CHAPTER

11

Optimizing Windows

In this chapter, you will learn:

- About Windows utilities and tools you can use to solve problems with Windows
- How to optimize Windows to improve performance
- How to manually remove software

In the last chapter, you learned about the tools and strategies to maintain Windows and about the importance of keeping good backups. This chapter takes you one step further as a PC support technician so that you can get the best performance out of Windows. We begin the chapter learning about the Windows tools you'll need to optimize Windows. Then we turn our attention to the steps you can follow to cause a sluggish Windows system to perform at its best and how to manually remove software that does not uninstall using normal methods. As you read the chapter, you might consider following along using a Windows 7 system.

Notes Windows installed in a virtual machine is an excellent environment to use when practicing the skills in this chapter.

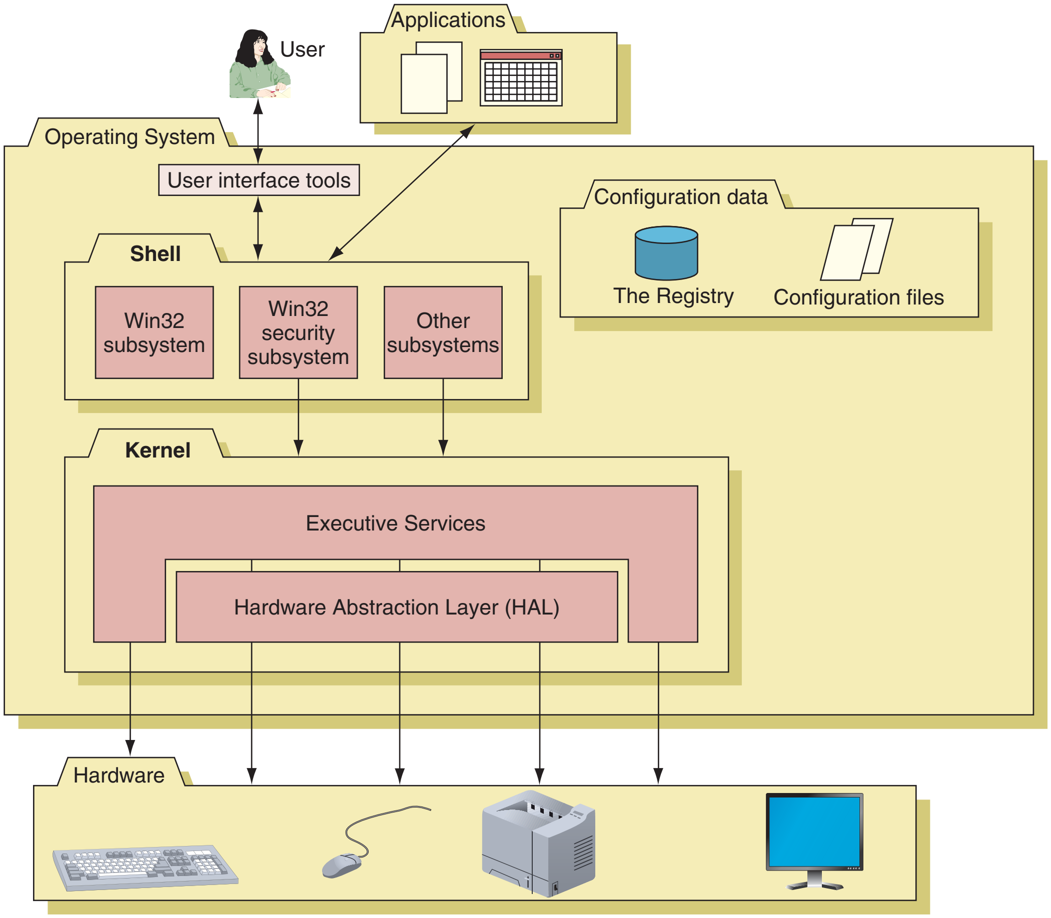
WINDOWS UTILITIES AND TOOLS TO SUPPORT THE OS

A+
220-802
1.4

Knowledge is power when it comes to supporting Windows. In this part of the chapter, you learn more about how Windows works and to use some Windows tools to poke around under the hood to see what is really happening that is slowing Windows down or giving other problems.

WHAT IS THE SHELL AND THE KERNEL?

Sounds like we're talking about a grain of wheat, but Windows has a shell and a kernel and you need to understand what they are and how they work so you can solve problems with each. A **shell** is the portion of an OS that relates to the user and to applications. The **kernel** is responsible for interacting with hardware. Figure 11-1 shows how the shell and kernel relate to users, applications, and hardware. In addition, the figure shows a third component of an OS, the configuration data. For Windows, this data is primarily contained in the registry.



© Cengage Learning 2014

Figure 11-1 Inside an operating system, different components perform various functions

THE WINDOWS SHELL

The shell provides tools such as Windows Explorer or the Windows desktop as a way for the user to do such things as select music to burn to a CD or launch an application. For applications, the shell provides commands and procedures that applications can call on to do such things as print a document, read from a storage device, or display a photograph on-screen.

The shell is made up of several subsystems that all operate in **user mode**, which means these subsystems have only limited access to system information and can access hardware

A+
220-802
1.4

only through other OS services. One of these subsystems, the Win32 security subsystem, provides logon to the system and other security functions, including privileges for file access. All applications relate to Windows by way of the Win32 subsystem.

THE WINDOWS KERNEL

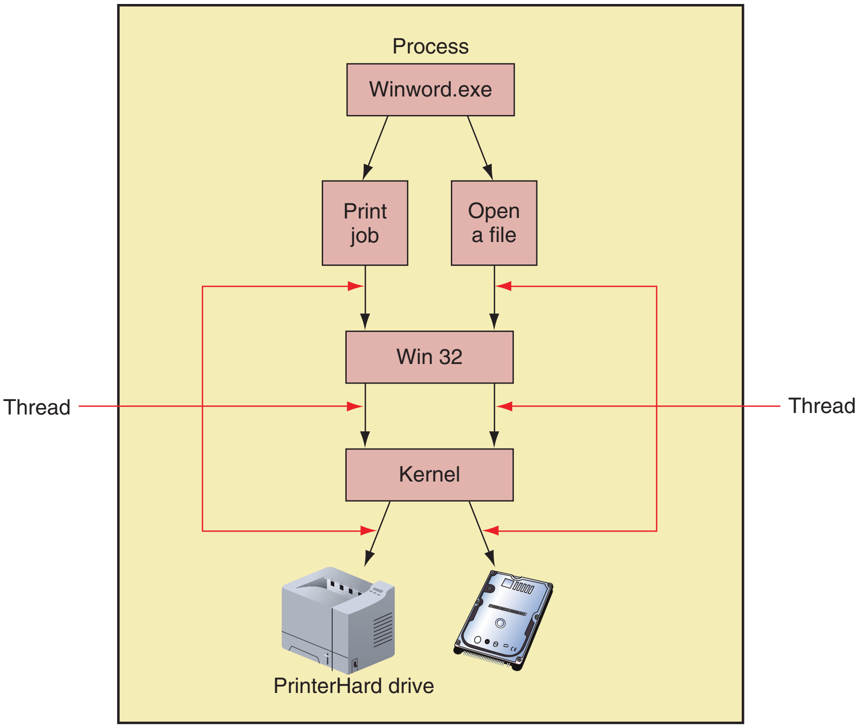
The kernel, or core, of the OS is responsible for interacting with hardware. Because the kernel operates in **kernel mode**, it has more power to communicate with hardware devices than the shell has. Applications operating under the OS cannot get to hardware devices without the shell passing those requests to the kernel. This separation of tasks provides for a more stable system and helps to prevent a wayward application from destabilizing the system.

The kernel has two main components: 1) the **HAL (hardware abstraction layer)**, which is the layer closest to the hardware, and 2) the **executive services** interface, which is a group of services that operate in kernel mode between the user mode subsystems and the HAL. Executive services contained in the ntoskrnl.exe program file manage memory, I/O devices, file systems, some security, and other key components directly or by way of device drivers.

When Windows is first installed, it builds the HAL based on the type of CPU installed. The HAL cannot be moved from one computer to another, which is one reason you cannot copy a Windows installation from one computer to another.

HOW WINDOWS MANAGES APPLICATIONS

When an application is first installed, its program files are normally stored on the hard drive. When the application is launched, the program is copied from the hard drive into memory and there it is called a process. A **process** is a program that is running under the authority of the shell, together with the system resources assigned to it. System resources might include other programs it has started and memory addresses to hold its data. When the process makes a request for resources, this request is made to the Win32 subsystem and is called a thread. A **thread** is a single task, such as the task of printing a file that the process requests from the kernel. Figure 11-2 shows two threads in action, which is possible



© Cengage Learning 2014

Figure 11-2 A process with more than one thread is called multithreading

A+
220-802
1.4

because the process and Windows support multithreading. Sometimes a process is called an instance, such as when you say to a user, “Open two instances of Internet Explorer.” Technically, you are saying to open two Internet Explorer processes.

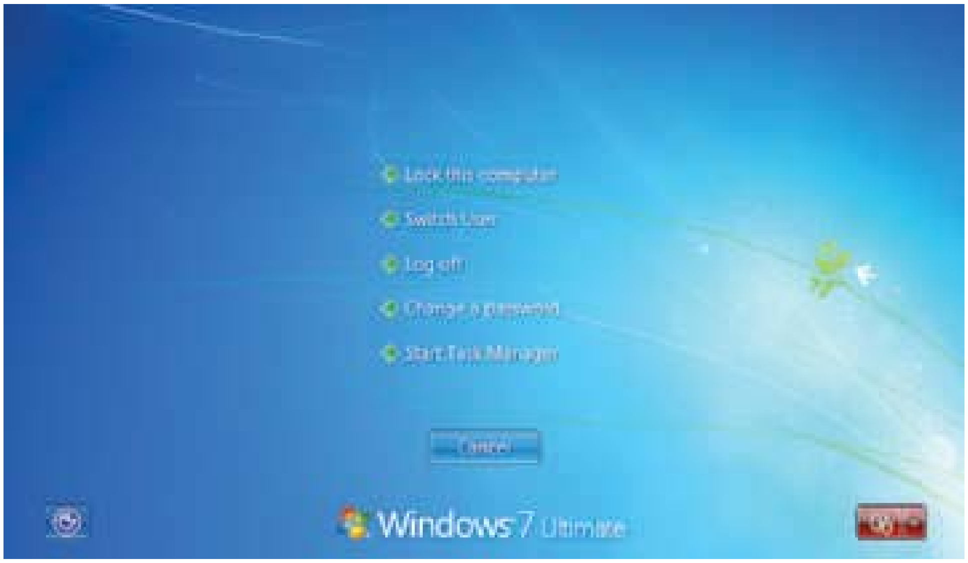
A+ Exam Tip The A+ 220-802 exam expects you to know how to use Task Manager, MSconfig, the Services console, Computer Management console, MMC, Event Viewer, Task Scheduler, the Registry Editor, and Performance Monitor. All these tools are covered in this part of the chapter.

Now that you are familiar with the concepts of how Windows works, let’s see how to use some tools that can help us manage Windows components and processes.

TASK MANAGER

Task Manager (Taskmgr.exe) lets you view the applications and processes running on your computer as well as information about process and memory performance, network activity, and user activity. Several ways to access Task Manager are:

- Press **Ctrl+Alt+Delete**. Depending on your system, the security screen (see Figure 11-3) or Task Manager appears. If the security screen appears, click **Start Task Manager**. This method works well when the system has a problem and is frozen.
- Right-click a blank area in the taskbar, and select **Start Task Manager** from the shortcut menu.
- Press **Ctrl+Shift+Esc**.
- Click **Start**, enter **taskmgr.exe** in the search box, and press **Enter**.

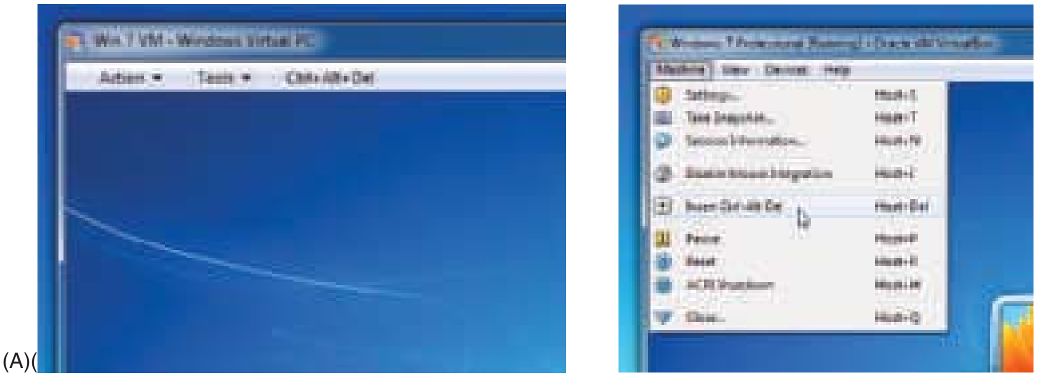


Source: Microsoft Windows 7

Figure 11-3 Use the security screen to launch Task Manager

Notes When working with a virtual machine, you cannot send the Ctrl+Alt+Delete keystrokes to the guest operating system in the VM because these keystrokes are always sent to the host operating system. To send the Ctrl+Alt+Delete keystrokes to a VM in Windows Virtual PC, click **Ctrl+Alt+Delete** in the VM menu bar (see Figure 11-4a). To send the Ctrl+Alt+Delete keystrokes to a VM in Oracle VirtualBox, click **Machine** and click **Insert Ctrl+Alt+Del** (see Figure 11-4b).

A+
220-802
1.4

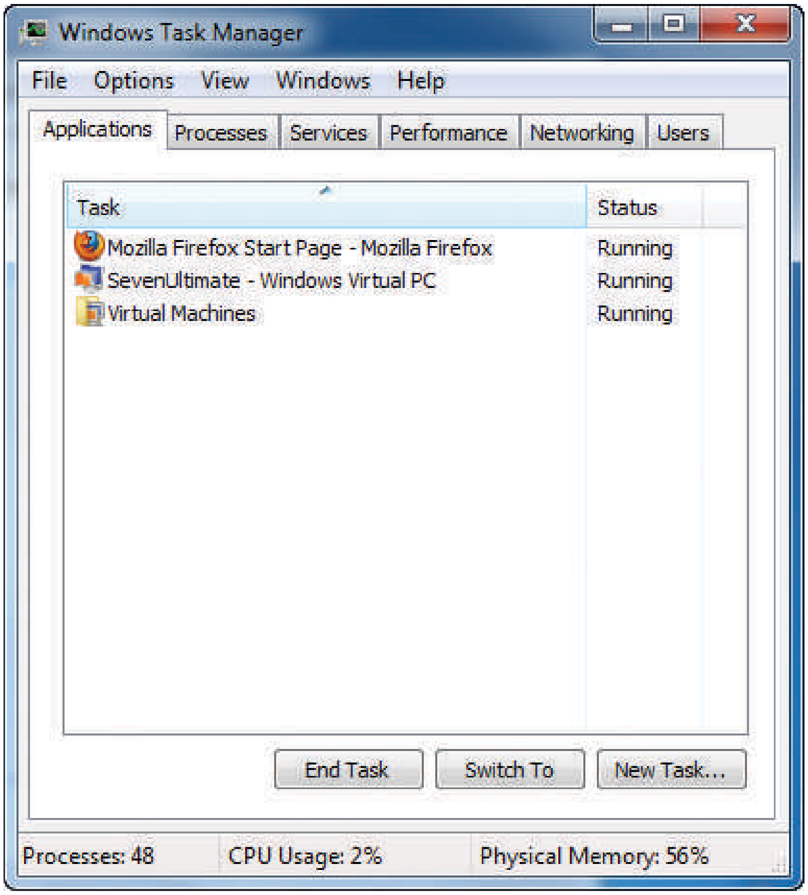


Source: Microsoft Virtual PC and Oracle VirtualBox

Source: Microsoft Virtual PC and Oracle VirtualBox

Figure 11-4 Send the Ctrl+Alt+Delete keystrokes to a VM managed by (a) Windows Virtual PC or (b) Oracle VirtualBox

Windows 7/Vista Task Manager has six tabs: Applications, Processes, Services, Performance, Networking, and Users (see Figure 11-5). Let's see how each tab of the Task Manager window works.



