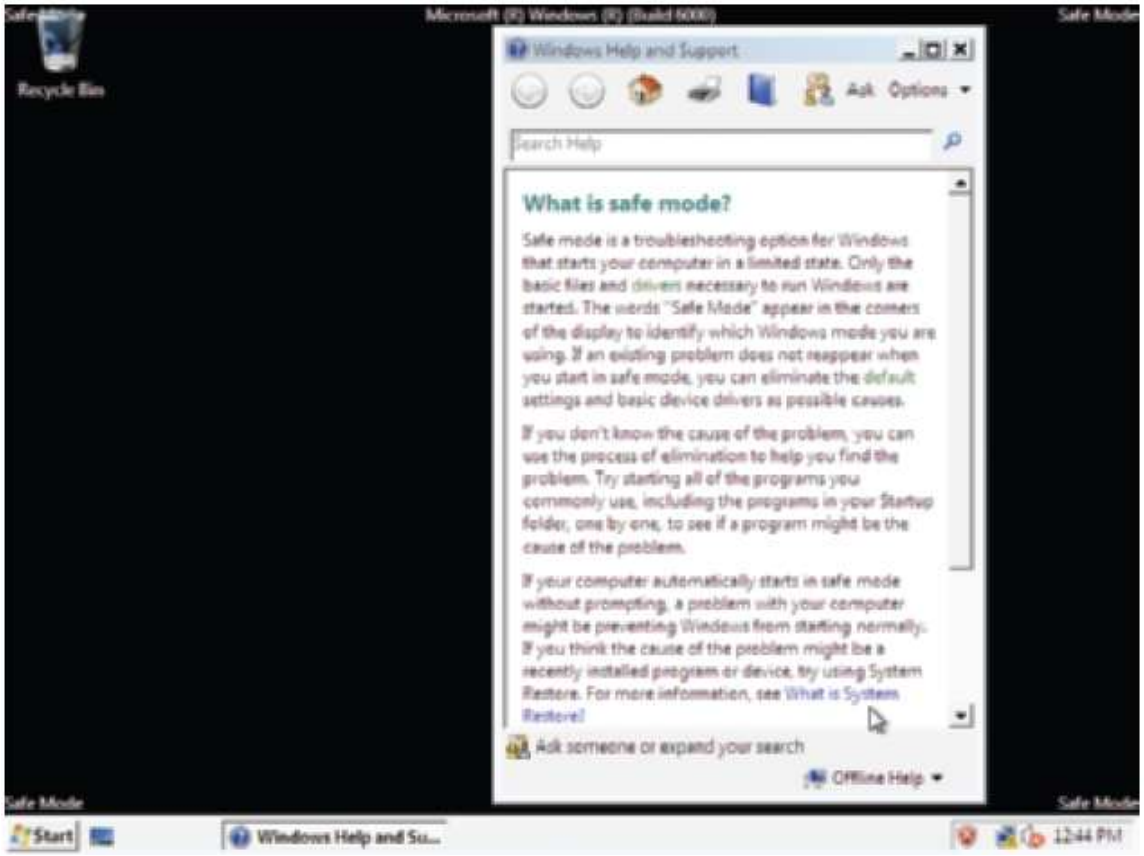

Figure 6-28 Safe Mode loads a minimum Vista configuration
Courtesy: Course Technology/Cengage Learning

Advanced Boot Options Menu (cont'd.)

- Recovering the system using Safe Mode
  - Use System restore
  - Scan system for virus and run Chkdsk
  - Use Device Manager to uninstall, disable a device with problems, or roll back a driver
  - Use Msconfig to disable unneeded services or startup processes
  - Use Programs and Features window to uninstall software
  - Investigate problems

Advanced Boot Options Menu (cont'd.)

- Tips about loading Safe Mode
  - Safe mode selection order
    - First, try Safe Mode with Networking
    - Next, try Safe Mode
    - Then, try Safe Mode with Command prompt
  - Safe Mode won't load if core Windows components are corrupted
  - When loading Windows in Safe Mode
    - All files used for the load are recorded in Ntbtlog.txt file
    - File might identify service, device driver, or application loaded at startup causing a problem

Advanced Boot Options Menu (cont'd.)

- Safe mode with networking
  - Use when solving a problem with booting and network access is needed
- Safe mode with command prompt
  - Use the SFC command to verify system files
  - Use the Chkdsk command to check for file system errors
  - If problem not solved, launch System Restore

Advanced Boot Options Menu (cont'd.)