Windows Task Manager

File Options View Windows Help

Applications | Processes | Services | Performance | Networking | Users

Task	Status
Mozilla Firefox Start Page - Mozilla Firefox	Running
SevenUltimate - Windows Virtual PC	Running
Virtual Machines	Running

End Task | Switch To | New Task...

Processes: 48 CPU Usage: 2% Physical Memory: 56%

Source: Microsoft Windows 7

Figure 11-5 The Applications tab in Task Manager shows the status of active applications

11

APPLICATIONS TAB

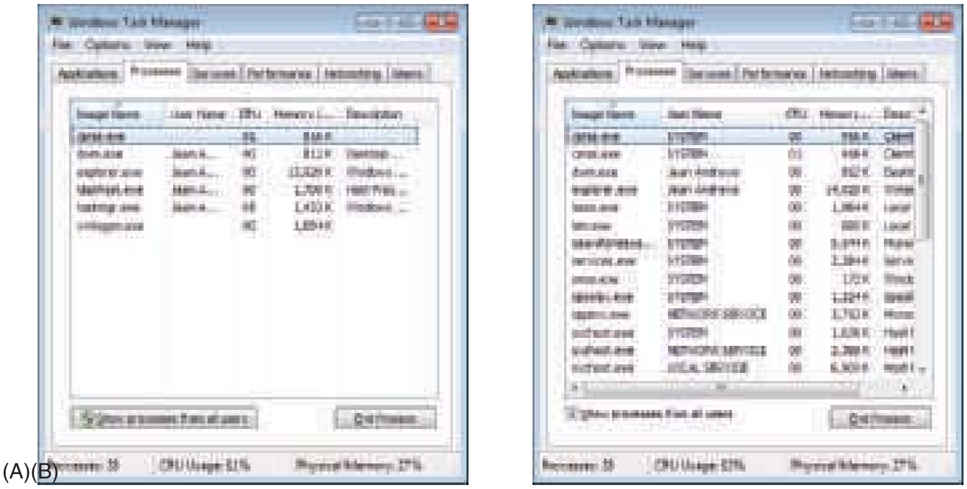
On the Applications tab shown in Figure 11-5, each application loaded can have one of two states: Running or Not Responding. If an application is listed as Not Responding, you can end it by selecting it and clicking the **End Task** button at the bottom of the window.

A+
220-802
1.4

The application will attempt a normal shutdown; if data has not been saved, you are given the opportunity to save it.

PROCESSES TAB

The Processes tab of Task Manager lists system services and other processes associated with applications, together with how much CPU time and memory the process uses. This information can help you determine which applications are slowing down your system. The Processes tab for Windows 7 Task Manager (see Figure 11-6a) shows the processes running under the current user. This screen shot was taken immediately after a Windows installation and before any applications were installed.


(A)(B)
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

Source: Microsoft Windows 7

Source: Microsoft Windows 7

Figure 11-6 Processes running under (a) the current user and (b) all users, for a new Windows 7 installation

To see all processes running, click **Show processes from all users** (see Figure 11-6b). Task Manager now shows processes running under the current user, System, Local Service, and Network Service accounts. Services running under these last three accounts cannot display a dialog box on-screen or interact with the user. To do that, the service must be running under a user account. Also, a service running under the System account has more core privileges than does a service running under another account.

To stop a process using Task Manager, select the process and click **End Process**. The process is ended abruptly. If the process belongs to an application, you will lose any unsaved information in the application. Therefore, if an application is hung, try using the Applications tab to end the task before turning to the Processes tab to end its underlying process.

If you want to end the process and all related processes, right-click the process and select **End Process Tree** from the shortcut menu. Be careful to not end critical Windows processes; ending these might crash your system.

Notes If your desktop locks up, you can use Task Manager to refresh it. To do so, press **Ctrl+Alt+Del** and then click **Start Task Manager**. Click the **Processes** tab. Select **Explorer.exe** (the process that provides the desktop) and then click **End Process**. Click **End process** in the warning box. Then click the **Applications** tab. Click **New Task**. Enter **Explorer.exe** in the Create New Task dialog box and click **OK**. Your desktop will be refreshed and any running programs will still be open.

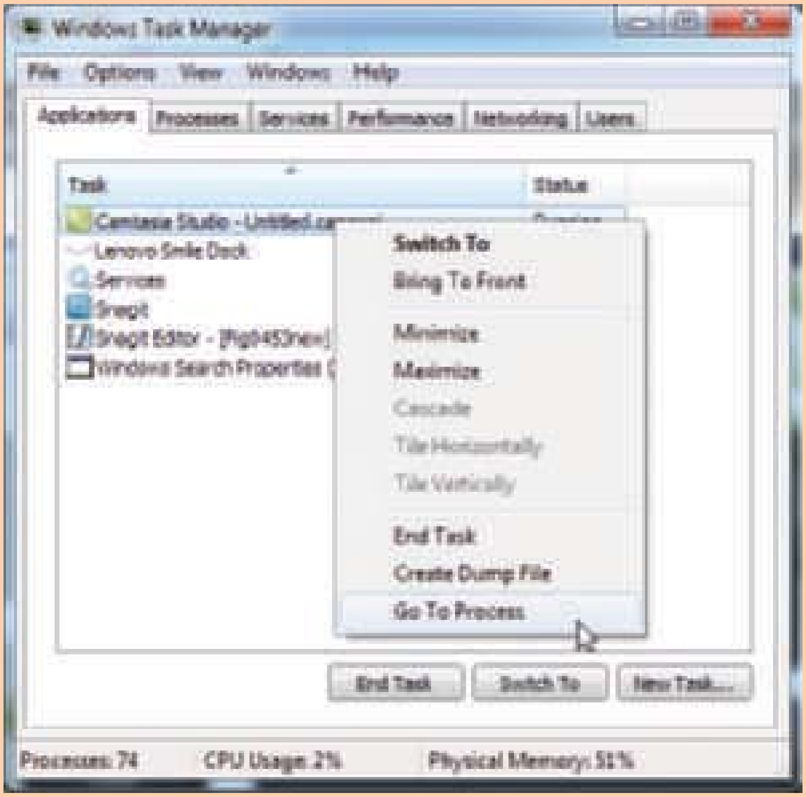
A+
220-802
1.4

APPLYING CONCEPTS ADJUST THE PRIORITY LEVEL OF AN APPLICATION

Each application running on your computer is assigned a priority level, which determines its position in the queue for CPU resources. You can use Task Manager to change the priority level for an application that is already loaded. If an application performs slowly, increase its priority. You should only do this with very important applications, because giving an application higher priority than certain background system processes can sometimes interfere with the operating system.

To use Task Manager to change the priority level of an open application, do the following:

1. In Task Manager, click the **Applications** tab. Right-click the application and select **Go To Process** from the shortcut menu (see Figure 11-7). The Processes tab is selected and the process that runs the application is selected.



Source: Microsoft Windows 7

Figure 11-7 Find the running process for this running application

2. Right-click the selected process. From the shortcut menu that appears, point to **Set Priority**, and set the new priority to **Above Normal** (see Figure 11-8). If that doesn't give satisfactory performance, then try **High**.

Notes Remember that any changes you make to an application's priority level affect only the current session.

A+
220-802
1.4

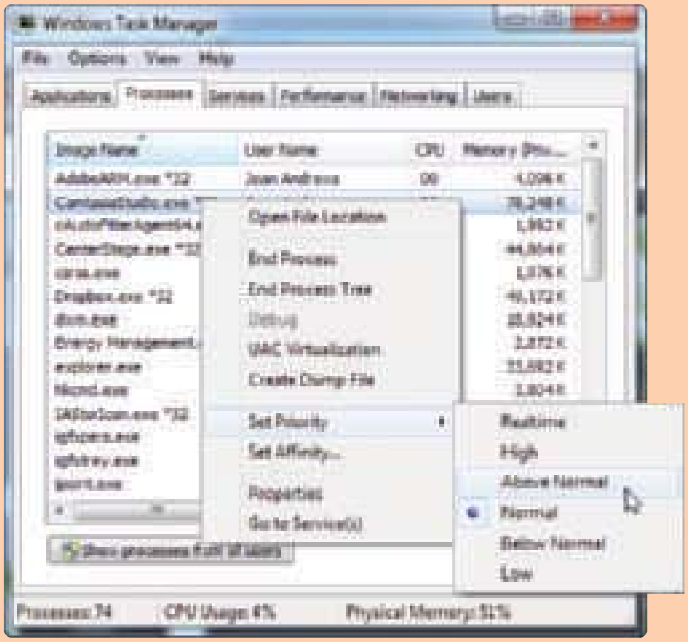


Image Name	User Name	CPU	Memory (Pri...
AdobeARM.exe *32	Joan Andrews	00	4,096 K
CamtasiaStudio.exe			78,248 K
cAudioFilterAgent64.e			1,992 K
CenterStage.exe *32			44,804 K
csrss.exe			1,376 K
Dropbox.exe *32			40,172 K
dwm.exe			18,824 K
Energy Management...			3,872 K
explorer.exe			33,492 K
hkcmd.exe			3,804 K
IAStorIcon.exe *32			
igfxpers.exe			
igfxtray.exe			
ipoint.exe			

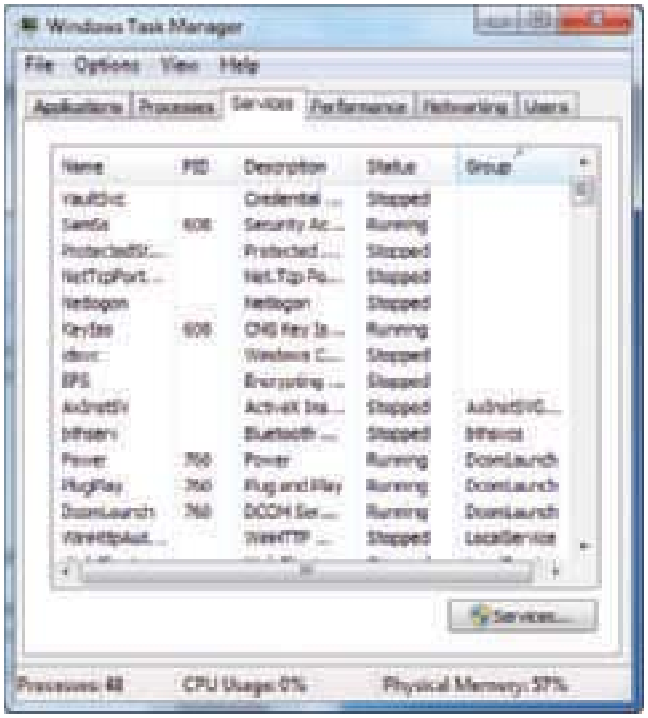
Processes: 74 CPU Usage: 4% Physical Memory: 51%

Source: Microsoft Windows 7

Figure 11-8 Change the priority level of a running application

SERVICES TAB

The third Task Manager tab, the Services tab, is shown in Figure 11-9. This tab lists the services currently installed along with the status of each service. Recall that a service is a program that runs in the background and is called on by other programs to perform a


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Services...

Name	PID	Description	Status	Group
VaultSvc		Credential ...	Stopped	
SamSs	608	Security Ac...	Running	
ProtectedSt...		Protected ...	Stopped	
NetTcpPort...		Net.Tcp Po...	Stopped	
Netlogon		Netlogon	Stopped	
KeyIso	608	CNG Key Is...	Running	
idsvc		Windows C...	Stopped	
EFS		Encrypting ...	Stopped	
AxInstSV		ActiveX Ins...	Stopped	AxInstSVG...
bthserv		Bluetooth ...	Stopped	bthsvcs
Power	760	Power	Running	DcomLaunch
PlugPlay	760	Plug and Play	Running	DcomLaunch
DcomLaunch	760	DCOM Ser...	Running	DcomLaunch
WinHttpAut...		WinHTTP ...	Stopped	LocalService

Processes: 48 CPU Usage: 0% Physical Memory: 57%

Source: Microsoft Windows 7

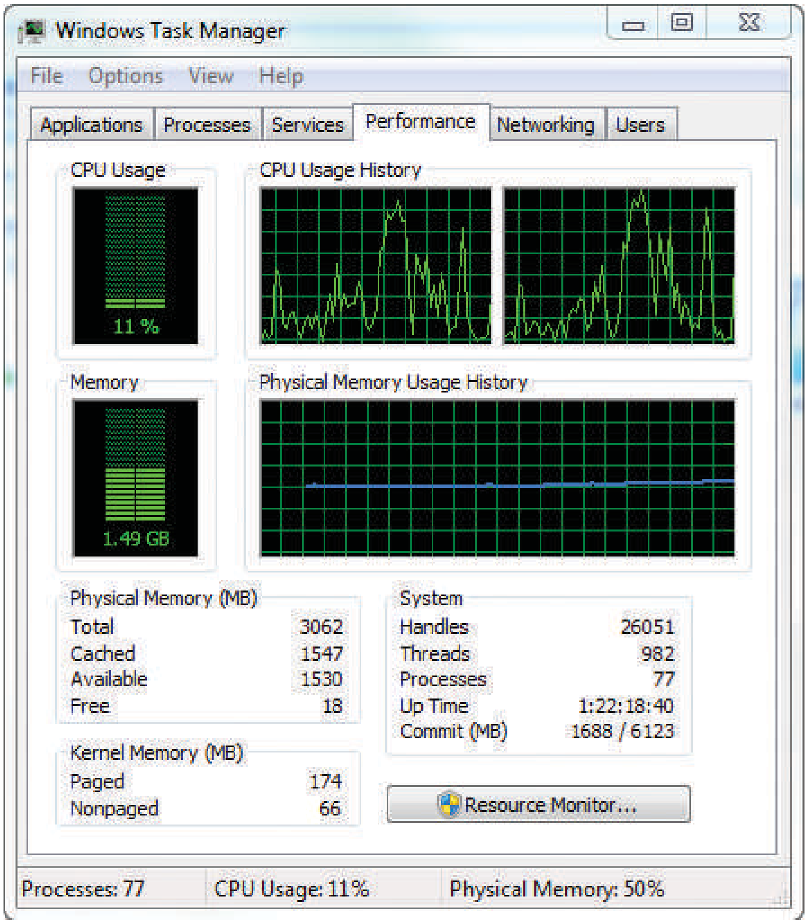
Figure 11-9 The Services tab of Windows 7 Task Manager gives the current status of all installed services

A+
220-802
1.4

background task. Running services are sometimes listed in the notification area of the taskbar. To manage a service, click the **Services** button at the bottom of the window to go to the Services console. How to use this console is discussed later in the chapter.

PERFORMANCE TAB

The fourth Task Manager tab, the Performance tab, is shown in Figure 11-10. It provides graphs that can give you a quick look at how system resources are used.



Physical Memory (MB)	
Total	3062
Cached	1547
Available	1530
Free	18

Kernel Memory (MB)	
Paged	174
Nonpaged	66

System	
Handles	26051
Threads	982
Processes	77
Up Time	1:22:18:40
Commit (MB)	1688 / 6123

Processes: 77 CPU Usage: 11% Physical Memory: 50%

Source: Microsoft Windows 7

Figure 11-10 The Performance tab window shows details about how system resources are being used

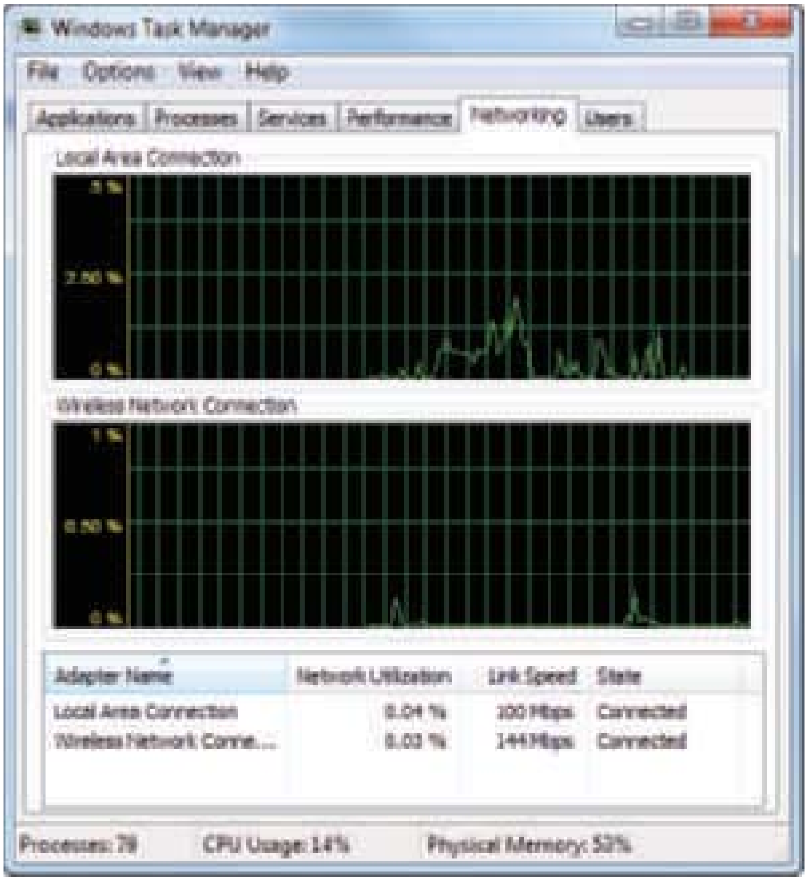
Here is an explanation of the information in the graphs on this tab:

- The *CPU Usage* graph indicates the percentage of time the CPU is currently being used. If the graph indicates heavy CPU use, you need to use other tools, such as the Resource Monitor, to investigate the program(s) hogging the CPU. How to use the Resource Monitor is covered later in the chapter.
- The *CPU Usage History* graphs show this same percentage of use over recent time.
- The left *Memory* graph shows the amount of memory currently used.
- The right *Physical Memory Usage History* graph shows how much memory has recently been used. If this blue bar is a flat line near the top of the graph, you definitely need to add more RAM to the system.

A+
220-802
1.4

NETWORKING TAB

The Networking tab lets you monitor network activity and bandwidth used. You can use it to see how heavily the network is being used by this computer. For example, in Figure 11-11, you can see that the wireless connection is running at 144 Mbps, while the local (wired) connection is running at 100 Mbps. The wired connection is slower than the wireless connection, but is used more because it is listed first. In Chapter 15, you learn how to change the order in which network connections are used.



Adapter Name	Network Utilization	Link Speed	State
Local Area Connection	0.04 %	100 Mbps	Connected
Wireless Network Conne...	0.03 %	144 Mbps	Connected

Processes: 78 CPU Usage: 14% Physical Memory: 52%

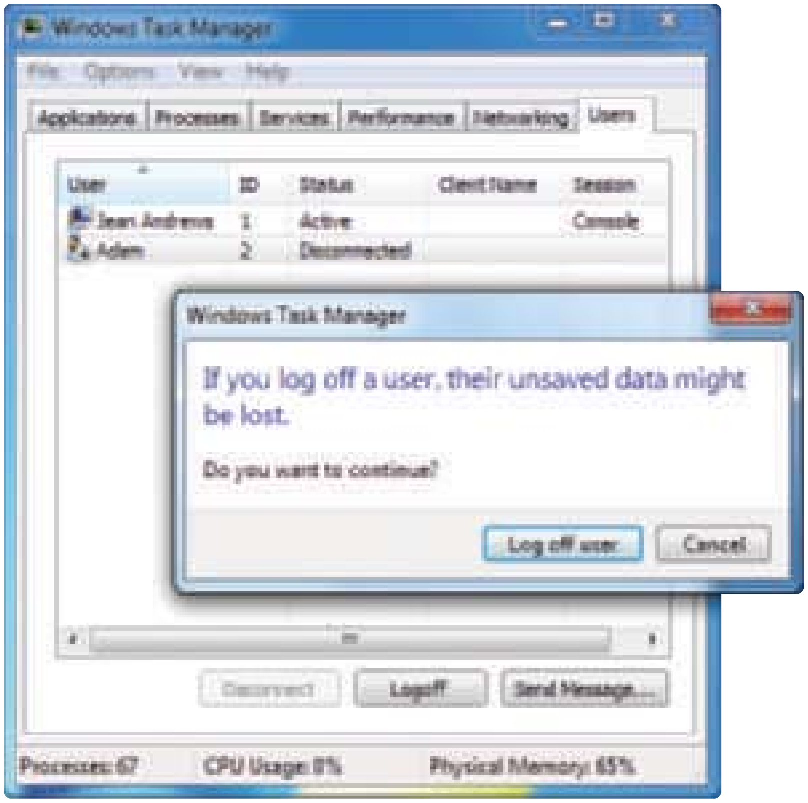
Source: Microsoft Windows 7

Figure 11-11 Use the Networking tab of Task Manager to monitor network activity

USERS TAB

The Users tab shows all users currently logged on to the system. To improve Windows performance or just before you shut down the system, you can log off a user. Before you log off another user, you can select the **Processes** tab and click **Show processes from all users** to verify no applications are running under that user account. Then return to the Users tab, select the user, and click **Logoff**. The dialog box shown in Figure 11-12 appears, warning that unsaved data might be lost. Click **Log off user** to complete the operation.

A+
220-802
1.4


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
User ID Status Client Name Session
Jean Andrews 1 Active Console
Adam 2 Disconnected
Disconnect Logoff Send Message...
Processes: 67 CPU Usage: 0% Physical Memory: 65%
Log off user Cancel

Windows Task Manager

If you log off a user, their unsaved data might be lost.

Do you want to continue?

Source: Microsoft Windows 7

Figure 11-12 Use Task Manager to log off a user

Hands-on Project 11-1 Research Running Processes

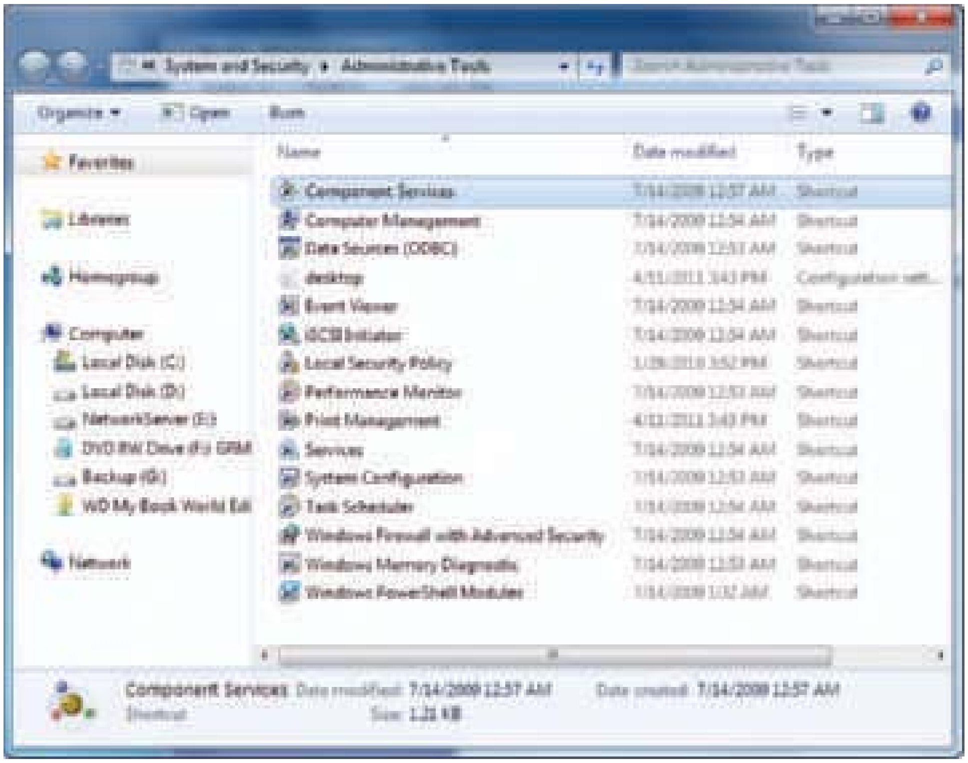
Boot to the Windows desktop and then use Task Manager to get a list of all the running processes on your machine. Use the Windows Snipping Tool to save and print the Task Manager screens showing the list of processes. Next, boot the system in Safe Mode with Networking and use Task Manager to list running processes. (Recall you can press F8 during startup to see the Advanced Boot Options menu from which you can start Windows in Safe Mode with Networking.) Which processes that were loaded normally are not loaded when the system is running in Safe Mode?

A+
220-802
1.1, 1.4

ADMINISTRATIVE TOOLS

Windows offers a group of Administrative tools in the Control Panel that are used by technicians and developers to support Windows. To see the list of tools, open Control Panel and then click **Administrative Tools**. Figure 11-13 shows the Administrative Tools window for Windows 7 Ultimate. The Home editions of Windows 7 do not include the Local Security Policy (controls many security settings on the local computer) or Print Management (manages print servers on a network).

A+
220-802
1.1, 1.4



Name	Date modified	Type
Component Services	7/14/2009 12:57 AM	Shortcut
Computer Management	7/14/2009 12:54 AM	Shortcut
Data Sources (ODBC)	7/14/2009 12:53 AM	Shortcut
desktop	4/11/2011 3:43 PM	Configuration sett...
Event Viewer	7/14/2009 12:54 AM	Shortcut
iSCSI Initiator	7/14/2009 12:54 AM	Shortcut
Local Security Policy	1/28/2010 3:52 PM	Shortcut
Performance Monitor	7/14/2009 12:53 AM	Shortcut
Print Management	4/11/2011 3:43 PM	Shortcut
Services	7/14/2009 12:54 AM	Shortcut
System Configuration	7/14/2009 12:53 AM	Shortcut
Task Scheduler	7/14/2009 12:54 AM	Shortcut
Windows Firewall with Advanced Security	7/14/2009 12:54 AM	Shortcut
Windows Memory Diagnostic	7/14/2009 12:53 AM	Shortcut
Windows PowerShell Modules	7/14/2009 1:32 AM	Shortcut

Component Services Date modified: 7/14/2009 12:57 AM Date created: 7/14/2009 12:57 AM
Shortcut Size: 1.21 KB

Source: Microsoft Windows 7

Figure 11-13 Administrative tools available in Windows 7 Ultimate

Several Administrative tools are covered next, including System Configuration, Services console, Computer Management, and Event Viewer. In Chapter 12, you learn to use more Administrative tools.

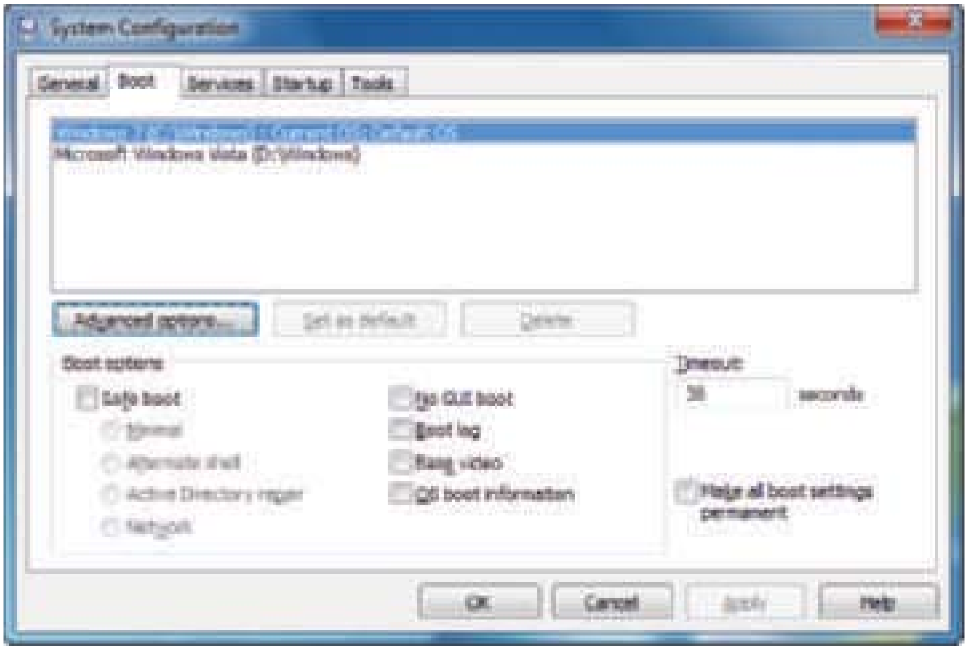
SYSTEM CONFIGURATION (MSCONFIG)

You can use the System Configuration (Msconfig.exe) utility, which is commonly pronounced "*M-S-config*," to find out what processes are launched at startup and to temporarily disable a process from loading.

Using MSconfig should be a temporary fix to disable a program or service from launching at startup, but it should not be considered a permanent fix. Once you've decided you want to make the change permanent, use other methods to permanently remove that process from Windows startup. For example, you might uninstall a program, remove it from a startup folder, or use the Services console to disable a service. Follow these steps to learn to use MSconfig:

1. To start MSconfig, click **Start**, enter **msconfig.exe** in the search box, and press **Enter**. The System Configuration box opens. Click the **Boot** tab to see information about the boot and control some boot settings. For example, in Figure 11-14, you can see this computer is set for a dual boot and, using this box, you can delete one of the choices for a dual boot from the boot loader menu.
2. Click the **Services** tab to see a list of all services launched at startup (see Figure 11-15). Notice that this tab has a Disable all button. If you use this button, you'll disable all nonessential Windows services as well as third-party services such as virus scan

A+
220-802
1.1, 1.4



System Configuration

General | Boot | Services | Startup | Tools

Windows 7 (C:\Windows) : Current OS; Default OS
Microsoft Windows Vista (D:\Windows)

Advanced options... | Set as default | Delete

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

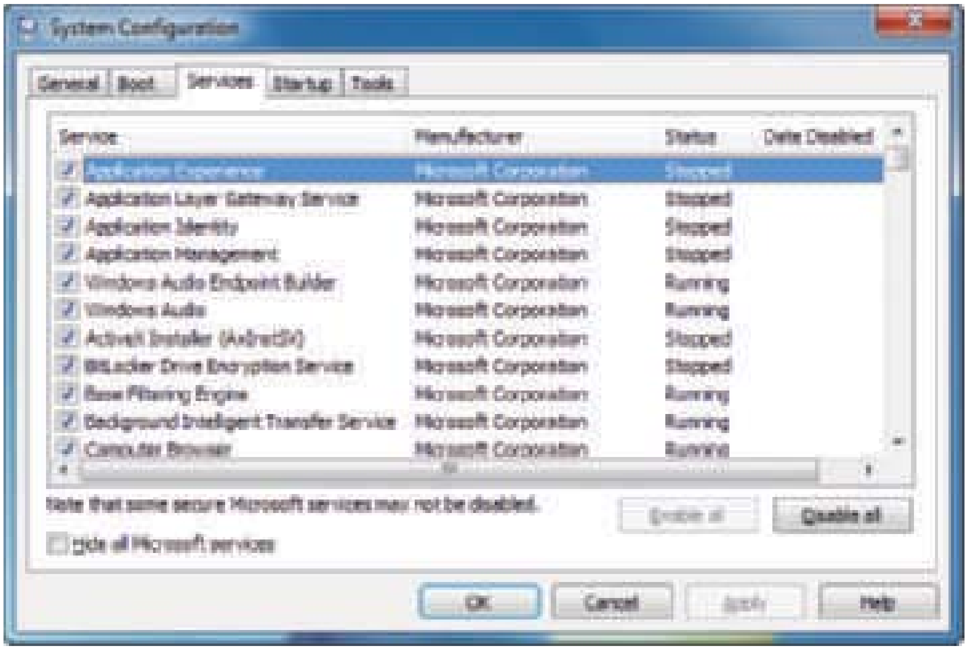
OK | Cancel | Apply | Help

Source: Microsoft Windows 7

Figure 11-14 Use the Boot tab to control boot settings

11

programs. Use it only for the most difficult Windows problems, because you'll disable some services that you might really want, such as Windows Task Scheduler, Print Spooler, Automatic Updates, and the System Restore service.