- Enable boot logging
  - Windows loads normally with regular desktop
  - All files used during load process are recorded
    - C:\Windows\Ntbtlog.txt

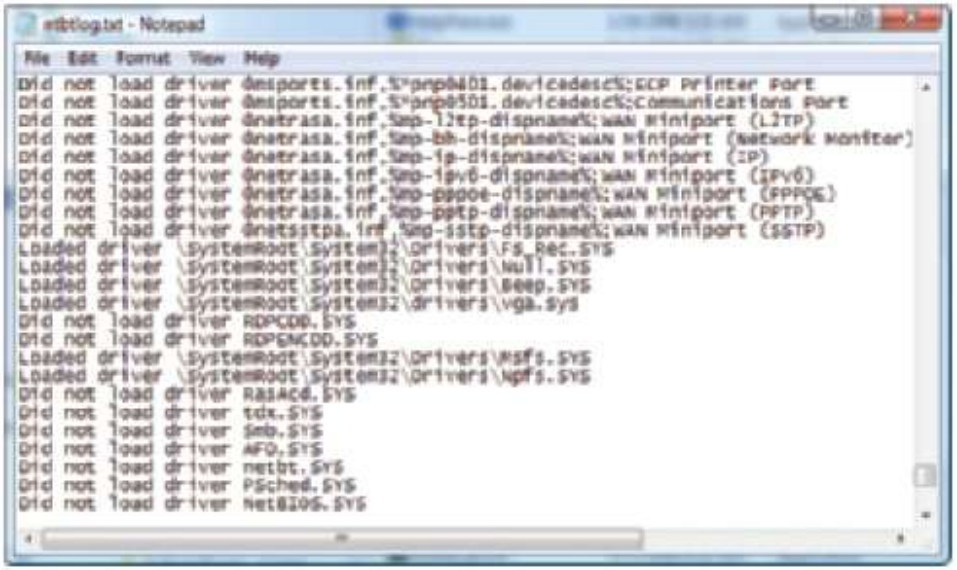

Figure 6-29 Sample Ntbtlog.txt file
Courtesy: Course Technology/Cengage Learning

Advanced Boot Options Menu (cont'd.)

- Enable low-resolution video (640x480)
  - Windows XP: "Enable VGA Mode"
  - Used when video setting does not allow screen to display clearly to fix a bad setting
- Last known good configuration
  - Saved in registry after each successful logon
  - Can undo a bad installation and solve the problem
  - Try the Last Known Good early in troubleshooting, before it's overwritten
    - When logging onto the system in Safe Mode, the Last Known Good not saved

Advanced Boot Options Menu (cont'd.)

- Directory services restore mode (Windows Domain controllers only)
  - Used as one step in the process of recovering from a corrupted Active Directory
- Debugging mode
  - Can move system boot logs from failing computer to another computer for evaluation
- Disable automatic restart on system failure
  - Stop rebooting upon encountering a system failure

The Windows Recovery Environment (Windows RE)

- Operating system launched from the Vista DVD
  - Provides graphical and command-line interfaces
- Steps to launch Windows RE
  - 1. Boot from Vista setup DVD, and select language preference
  - 2. Click Repair your computer
    - Recovery environment (RecEnv.exe) launches
  - 3. From the Recovery Options dialog box, select the Vista installation to repair
  - 4. System Recovery Options window appears
    - Lists recovery options