System Configuration

General | Boot | Services | Startup | Tools

Service	Manufacturer	Status	Date Disabled
☑ Application Experience	Microsoft Corporation	Stopped	
☑ Application Layer Gateway Service	Microsoft Corporation	Stopped	
☑ Application Identity	Microsoft Corporation	Stopped	
☑ Application Management	Microsoft Corporation	Stopped	
☑ Windows Audio Endpoint Builder	Microsoft Corporation	Running	
☑ Windows Audio	Microsoft Corporation	Running	
☑ ActiveX Installer (AxInstSV)	Microsoft Corporation	Stopped	
☑ BitLocker Drive Encryption Service	Microsoft Corporation	Stopped	
☑ Base Filtering Engine	Microsoft Corporation	Running	
☑ Background Intelligent Transfer Service	Microsoft Corporation	Running	
☑ Computer Browser	Microsoft Corporation	Running	

Note that some secure Microsoft services may not be disabled.

Enable all | Disable all

□ Hide all Microsoft services

OK | Cancel | Apply | Help

Source: Microsoft Windows 7

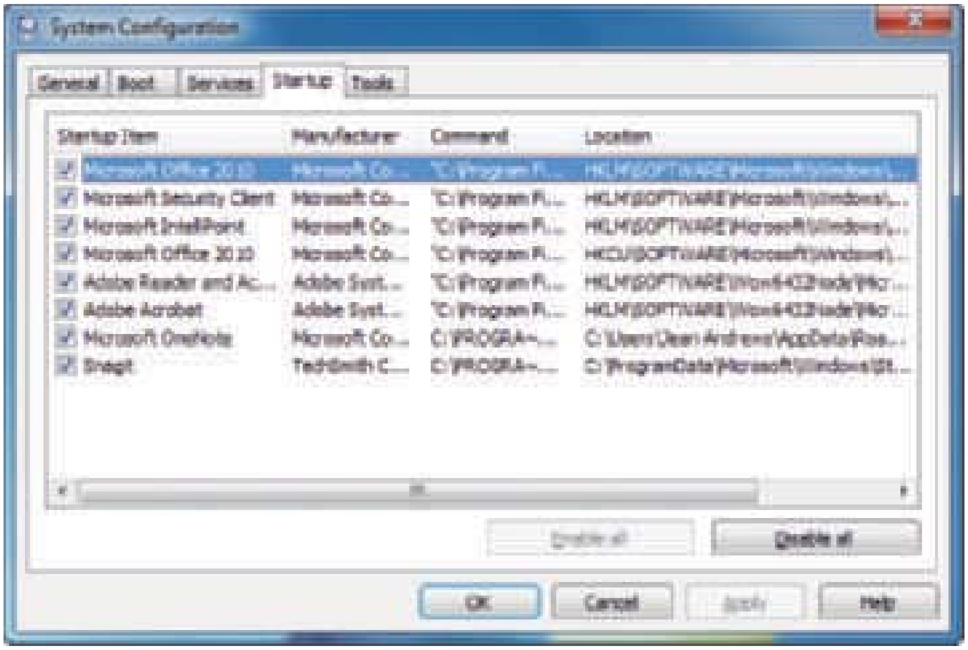
Figure 11-15 Use MSconfig to view and control services launched at startup

3. To view only those services put there by third-party software, check **Hide all Microsoft services**. If you have antivirus software running in the background (and you should), you'll see that listed as well as any service launched at startup and put there

A+
220-802
1.1, 1.4

by installed software. Uncheck all services you don't want. If you don't recognize a service, try entering its name in a search string at *www.google.com* for information about the program. If the program is a service, you can permanently stop it by using the Services console or uninstalling the software.

4. Click the **Startup** tab to see a list of programs that launch at startup (see Figure 11-16). These programs launch at startup by way of a startup folder or a registry key entry. To disable all nonessential startup tasks, click **Disable all**. Or you can check and uncheck an individual startup program to enable or disable it. The Startup tab can be useful when trying to understand how a program is launched at startup because it offers the Location column. This column shows the registry key or startup folder where the startup entry is made.



Startup Item	Manufacturer	Command	Location
☑ Microsoft Office 2010	Microsoft Co...	"C:\Program Fi...	HKLM\SOFTWARE\Microsoft\Windows\...
☑ Microsoft Security Client	Microsoft Co...	"C:\Program Fi...	HKLM\SOFTWARE\Microsoft\Windows\...
☑ Microsoft IntelliPoint	Microsoft Co...	"C:\Program Fi...	HKLM\SOFTWARE\Microsoft\Windows\...
☑ Microsoft Office 2010	Microsoft Co...	"C:\Program Fi...	HKCU\SOFTWARE\Microsoft\Windows\...
☑ Adobe Reader and Ac...	Adobe Syst...	"C:\Program Fi...	HKLM\SOFTWARE\Wow6432Node\Micr...
☑ Adobe Acrobat	Adobe Syst...	"C:\Program Fi...	HKLM\SOFTWARE\Wow6432Node\Micr...
☑ Microsoft OneNote	Microsoft Co...	C:\PROGRA~...	C:\Users\Jean Andrews\AppData\Roa...
☑ Snagit	TechSmith C...	C:\PROGRA~...	C:\ProgramData\Microsoft\Windows\St...

Source: Microsoft Windows 7

Figure 11-16 Select startup processes to enable or disable

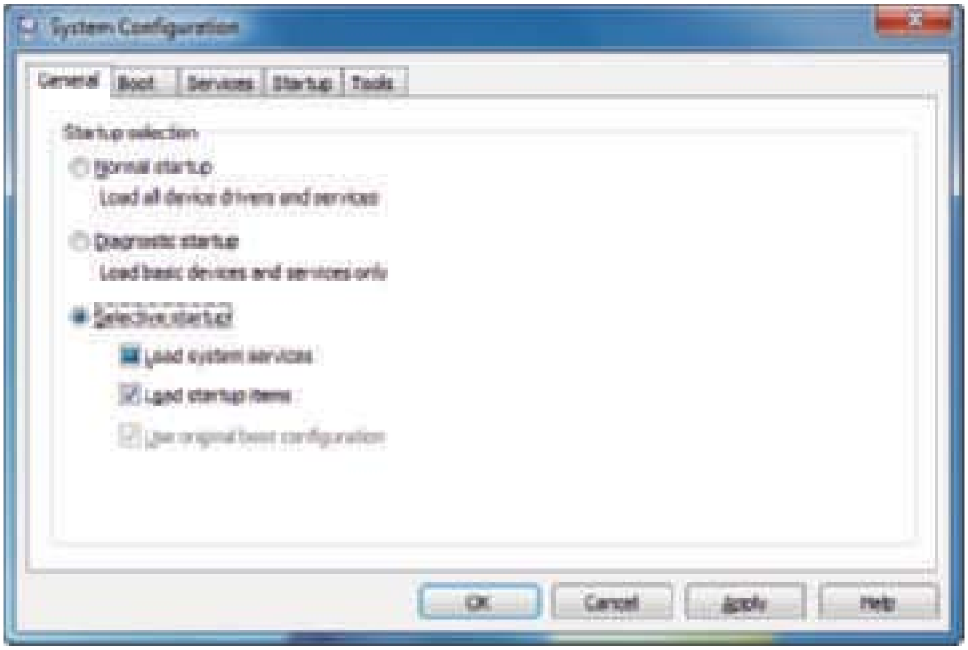
> **Notes** When using MSconfig to troubleshoot startup problems, keep a handwritten list of programs you enable or disable so you can backtrack, if necessary.

5. If you made changes, click **Apply**. Now click the **General** tab and you should see *Selective startup* selected, as shown in Figure 11-17. Close the MSconfig box and restart the computer.

6. Watch for error messages during or after the boot that indicate you've created a problem with your changes. For instance, after the boot, you might find out you can no longer use that nifty little utility that came with your digital camera. To fix the problem, you need to find out which service or program you stopped that you need for that utility. Go back to the MSconfig tool and enable that one service and reboot.

The Tools tab in the System Configuration box gives you quick access to other Windows tools you might need during a troubleshooting session (see Figure 11-18).

A+
220-802
1.1, 1.4



Startup selection

○ Normal startup
Load all device drivers and services

○ Diagnostic startup
Load basic devices and services only

● Selective startup

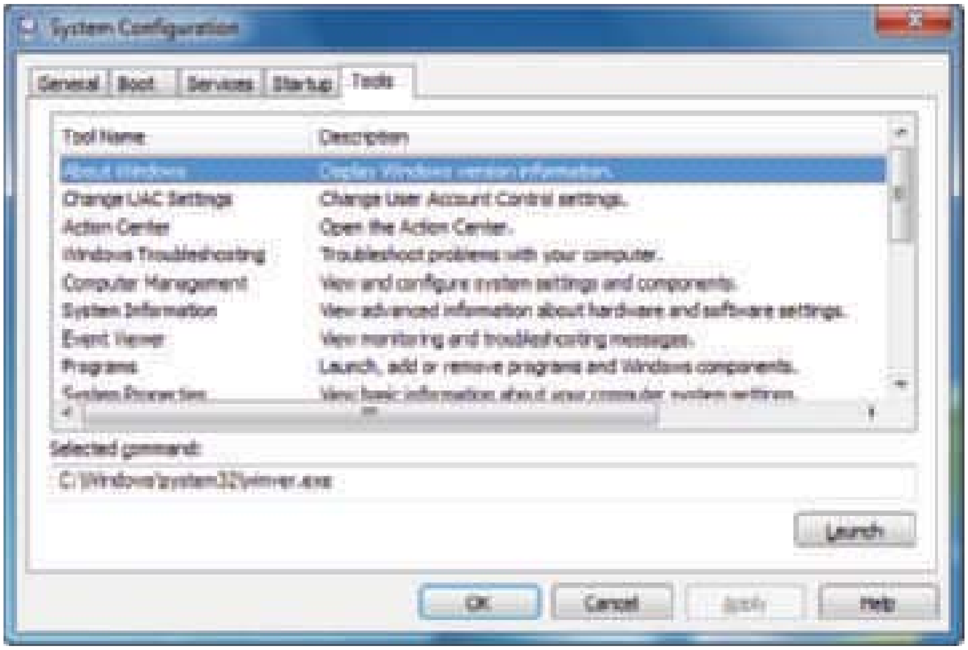
■ Load system services

☑ Load startup items

☑ Use original boot configuration

Source: Microsoft Windows 7

Figure 11-17 MSconfig is set to control the Windows startup programs



Tool Name	Description
About Windows	Display Windows version information.
Change UAC Settings	Change User Account Control settings.
Action Center	Open the Action Center.
Windows Troubleshooting	Troubleshoot problems with your computer.
Computer Management	View and configure system settings and components.
System Information	View advanced information about hardware and software settings.
Event Viewer	View monitoring and troubleshooting messages.
Programs	Launch, add or remove programs and Windows components.
System Properties	View basic information about your computer system settings.

Selected command:

C:\Windows\system32\winver.exe

Source: Microsoft Windows 7

Figure 11-18 The Tools tab makes it easy to find troubleshooting tools

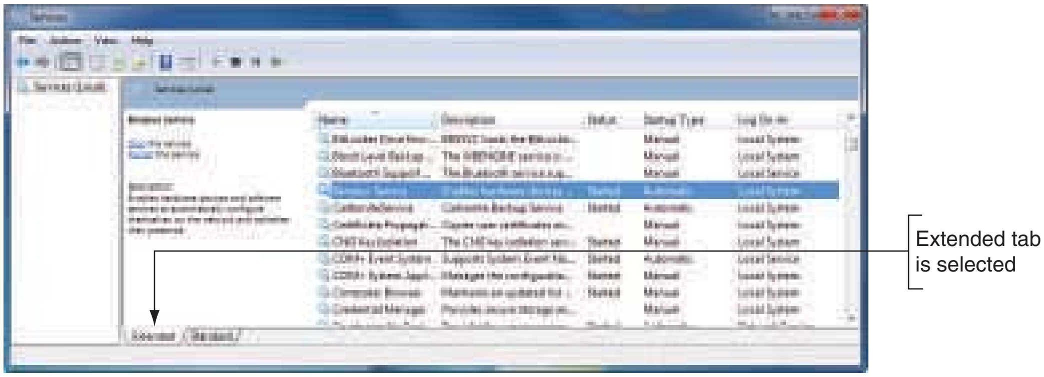
Notes MSconfig reports only what it is programmed to look for when listing startup programs and services. It looks only in certain registry keys and startup folders, and sometimes MSconfig does not report a startup process. Therefore, don't consider its list of startup processes to be complete.

Vista Differences Windows Vista uses the System Configuration utility to control startup programs just as does Windows 7. In addition, Vista offers Software Explorer, a user-friendly tool to control startup programs. To learn how to use Software Explorer, see Appendix B.

A+
220-802
1.1, 1.4

SERVICES CONSOLE

The Services console (the program file is services.msc) is used to control the Windows and third-party services installed on a system. To launch the Services console, type **Services.msc** in the search box and press **Enter**. If the Extended tab at the bottom of the window is not selected, click it (see Figure 11-19). This tab gives a description of a selected service.

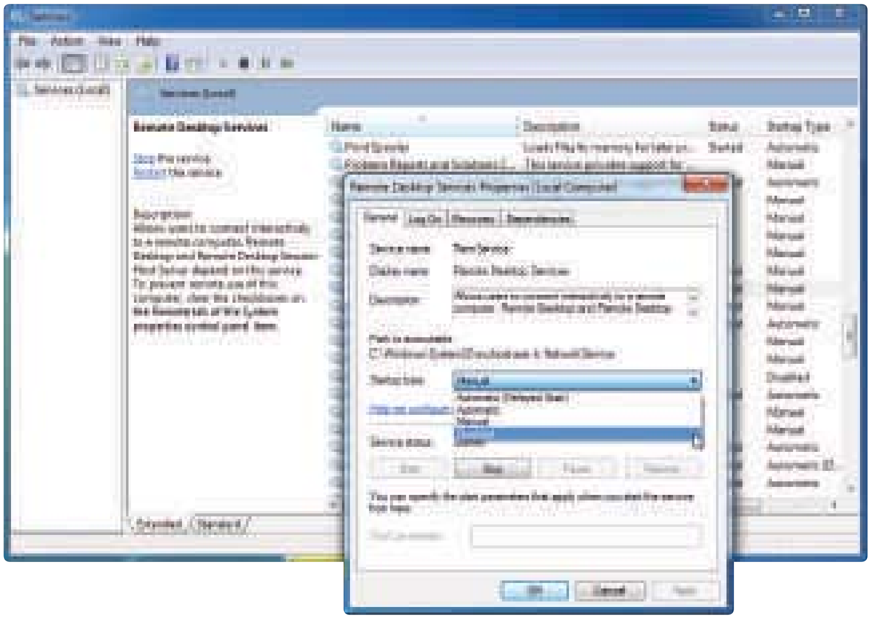


Source: Microsoft Windows 7

Figure 11-19 The Services console is used to manage Windows Services

When you click a service to select it and the description is missing, most likely the service is a third-party service put there by an installed application. To get more information about a service or to stop or start a service, right-click its name and select **Properties** from the shortcut menu. In the Properties box (see Figure 11-20), the startup types for a service are:

- *Automatic (Delayed Start).* Starts shortly after startup, after the user logs on, so as not to slow down the startup process
- *Automatic.* Starts when Windows loads
- *Manual.* Starts as needed
- *Disabled.* Cannot be started



Source: Microsoft Windows 7

Figure 11-20 Manage a service with the service Properties box

A+
220-802
1.1, 1.4

Notes If you suspect a Windows system service is causing a problem, you can use MSconfig to disable the service. If this works, then try replacing the service file with a fresh copy from the Windows setup DVD.

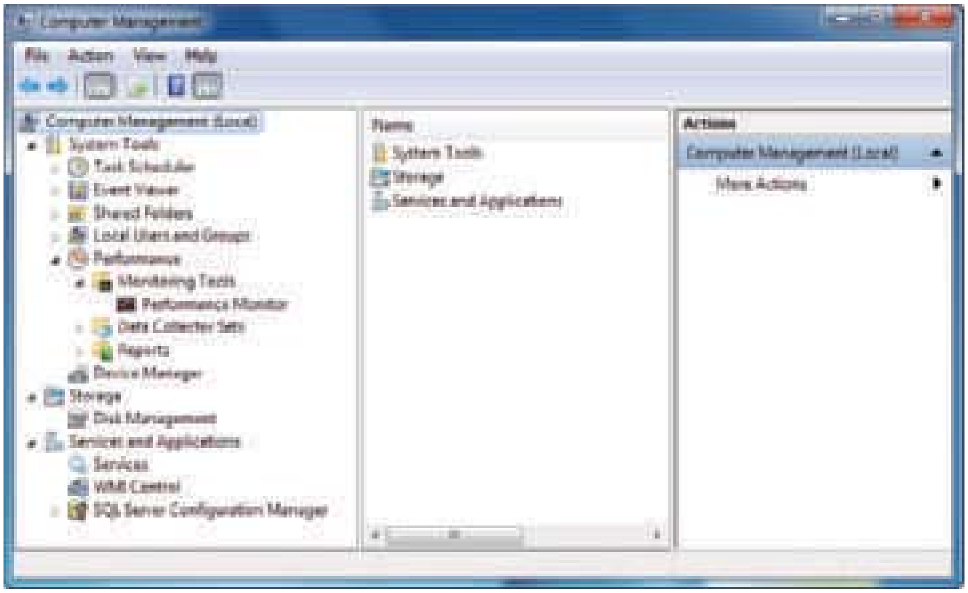
COMPUTER MANAGEMENT

Computer Management (Compmgmt.msc) contains several tools that can be used to manage the local PC or other computers on the network. The window is called a console because it consolidates several Windows administrative tools. To use most of these tools, you must be logged on as an administrator, although you can view certain settings in Computer Management if you are logged on with lesser privileges.

As with most Windows tools, there are several ways to access Computer Management:

- Click **Start**, enter **Computer Management** or **compmgmt.msc** in the search box, and press **Enter**.
- Click **Start**, right-click **Computer,** and select **Manage** from the shortcut menu.
- In Control Panel, look in the **Administrative Tools** group.

The Computer Management window is shown in Figure 11-21. Using this window, you can access Task Scheduler, Event Viewer, performance monitoring tools including the Windows 7 Performance Monitor and the Vista Reliability and Performance Monitor, Device Manager, Disk Management, and the Services console. You can also manage user accounts and user groups (covered in Chapter 17). Several tools available from the Computer Management window are covered in this chapter.



Source: Microsoft Windows 7

Figure 11-21 Windows Computer Management combines several administrative tools into a single easy-to-access window

MICROSOFT MANAGEMENT CONSOLE (MMC)

Microsoft Management Console (MMC; the program file is mmc.exe) is a Windows utility that can be used to build your own customized console windows. In a console, these individual tools are called snap-ins. A console is saved in a file with an .msc file extension, and a

A+
220-802
1.1, 1.4

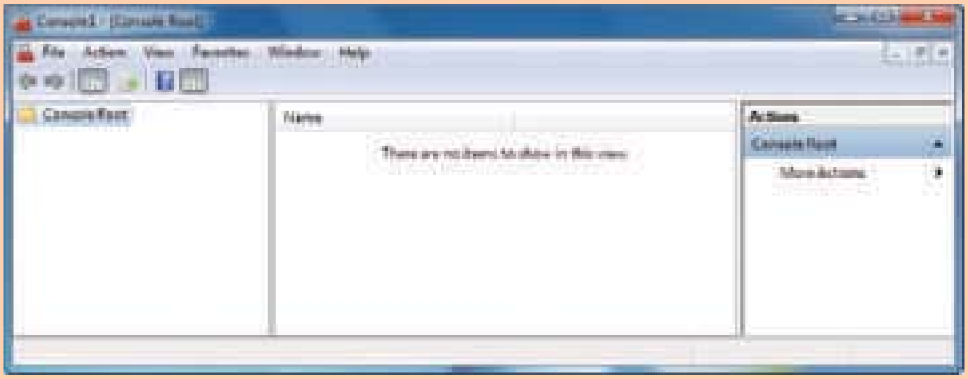
snap-in in a console can itself be a console. To use all the functions of MMC, you must be logged on with administrator privileges.

Notes A program that can work as a snap-in under the MMC has an .msc file extension.

APPLYING CONCEPTS CREATE A CONSOLE

If you find yourself often using a few Windows tools, consider putting them in a console stored on your desktop. Follow these steps to create a console:

1. Click **Start**, enter **mmc.exe** in the search box, and press **Enter**. Respond to the UAC box. An empty console window appears, as shown in Figure 11-22.

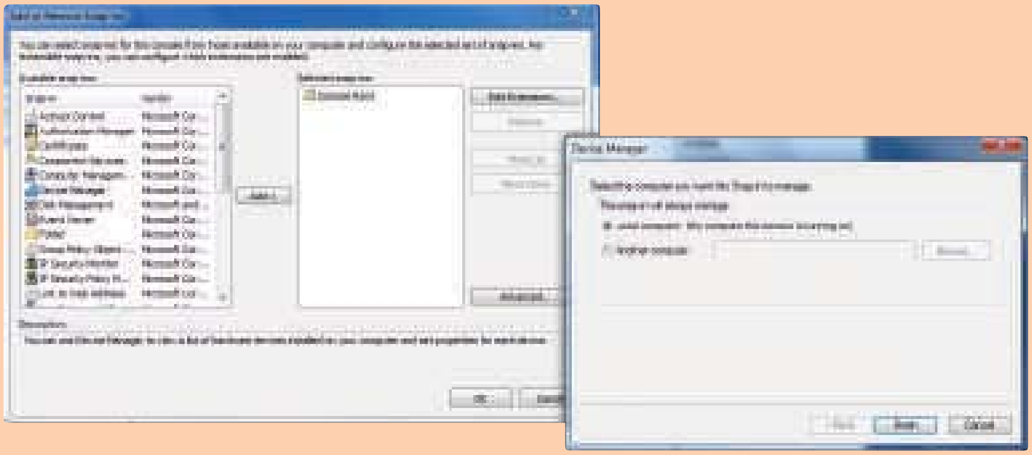


There are no items to show in this view.

Source: Microsoft Windows 7

Figure 11-22 An empty console

2. Click **File** in the menu bar and then click **Add/Remove Snap-in**. The Add or Remove Snap-ins box opens, as shown on the left side of Figure 11-23.



Source: Microsoft Windows 7

Figure 11-23 Add a snap-in to the new console

A+
220-802
1.1, 1.4

3. Select a snap-in from the list in the Add or Remove Snap-ins box. Notice a description of the snap-in appears at the bottom of the window. The snap-ins that appear in this list depend on the edition of Windows 7/Vista you have installed and what other components are installed on the system. Click **Add** to add the snap-in to the console. (For Windows XP, in the Add/Remove Snap-In box, click **Add**. A list of snap-ins appears. Select one and click **Add**.)

4. If parameters for the snap-in need defining, a dialog box opens that allows you to set up these parameters. The dialog box offers different selections, depending on the snap-in being added. For example, when Device Manager is selected, a dialog box appears, asking you to select the computer that Device Manager will monitor (see the right side of Figure 11-23). Select **Local computer (the computer this console is running on)** and click **Finish**. The snap-in now appears in the list of snap-ins for this console.

5. Repeat Steps 3 and 4 to add all the snap-ins that you want to the console. When you finish, click **OK** in the Add or Remove Snap-ins box.

6. To save the console, click **File** in the menu bar and then click **Save As**. The Save As dialog box opens.

7. The default location for the console file is C:\Users\username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools. However, you can save the console to any location, such as the Windows desktop. However, if you save the file to its default location, the console will appear as an option under Administrative Tools in the Start menu. Select the location for the file, name the file, and click **Save**. Then close the console window.

Notes After you create a console, you can copy the .msc file to any computer or place a shortcut to it on the desktop.

Hands-on Project 11-2 Use the Microsoft Management Console

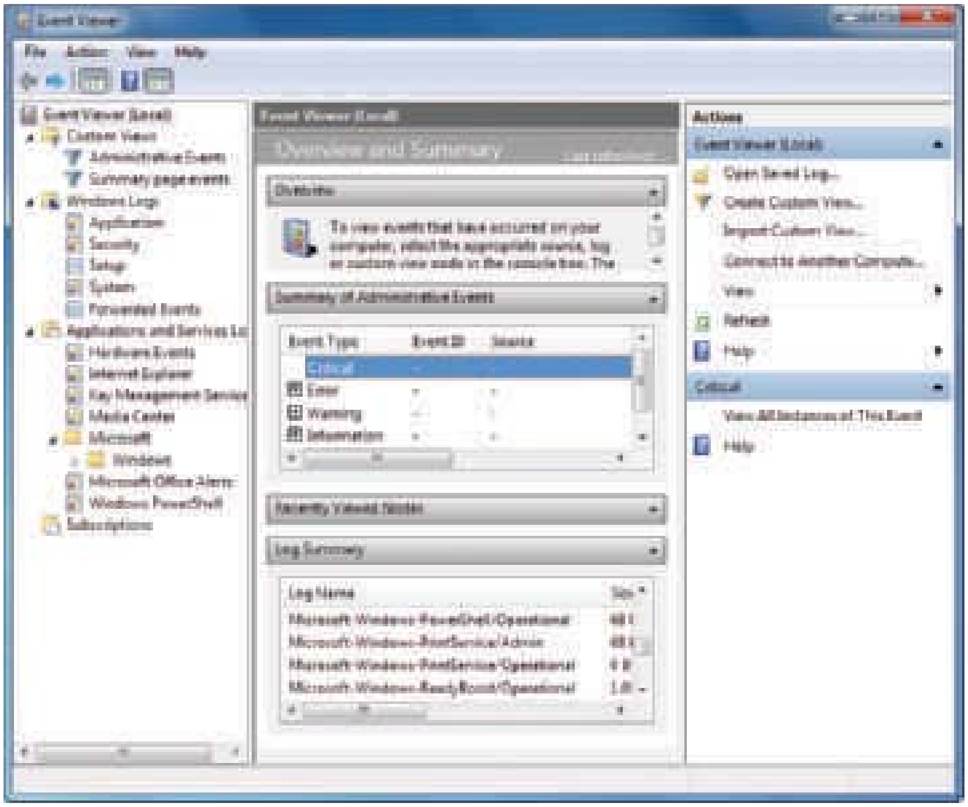
Using the Microsoft Management Console, create a customized console. Put two snap-ins in the console: Device Manager and Event Viewer. Store a shortcut to your console on the Windows desktop. Copy the console to another computer and install it on the Windows desktop.

EVENT VIEWER

Just about anything that happens in Windows is logged by Windows, and these logs can be viewed using Event Viewer (Eventvwr.msc). You can find events such as a hardware or network failure, OS error messages, a device or service that has failed to start, or General Protection Faults.

Event Viewer is a Computer Management console snap-in, and you can open it by using the Computer Management window, by entering **Event Viewer** or **Eventvwr.msc** in the search box, or by using the Administrative Tools group in Control Panel. The Windows 7/Vista Event Viewer window is shown in Figure 11-24. The XP Event Viewer is shown in Figure 11-25. The XP Event Viewer does not keep as many logs as does the Windows 7/Vista Event Viewer.

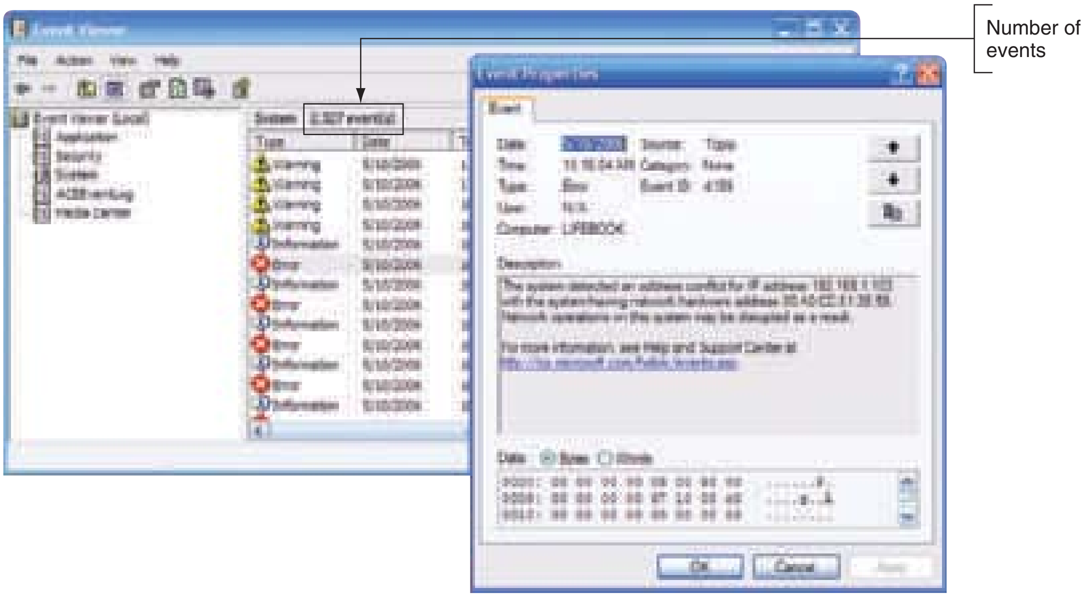
A+
220-802
1.1, 1.4



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The

Source: Microsoft Windows 7

Figure 11-24 Use Event Viewer to see logs about hardware, Windows, security, and applications events



The system detected an address conflict for IP address 192.168.1.102 with the system having network hardware address 00-40-CA-51-38-9B. Network operations on this system may be disrupted as a result.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

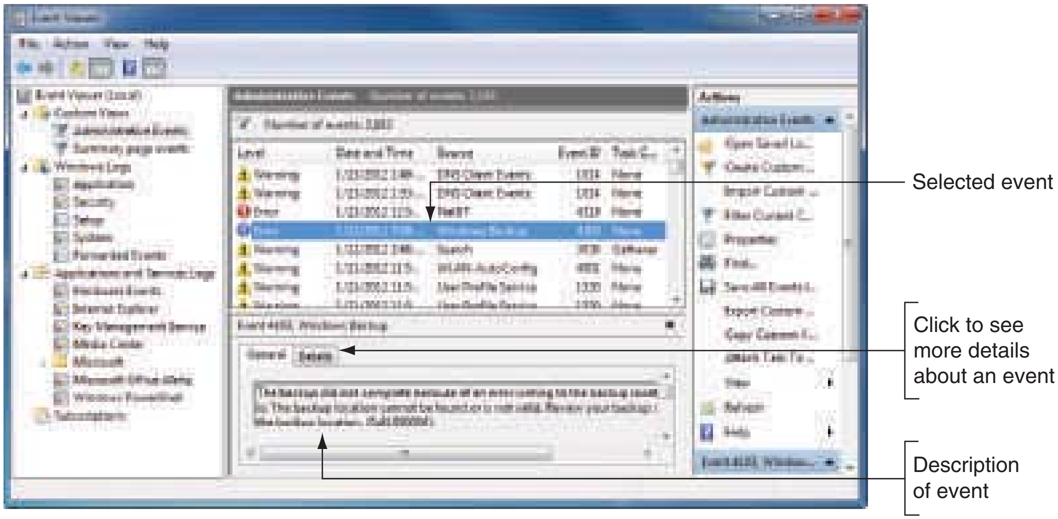
Source: Microsoft Windows 7

Figure 11-25 Event Viewer in Windows XP works about the same way as the Windows 7/Vista Event Viewer

The different views of logs are listed in the left pane, and you can drill down into subcategories of these logs. You can filter and sort logs to help find what you need. First select a log in the left pane and then click an event in the middle pane to see details about

A+
220-802
1.1, 1.4

the event. For example, in Figure 11-26, the Administrative Events log shows an event recorded by Windows Backup.