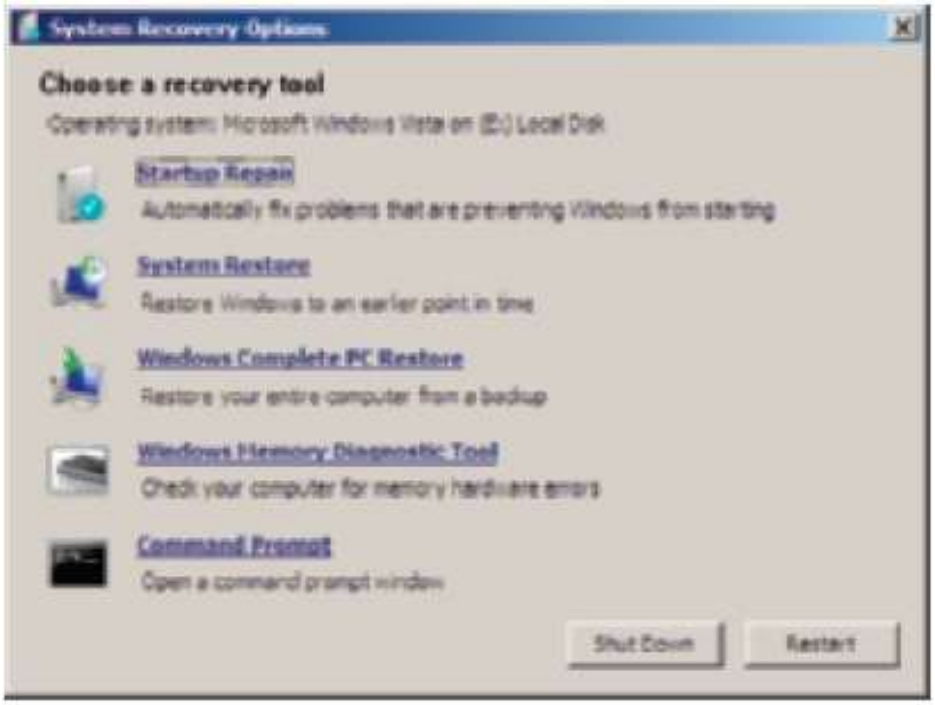

Figure 6-34 Recovery tools in Windows RE
Courtesy: Course Technology/Cengage Learning

The Windows Recovery Environment (cont'd)

- Steps to launch Windows RE (cont'd.)
  - 5. Startup Repair can automatically fix many Windows problems
  - 6. Startup Repair suggests solutions
  - 7. View list of items examined and actions taken
    - Click on Click here for diagnostic and repair details
    - View log file
  - 8. View list of restore points
  - 9. Windows Complete PC Restore
    - Completely restore drive C and possibly other drives to state when last backup made

The Windows Recovery Environment (cont'd)

- Steps to launch Windows RE (cont'd.)
  - 10. Use the Windows Memory Diagnostic Tool
  - 11. Click Command Prompt to open a command prompt window
    - Issue commands: repair corrupted Vista system or recover data
  - 12. Reboot in between fixes
  - Exiting the Recovery Environment
    - Click Shut Down or Restart

The Command Prompt Window in Windows RE

- Use when graphical tools available in Windows RE fail to solve the Vista problem
  - Can issue commands to repair system files, boot records, and partitions
  - Restore registry files using those saved in the C:\Windows\System32\Config\RegBack folder

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 6-3 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 6-4 Steps to restore the registry files

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 6-4 Steps to restore the registry files (continued)

Windows 2000/XP Tools for Solving Startup Problems

- Topics covered
  - Boot process and the Boot.ini file
  - Tools that can help when Windows 2000/XP gives startup problems
    - Advanced Options Menu
    - Windows 2000/XP Boot Disk
    - Recovery Console
    - Windows 2000 Emergency Repair process

What Happens When Windows 2000/XP Starts Up

- Windows 2000/XP system has started up when the user logged on, Windows desktop loaded, hourglass associated with pointer disappeared

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 6-5 Steps in the Windows 2000/XP boot process for systems with Intel-based processors (continued)

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 6-5 Steps in The Windows 2000/XP boot process for systems with Intel-based processors (continued)

Files Needed to Start 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 6-6 Files needed to boot Windows 2000/XP successfully

The BOOT.INI File

- Hidden text file in active partition root directory
  - Ntldr reads boot.ini to determine available operating systems and how to set up the boot

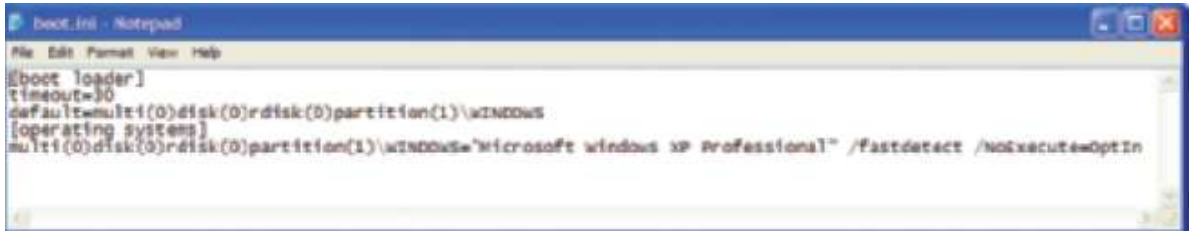

Figure 6-41 A sample Windows XP Boot.ini file
Courtesy: Course Technology/Cengage Learning

Figure 6-42 A sample Boot.ini file on a dual-boot system
Courtesy: Course Technology/Cengage Learning

The BOOT.INI File (cont'd.)