Source: Microsoft Windows 7

Figure 11-26 Click an event to see details about the event

Three main types of events are Error, Warning, and Information. Error events are the most important and indicate something went wrong with the system, such as a scheduled backup failed to work. Warning events indicate failure might occur in the future.

Here are the views of logs that are the most useful:

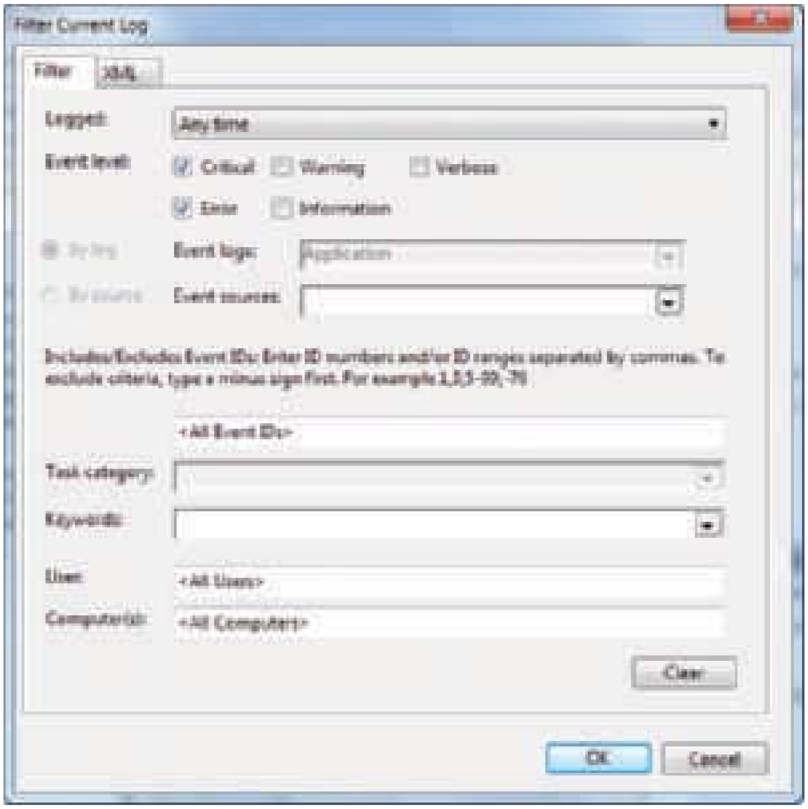
- ***Administrative Events log.*** This log is a filtered log that shows only Warning and Error events intended for the administrator. This log is in the Custom Views category and is selected in Figure 11-26.
- ***Application log.*** In the Windows Logs group, look in the Application log for events recorded by an application. This log might help you identify why an application is causing problems.
- ***Security log.*** Events in the Security log are called audits and include successful and unsuccessful logins to a user account and attempts from another computer on the network to access shared resources on this computer.
- ***Setup log.*** Look in the Setup log for events recorded when applications are installed.
- ***System log.*** Look in the System log to find events triggered by Windows components, such as a device driver failing to load or a problem with hardware.
- ***Forwarded Events log.*** This log receives events that were recorded on other computers and sent to this computer.

When you first encounter a Windows, hardware, application, or security problem, get in the habit of checking Event Viewer as one of your first steps toward investigating the problem. To save time, first check the Administrative Events log because it filters out all events except Warning and Error events.

If you want to create your own filtered events log, right-click any log in the left pane and select **Filter Current Log** from the shortcut menu. (For Windows XP, select **Properties** from the shortcut menu and then click the **Filter** tab.) The Filter Current Log box appears (see Figure 11-27).

The Filter Current Log box offers many ways to filter events. To view the most significant events to troubleshoot a problem, check **Critical** and **Error** under the Event level, as shown in Figure 11-27. Critical events are those errors that Windows believes are affecting critical

A+
220-802
1.1, 1.4


Filter Current Log

Filter | XML

Logged: Any time

Event level: ☑ Critical ☐ Warning ☐ Verbose

☑ Error ☐ Information

● By log Event logs: Application

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Figure 11-27 Criteria to filter events in Event Viewer

Source: Microsoft Windows 7

Windows processes. After you select the filters, click **OK**. Only the events that match your filters are listed. To remove the filter, right-click the log and select **Clear Filter**.

Besides filtering a log, here are other useful tips when dealing with logs:

- To sort a list of events, click a column heading in the middle pane.
- To save a filtered log file so you can view it later, right-click the log and select **Save Filtered Log File As** (see Figure 11-28). The log file is assigned an .evtx file extension. When you later double-click this file, it appears in an Event Viewer window. You might want to email a filtered log file to others who are helping you troubleshoot a problem.

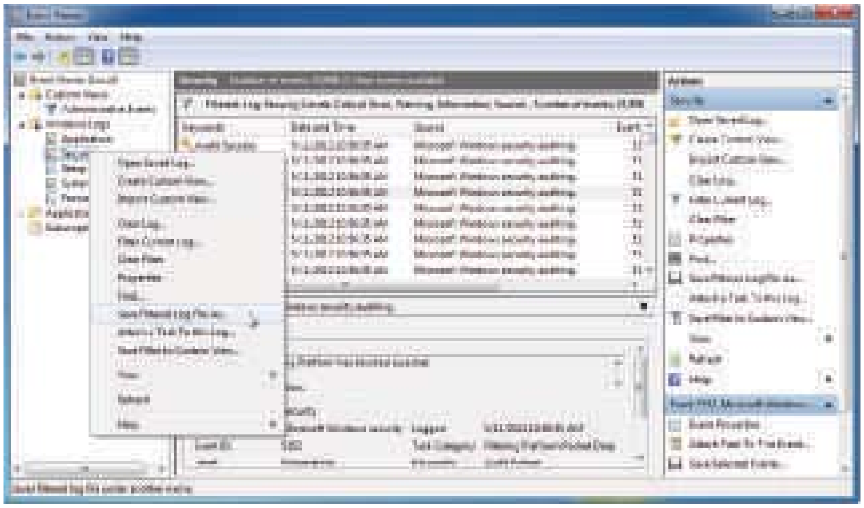


Figure 11-28 Save a filtered log file so that you can view it later

Source: Microsoft Windows 7

A+
220-802
1.1, 1.4

- To control the size of a log file, you can clear it. In the log's shortcut menu, select **Clear Log**. Before clearing the log, Event Viewer gives you a chance to save it.
- Select **Properties** in the log's shortcut menu to control the maximum size of the log file and to cause the events to be archived before they are overwritten.

APPLYING CONCEPTS

Event Viewer can be useful in solving intermittent hardware problems. For example, I once worked in an office where several people updated Microsoft Word documents stored on a file server. For weeks, people complained about these Word documents getting corrupted. We downloaded the latest patches for Windows and Microsoft Office and scanned for viruses, thinking that the problem might be with Windows or the application. Then we suspected a corrupted template file for building the Word documents. But nothing we did solved our problem of corrupted Word documents. Then one day someone thought to check Event Viewer on the file server. The Event Viewer had faithfully been recording errors when writing to the hard drive. What we had suspected to be a software problem was, in fact, a failing hard drive, which was full of bad sectors. We replaced the drive and the problem went away. That day I learned the value of checking Event Viewer very early in the troubleshooting process.

Hands-on Project 11-3 Use Event Viewer

Event Viewer can be intimidating to use but is really nothing more than a bunch of logs to search and manipulate. If you have Microsoft Office installed, open a Word document, make some changes in it, and close it without saving your changes. Now look in **Applications and Services Logs**, **Microsoft**, and **Microsoft Office Alerts**. What event is recorded about your actions?

11

TASK SCHEDULER

Windows Task Scheduler can be set to launch a task or program at a future time, including at startup. When applications install, they might schedule tasks to check for and download their program updates. Task Scheduler stores tasks in a file stored in the C:\Windows\System32\Tasks folder. For example, in Figure 11-29, there are seven scheduled tasks showing and other tasks are stored in four folders.

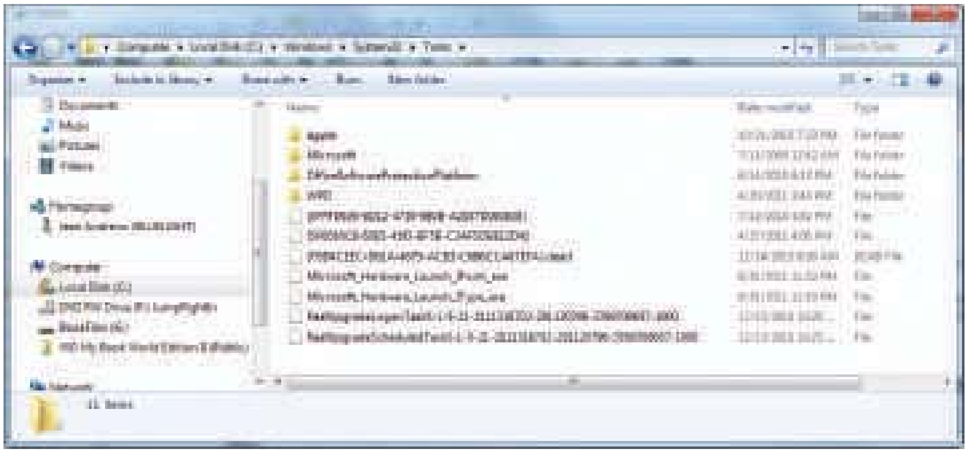
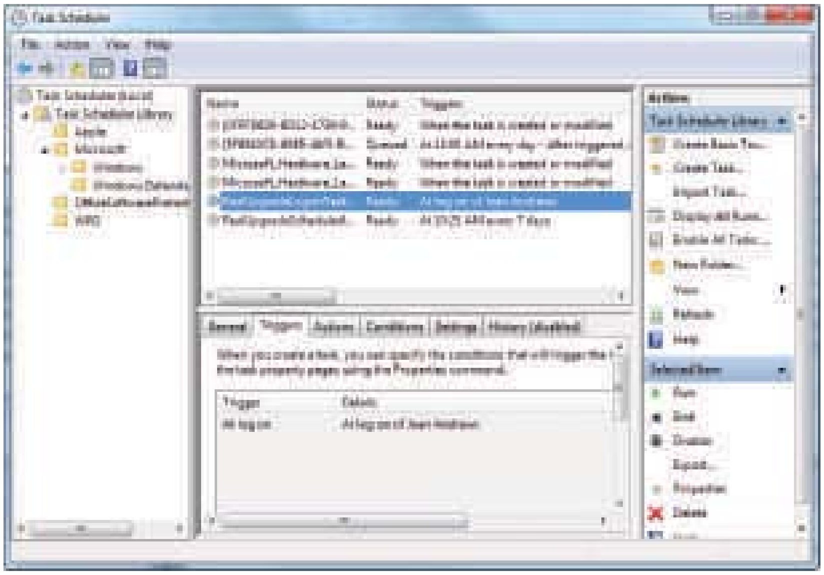


Figure 11-29 The Tasks folder contains tasks that launch at startup

Source: Microsoft Windows 7

A+
220-802
1.1, 1.4

To open Task Scheduler from the Control Panel, double-click **Task Scheduler** in the Administrative Tools group. Alternately, you can click Start, All Programs, Accessories, System Tools, and Task Scheduler. The Task Scheduler window is shown in Figure 11-30.



Source: Microsoft Windows 7

Figure 11-30 View and manage tasks from the Task Scheduler window

Here is what you need to know to use the Task Scheduler window:

- In the left pane, drill down into groups and subgroups. Tasks in a group are listed in the middle pane.
- To see details about a task, including what triggers it, what actions it performs, the conditions and settings related to the task, and the history of past actions, select the task and then click the tabs in the lower-middle pane. For example, in Figure 11-30, you can see that the RealUpgradeLogonTask is scheduled to run when I log on.
- To add a new task, first select the group for the new task and then click **Action**, **Create Basic Task**. A wizard appears to step you through creating the task.
- To delete, disable, or run a task, select it and in the Action menu or in the Actions pane, click Delete, Disable, or Run.

Notes Tasks can be hidden in the Task Scheduler window. To be certain you're viewing all scheduled tasks, unhide them. In the menu bar, click **View**, and then **Show Hidden Tasks**.

Hands-on Project 11-4 Practice Launching Programs at Startup

Do the following to practice launching programs at startup, listing the steps you took for each activity:

1. Configure Scheduled Tasks to launch Notepad each time the computer starts and any user logs on. List the steps you took.
2. Put a shortcut in a startup folder so that any user launches a command prompt window at startup. See Appendix G for a list of startup folders.
3. Restart the system and verify that both programs are launched. Did you receive any errors?
4. Remove the two programs from the startup process.

A+
220-802
1.1, 1.4

THE REGISTRY EDITOR

Many actions, such as installing application software or hardware, can result in changes to the registry. These changes can create new keys, add new values to existing keys, and change existing values. For a few difficult problems, you might need to edit or remove a registry key. This part of the chapter looks at how the registry is organized, which keys might hold entries causing problems, and how to back up and edit the registry using the **Registry Editor (regedit.exe)**. Let's first look at how the registry is organized, and then you'll learn how to back up and edit the registry.

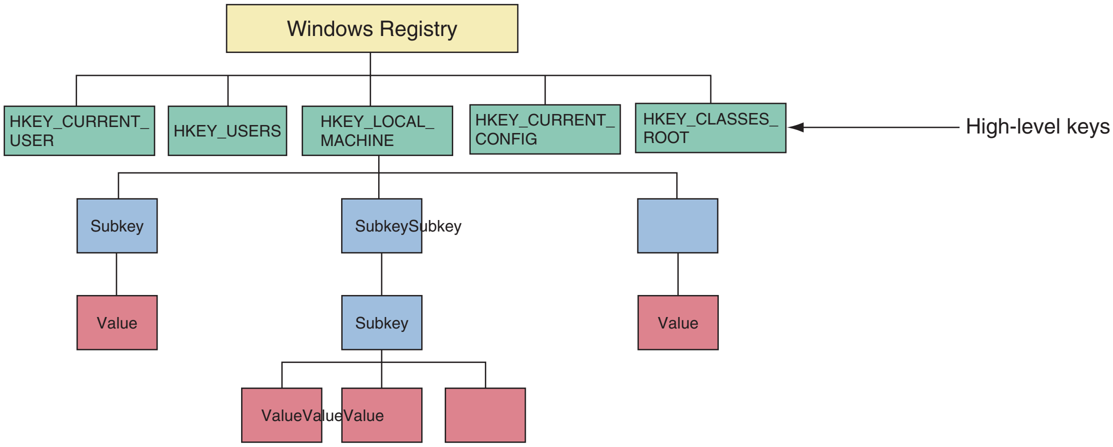
HOW THE REGISTRY IS ORGANIZED

The most important Windows component that holds information for Windows is the registry. The **registry** is a database designed with a treelike structure (called a hierarchical database) that contains configuration information for Windows, users, software applications, and installed hardware devices. During startup, Windows builds the registry in memory and keeps it there until Windows shuts down. During startup, after the registry is built, Windows reads from it to obtain information to complete the startup process. After Windows is loaded, it continually reads from many of the subkeys in the registry.

Windows builds the registry from the current hardware configuration and from information it takes from these files:

- Five files stored in the C:\Windows\System32\config folder; these files are called hives, and they are named the SAM (Security Accounts Manager), Security, Software, System, and Default hives. (Each hive is backed up with a log file and a backup file, which are also stored in the C:\Windows\System32\config folder.)
- For Windows 7/Vista, the C:\Users\username\Ntuser.dat file, which holds the preferences and settings of the currently logged-on user.
- Windows XP uses information about the current user stored in two files:
  - C:\Documents and Settings\username\Ntuser.dat
  - C:\Documents and Settings\username\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat

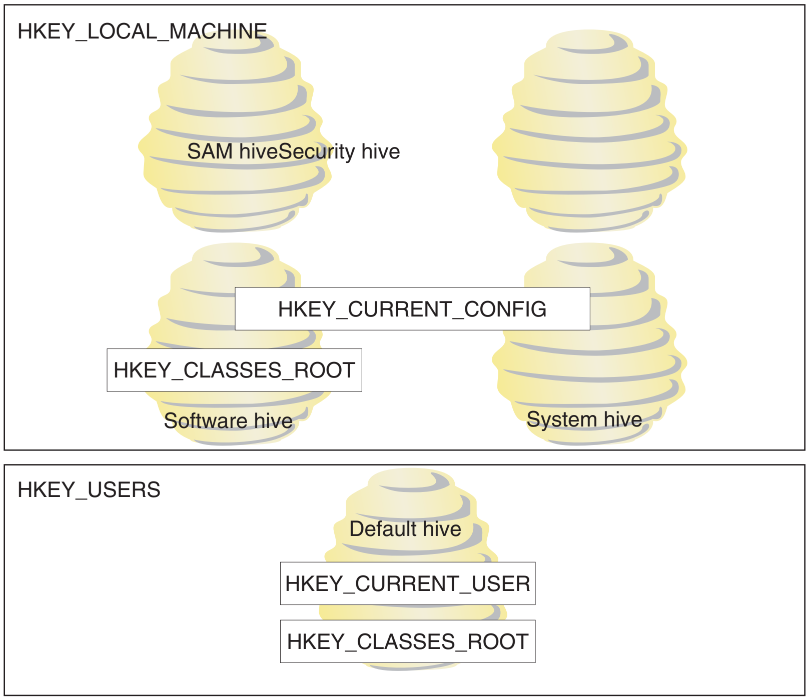
After the registry is built in memory, it is organized into five high-level keys (see Figure 11-31). Each key can have subkeys, and subkeys can have more subkeys and can be assigned one or more values. The way data is organized in the hive files is different from the way it is organized in registry keys. Figure 11-32 shows the relationship between registry keys and hives. For example, in the figure, notice that the HKEY_CLASSES_ROOT key contains data that comes from the Software hive, and this data is also stored in the larger HKEY_LOCAL_MACHINE key.



© Cengage Learning 2014

Figure 11-31 The Windows registry is logically organized in five keys with subkeys

A+
220-802
1.1, 1.4



© Cengage Learning 2014

Figure 11-32 The relationship between registry keys and hives

Here are the five keys, including where they get their data and their purposes:

- HKEY_LOCAL_MACHINE (HKLM) is the most important key and contains hardware, software, and security data. The data is taken from four hives: the SAM hive, the Security hive, the Software hive, and the System hive. In addition, the HARDWARE subkey of HKLM is built when the registry is first loaded, based on data collected about the current hardware configuration.
- HKEY_CURRENT_CONFIG (HKCC) contains information that identifies each hardware device installed on the computer. Some of the data is gathered from the current hardware configuration when the registry is first loaded into memory. Other data is taken from the HKLM key, which got its data primarily from the System hive.
- HKEY_CLASSES_ROOT (HKCR) stores information that determines which application is opened when the user double-clicks a file. This process relies on the file's extension to determine which program to load. Data for this key is gathered from the HKLM key and the HKCU key.
- HKEY_USERS (HKU) contains data about all users and is taken from the Default hive.
- HKEY_CURRENT_USER (HKCU) contains data about the current user. The key is built when a user logs on using data kept in the HKEY_USERS key and data kept in the Ntuser.dat file of the current user.

Notes Device Manager reads data from the HKLM\HARDWARE key to build the information it displays about hardware configurations. You can consider Device Manager to be an easy-to-view presentation of this HARDWARE key data.

A+
220-802
1.1, 1.4

BEFORE YOU EDIT THE REGISTRY, BACK IT UP!

When you need to edit the registry, if possible, make the change from the Windows tool that is responsible for the key—for example, by using the Programs and Features window in Control Panel. If that doesn't work and you must edit the registry, always back up the registry before attempting to edit it. Changes made to the registry are implemented immediately. ***There is no undo feature in the Registry Editor, and no opportunity to change your mind once the edit is made.***

Here are the ways to back up the registry:

- ***Use System Protection to create a restore point.*** A restore point keeps information about the registry. You can restore the system to a restore point to undo registry changes, as long as the registry is basically intact and not too corrupted. Also know that, if System Protection is turned on, Windows 7/Vista automatically makes a daily backup of the registry hive files to the C:\Windows\System32\Config\RegBack folder.
- ***Back up a single registry key just before you edit the key.*** This method, called exporting a key, should always be used before you edit the registry. How to export a key is coming up in this chapter.
- ***Make an extra copy of the C:\Window\System32\config folder.*** This is what I call the old-fashioned shotgun approach to backing up the registry. This backup will help if the registry gets totally trashed. You can boot from the Windows setup DVD and use the Windows 7/Vista Recovery Environment or the XP Recovery Console to restore the folder from your extra copy. This method is drastic and not recommended except in severe cases. But, still, just to be on the safe side, I make an extra copy of this folder just before I start any serious digging into the registry.
- ***For Windows XP, back up the system state.*** Use Ntbackup in Windows XP to back up the system state, which also makes an extra copy of the registry hives. Windows XP stores the backup of the registry hives in the C:\Windows\repair folder.

In some situations, such as when you're going to make some drastic changes to the registry, you'll want to play it safe and use more than one backup method. Extra registry backups are always a good thing! Now let's look at how to back up an individual key in the registry, and then you'll learn how to edit the registry.

Notes Although you can edit the registry while in Safe Mode, you cannot create a restore point in Safe Mode.

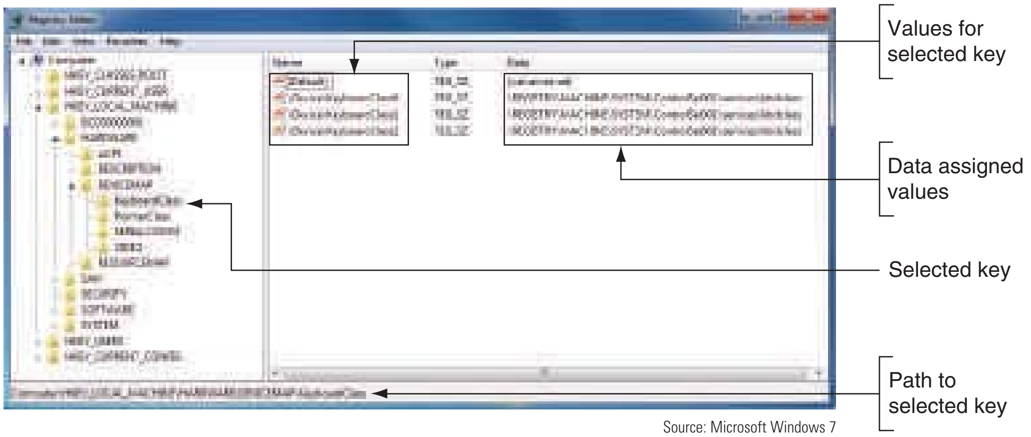
Backing Up and Restoring Individual Keys in the Registry

A less time-consuming method of backing up the registry is to back up a particular key that you plan to edit. However, know that if the registry gets corrupted, having a backup of only a particular key most likely will not help you much when trying a recovery. Also, although you could use this technique to back up the entire registry or an entire tree within the registry, it is not recommended.

To back up a key along with its subkeys in the registry, follow these steps:

1. Open the Registry Editor. To do that, click **Start** and type **regedit** in the search box, press **Enter**, and respond to the UAC box. Figure 11-33 shows the Registry Editor with the five main keys and several subkeys listed. Click the triangles on the left to see subkeys. When you select a subkey, such as KeyboardClass in the figure, the names of the values in that subkey are displayed in the right pane along with the data assigned to each value.

A+
220-802
1.1, 1.4

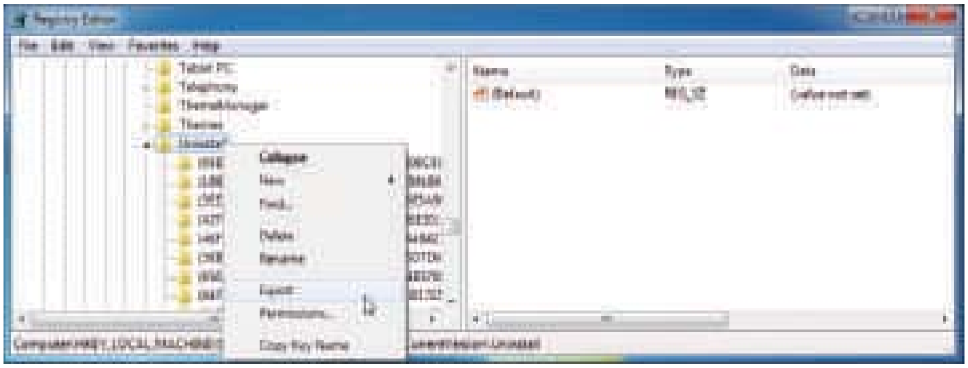


Source: Microsoft Windows 7

Figure 11-33 The Registry Editor showing the five main keys, subkeys, values, and data

Notes The full path to a selected key displays in the status bar at the bottom of the editor window. If the status bar is missing, click **View** in the menu bar and make sure **Status Bar** is checked.

2. Suppose we want to back up the registry key that contains a list of installed software, which is HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall. (HKLM stands for HKEY_LOCAL_MACHINE.) First click the appropriate triangles to navigate to the key. Next, right-click the key and select **Export** from the shortcut menu, as shown in Figure 11-34. The Export Registry File dialog box appears.



Source: Microsoft Windows 7

Figure 11-34 Using the Registry Editor, you can back up a key and its subkeys with the Export command

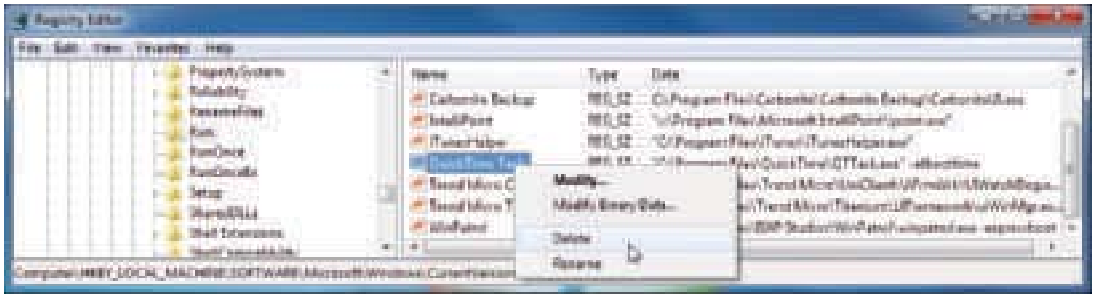
3. Select the location to save the export file and name the file. A convenient place to store an export file while you edit the registry is the desktop. Click **Save** when done. The file saved will have a .reg file extension.
4. You can now edit the key. Later, if you need to undo your changes, exit the Registry Editor and double-click the saved export file. The key and its subkeys saved in the export file will be restored. After you're done with an export file, delete it so that no one accidentally double-clicks it and reverts the registry to an earlier setting.

Editing the Registry

Before you edit the registry, you should use one or more of the four backup methods just discussed so that you can restore it if something goes wrong. To edit the registry, open the **Registry Editor** (**regedit.exe**), and locate and select the key in the left pane of the Registry

A+
220-802
1.1, 1.4

Editor, which will display the values stored in this key in the right pane. To edit, rename, or delete a value, right-click it and select the appropriate option from the shortcut menu. For example, in Figure 11-35, I'm ready to delete the value QuickTime Task and its data. Changes are immediately applied to the registry and there is no undo feature. (However, Windows or applications might need to read the changed value before it affects their operations.) To search the registry for keys, values, and data, click **Edit** in the menu bar and then click **Find**.



Source: Microsoft Windows 7

Figure 11-35 Right-click a value to modify, delete, or rename it

Caution Changes made to the registry take effect immediately. Therefore, take extra care when editing the registry. If you make a mistake and don't know how to correct a problem you create, then double-click the exported key to recover. When you double-click an exported key, the registry is updated with the values stored in this key.

11

Hands-on Project 11-5 Edit and Restore the Registry

Practice editing and restoring the registry by doing the following to change the name of the Recycle Bin on the Windows desktop:

1. Using the Registry Editor, export the registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer to an export file stored on the desktop.
2. To change the name of the Recycle Bin on the Windows 7/Vista desktop for the currently logged-on user, click the following subkey, which holds the name of the Recycle Bin: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\645FF040-5081-101B-9F08-00AA002F954E.
3. The data name is (Default), which means the value is not set and the default name, Recycle Bin, is used. To enter a new name for the Recycle Bin, in the right pane, double-click **(Default)**. The Edit String box appears. The Value data text box in the dialog box should be empty. If a value is present, you selected the wrong value. Check your work and try again.
4. Enter a new name for the Recycle Bin, for example, "Trash Can." Click **OK**.
5. Move the Registry Editor window so that you can see the Recycle Bin on the desktop. Don't close the window.
6. Right-click the desktop and select **Refresh** from the shortcut menu. The name of the Recycle Bin changes.
7. To restore the name to its default value, in the Registry Editor window, again double-click **(Default)**, delete your entry, and click **OK**.

A+
220-802
1.1, 1.4

8. To verify the change is made, refresh the Windows desktop. The Recycle Bin name should return to its default value.

9. Exit the Registry Editor and then delete the exported registry key stored on the desktop.

From these directions, you can see that changes made to the registry take effect immediately. Therefore, take extra care when editing the registry. If you make a mistake and don't know how to correct a problem you create, then you can restore the key that you exported by exiting the Registry Editor and double-clicking the exported key.

WINDOWS 7 TOOLS TO MONITOR PERFORMANCE AND OPTIMIZE RESOURCES

The Windows 7 tools for monitoring performance and optimizing resources that differ significantly from those in Vista or XP include the Windows 7 Performance Information and Tools window, Resource Monitor, Reliability Monitor, and Performance Monitor. These Windows 7 tools are covered next.