- Viewing and editing Boot.ini file using a text editor
  - Change folder options to view hidden system files
- Two main sections in Boot.ini
  - The [boot loader] section
    - Timeout information (30 second default)
    - Dual boot: path to the default operating system
  - The [operating systems] section
    - List of operating systems

The BOOT.INI File (cont'd.)

- The [operating systems] entry meanings
  - Multi(0): Use the first hard drive controller
  - Disk(0): Use only when booting from a SCSI hard drive
  - Rdisk(0): Use first hard drive
  - Partition(1): Use first partition on drive
- Switches used in [operating systems] section
  - /fastdetect
  - /NoExecuteOptIn
- Change boot.ini with System Properties box

Advanced Options Menu

- Press F8 when “Starting Windows” message appears
  - Menu used to diagnose and fix problems when booting Windows 2000/XP

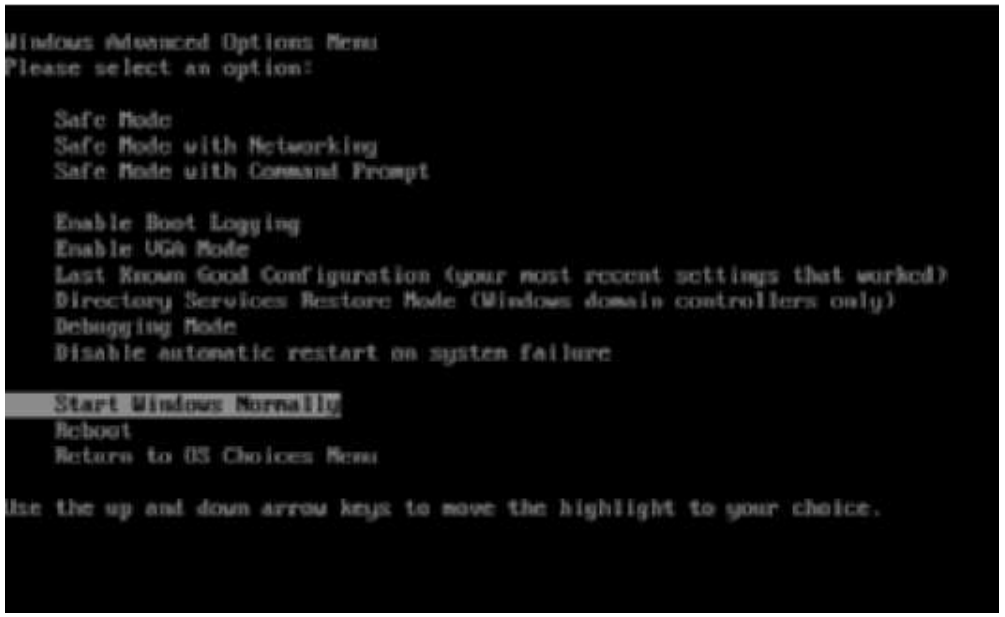

Figure 6-43 Press the F8 key at startup to display the Windows XP Advanced Options menu
Courtesy: Course Technology/Cengage Learning

Windows 2000/XP Boot Disk

- Boots the system bypassing boot files stored in the root directory of drive C
  - Can prove damaged sectors or missing or damaged files required to boot the OS
- Creating a boot disk
  - Format the disk with Windows 2000/XP
  - Copy files to the disk
- Windows 2000/XP desktop loads successfully from boot disk
  - Attempt to repair Windows 2000/XP installation

Windows 2000/XP Boot Disk (cont'd.)

- Steps to repair
  - 1. Load Recovery Console and use the Fixmbr and Fixboot to repair MBR and OS boot sector
  - 2. Run anti-virus software
  - 3. Verify hard drive partition table correct
  - 4. Defragment the hard drive
  - 5. Copy Ntldr, Ntdetect.com, Boot.ini from floppy disk to the root of the hard drive
  - 6. For SCSI hard drive, copy Ntbootdd.sys from floppy disk

Recovery Console

- Goes deeper than the Advanced Options Menu
- Used when Windows 2000/XP does not start properly or hangs during the load
- Works even when core Windows system files are corrupted
- Command-driven operating system
  - Does not use a GUI
  - Can access the FAT16, FAT32, NTFS file systems

Recovery Console (cont'd.)

- Tasks
  - Repair a damaged registry, system files, or hard drive file system
  - Enable or disable a service or device driver
  - Repair the master boot program on the hard drive or boot sector on the system partition
  - Repair a damaged Boot.ini file
  - Recover data when Windows installation is beyond repair
  - Offers security to prevent malicious use and many commands

Recovery Console (cont'd.)

- Commands to examine hard drive structure for errors and possibly fix them:
  - Fixmbr and Fixboot
  - Diskpart
  - Chkdsk
- Commands are available to restore Windows XP/2000 registry hive files from backups

Recovery Console (cont'd.)

- Disabling critical service or device driver
  - Determine name or description of service or driver
    - Look at error message
    - Boot to Advanced Options Menu, select Enable Boot Logging, compare Ntbtlog.txt file to one generated on a healthy system
  - Commands to list services and disable/enable a service:
    - Listsvc
    - Disable
    - Enable

Recovery Console (cont'd.)

- Commands to restore system files
  - Map, Systemroot, CD, Delete, Copy, Bootcfg, Expand

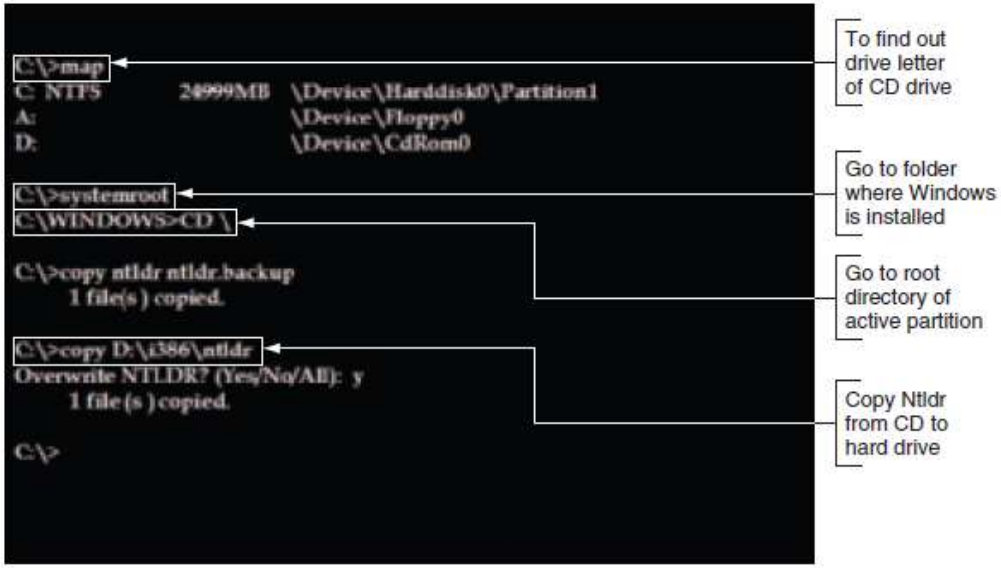

Figure 6-54 Recovery Console command to repair Ntldr
Courtesy: Course Technology/Cengage Learning

Recovery Console (cont'd.)

- Recover data
  - Change Recovery Console default settings
  - Use Copy command to copy data from the hard drive to other media
- Install Recovery Console on a working system
  - 1. Open a command window
  - 2. Change from current directory to the \i386 folder on the Windows 2000/XP CD
  - 3. Enter the command winnt32/cmdcons
  - 4. Restart the computer

Windows 2000 Emergency Repair Process

- Last resort
  - Restores system to the state it was in immediately after the Windows 2000 installation
- Process uses an Emergency Repair Disk (ERD)
  - Contains information about current installation
  - Points to a hard drive folder where registry backed up when Windows 2000 installed
    - Folder: %SystemRoot%\repair
    - In most systems: C:\Winnt\repair

Summary

- Many tools and settings are available for solving Windows problems occurring after startup
  - Tools Vista startup problems
    - Advanced Boot Options menu
    - Vista Recovery Environment
    - Windows RE command prompt
  - Tools for Windows 2000/XP startup problems
    - Advanced Options Menu
    - Windows 2000/XP Boot Disk
    - Recovery Console
    - Windows 2000 Emergency Repair process