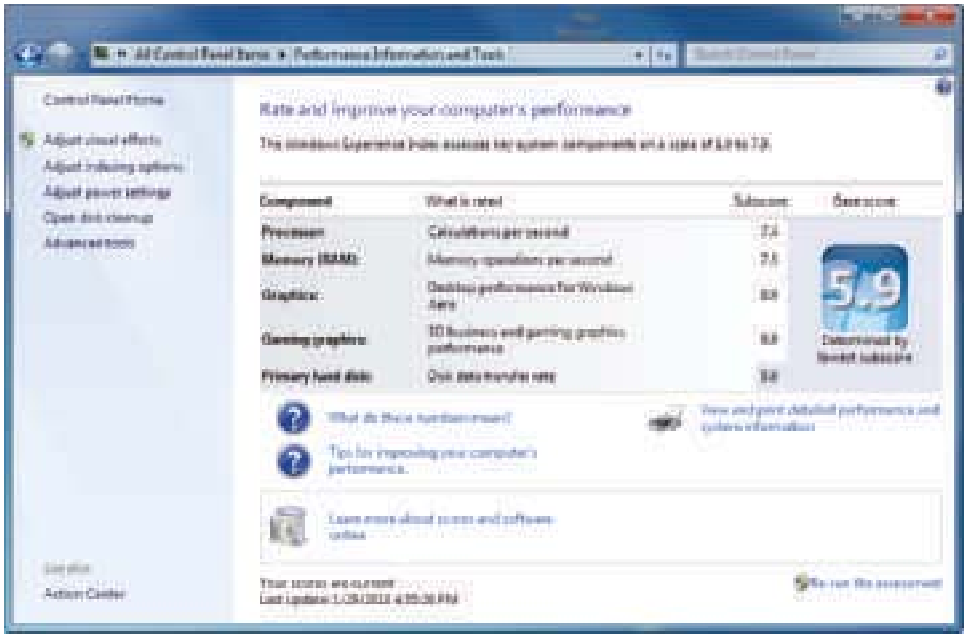
PERFORMANCE INFORMATION AND TOOLS WINDOW

The Performance Information and Tools window gives information to evaluate the performance of a system and to adjust Windows for best performance.

Use one of the following methods to open the Performance Information and Tools window:

- Click **Start**, right-click **Computer,** and select **Properties**. In the System window, click **Performance Information and Tools** (in Vista, click Performance).
- In the Action Center, click **View performance information**.

The Performance Information and Tools window for Windows 7 is shown in Figure 11-36, and the Vista window is shown in Figure 11-37.



All Control Panel Items ▸ Performance Information and Tools

Rate and improve your computer's performance

The Windows Experience Index assesses key system components on a scale of 1.0 to 7.9.

Component	What is rated	Subscore	Base score
Processor:	Calculations per second	7.4	5.9 Determined by lowest subscore
Memory (RAM):	Memory operations per second	7.5	
Graphics:	Desktop performance for Windows Aero	[illegible]	
Gaming graphics:	3D business and gaming graphics performance	[illegible]	
Primary hard disk:	Disk data transfer rate	5.9	

Your scores are current.
Last Update: 1/26/2012 4:55:36 PM

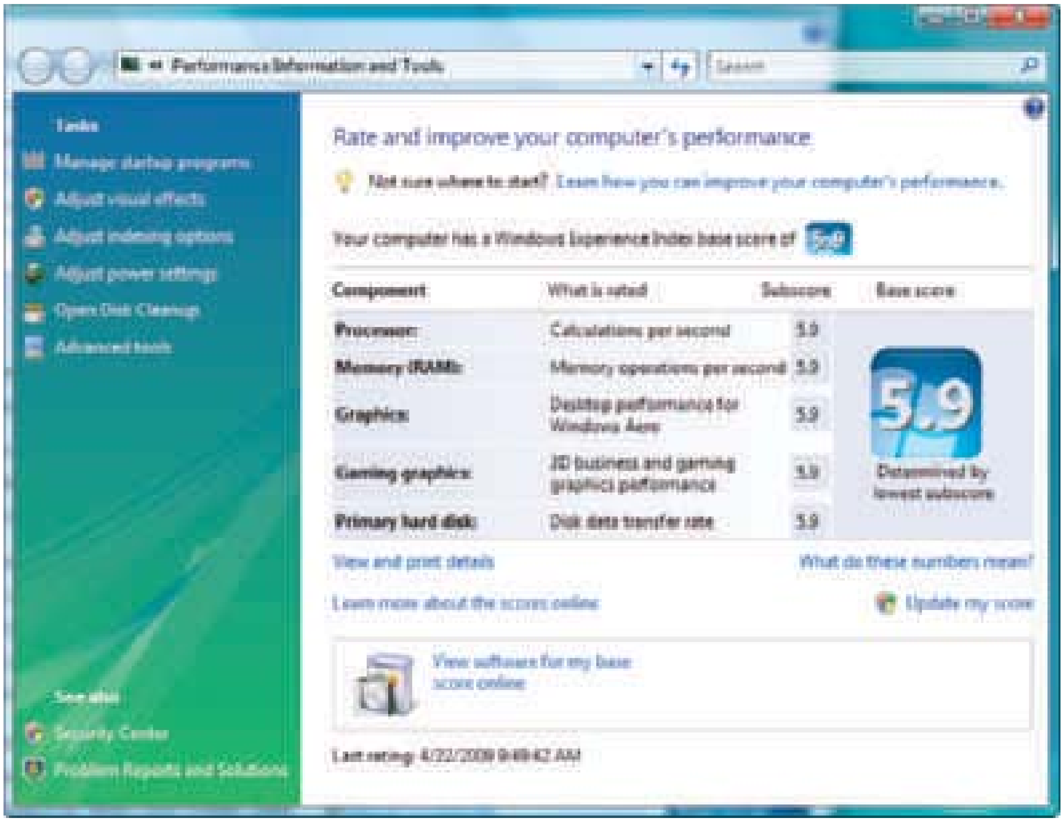
Control Panel Home
Adjust visual effects
Adjust indexing options
Adjust power settings
Open disk cleanup
Advanced tools
What do these numbers mean?
Tips for improving your computer's performance.
View and print detailed performance and system information
Learn more about scores and software online
Re-run the assessment
See also
Action Center

Source: Microsoft Windows 7

Figure 11-36 The Windows Experience Index gives a rating of key system components in this Windows 7 computer

A+
220-802
1.1, 1.4

> **Notes** To see more detail about the Windows 7 system and to print these details, click **View and print detailed performance and system information**.



Rate and improve your computer's performance

Not sure where to start? Learn how you can improve your computer's performance.

Your computer has a Windows Experience Index base score of 5.9

Component	What is rated	Subscore	Base score
Processor:	Calculations per second	5.9	5.9 Determined by lowest subscore
Memory (RAM):	Memory operations per second	5.9	
Graphics:	Desktop performance for Windows Aero	5.9	
Gaming graphics:	3D business and gaming graphics performance	5.9	
Primary hard disk:	Disk data transfer rate	5.9	

Last rating: 4/22/2009 9:48:42 AM

Source: Microsoft Windows 7

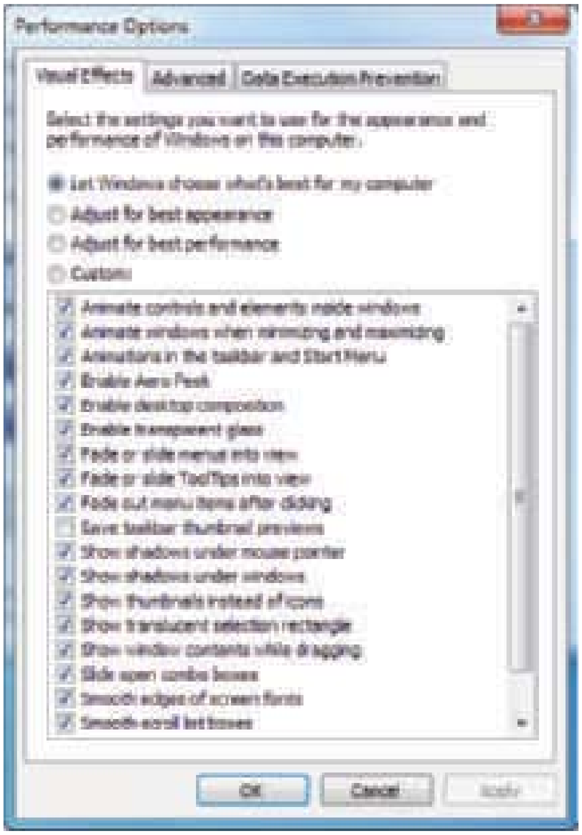
Figure 11-37 The Windows Experience Index for this Vista system reports no potential bottlenecks

The Windows Experience Index evaluates key system components to give a high-level view of the computer's performance. Five key components are rated on a scale of 1.0 to 7.9. The index is the lowest value of all five ratings because this component is considered the bottleneck component for overall performance.

The left pane contains links to adjusting visual effects, indexing options, and power settings and tools to clean up the hard drive. These utilities can help improve a system's performance and provide more information about the system. Follow these steps to use the tools:

1. Click **Adjust visual effects** to open the Performance Options box (see Figure 11-38). On the Visual Effects tab of this box, you can choose to adjust visual effects for best performance or best appearance. If resources are low on a system, adjusting for best performance can remove a system bottleneck hogging resources. You can also enable or disable individual visual effects to customize the visual effects, creating a balance between best performance and best appearance.

A+
220-802
1.1, 1.4



Select the settings you want to use for the appearance and performance of Windows on this computer.

● Let Windows choose what's best for my computer
○ Adjust for best appearance
○ Adjust for best performance
○ Custom:

☑ Animate controls and elements inside windows
☑ Animate windows when minimizing and maximizing
☑ Animations in the taskbar and Start Menu
☑ Enable Aero Peek
☑ Enable desktop composition
☑ Enable transparent glass
☑ Fade or slide menus into view
☑ Fade or slide ToolTips into view
☑ Fade out menu items after clicking
☐ Save taskbar thumbnail previews
☑ Show shadows under mouse pointer
☑ Show shadows under windows
☑ Show thumbnails instead of icons
☑ Show translucent selection rectangle
☑ Show window contents while dragging
☑ Slide open combo boxes
☑ Smooth edges of screen fonts
☑ Smooth-scroll list boxes

Source: Microsoft Windows 7

Figure 11-38 Balance visual effects between best performance and best appearance

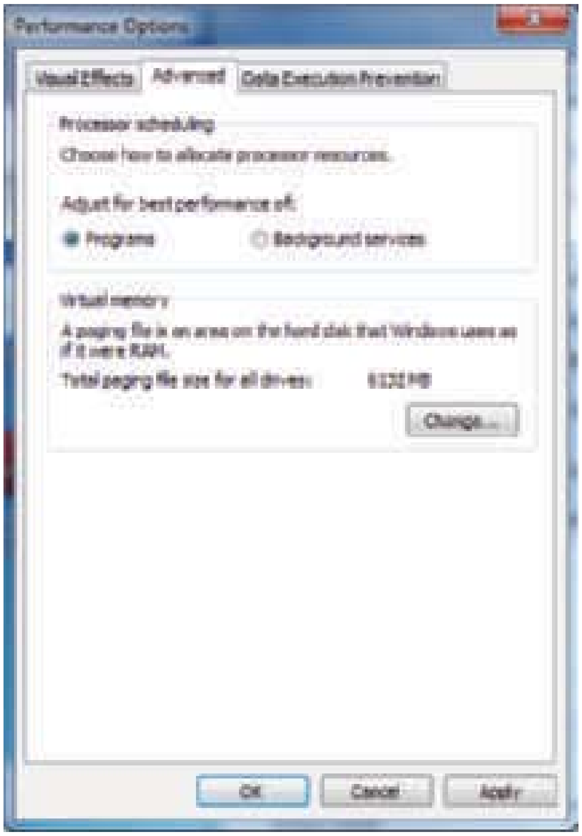
Notes You can also open the Performance Options box from the System Properties box. In the System Properties box, on the **Advanced** tab, click **Settings** in the Performance area.

2. Click the **Advanced** tab on the Performance Options box to choose how to allocate processor resources, adjusting for best performance between programs running in the foreground and programs running in the background (see Figure 11-39).

Notes Reducing the CPU processing time allowed for programs is called throttling the programs.

3. Also notice on the Advanced tab the ability to adjust virtual memory. Click **Change** to move the file to a different hard drive, which can free up space on the Windows volume and might improve performance.
4. Also in the left pane in the Performance and Information Tools window (refer to Figure 11-36), you can click **Advanced tools** to see a list of performance issues and to open Task Manager, Disk Defragmenter, Event Viewer, Windows 7 Performance Monitor, Windows 7 Resource Monitor, Vista Reliability and Performance Monitor, and other tools.

A+
220-802
1.1, 1.4



Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

● Programs ○ Background services

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 6132 MB

Source: Microsoft Windows 7

Figure 11-39 Use the Advanced tab of the Performance Options box to adjust how processor resources are allocated to programs and background services

WINDOWS 7 RESOURCE MONITOR

Windows 7 **Resource Monitor** (resmon.exe) monitors the performance of the processor, memory, hard drive, and network. As you learned earlier in the chapter, Task Manager reports some of this information. To access Resource Monitor, use one of these methods:

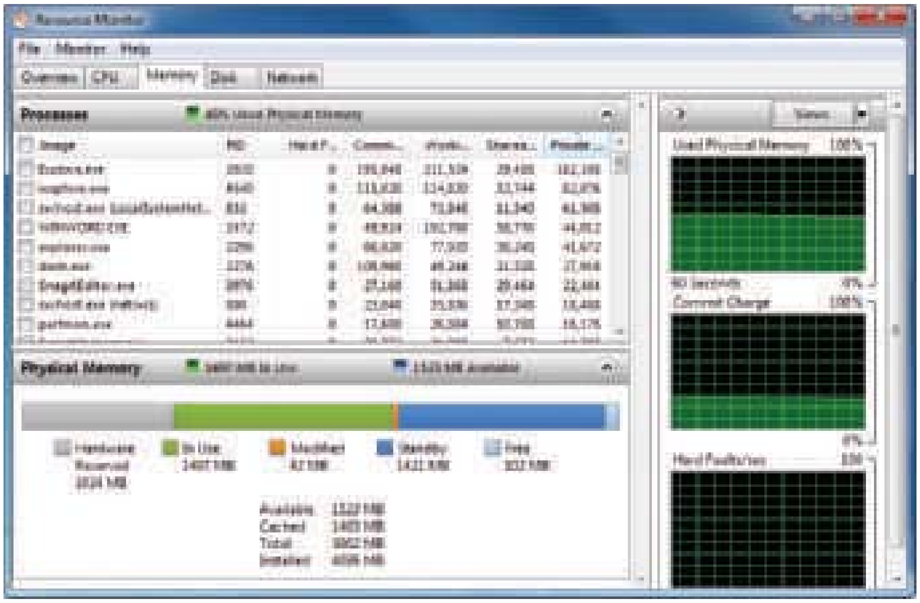
- In Task Manager, click **Resource Monitor** on the Performance tab.
- In the Performance Information and Tools window, click **Advanced tools**, and then click **Open Resource Monitor**.
- In the Computer Management window, in the System Tools, Performance group, click **Monitoring Tools**, **More Actions**, and **Resource Monitor**.

The Resource Monitor window is shown in Figure 11-40 with the Memory tab selected.

The bar graphically showing how memory is used accounts for all the memory installed in a system. The graph shows these five ways memory is used:

- Hardware Reserved memory is used by BIOS and certain drivers such as the video drivers. Windows does not have access to this memory. For example, compare total memory reported by Task Manager in Figure 11-10 earlier in the chapter to installed memory reported by Resource Monitor in Figure 11-40 for the same system.
- In Use memory is used by other drives, the OS, and applications.
- Modified memory will be available as soon as its contents are written to disk.
- Standby memory is holding data and code that is ready to use.
- Free memory will be used as the system needs it.

A+
220-802
1.1, 1.4



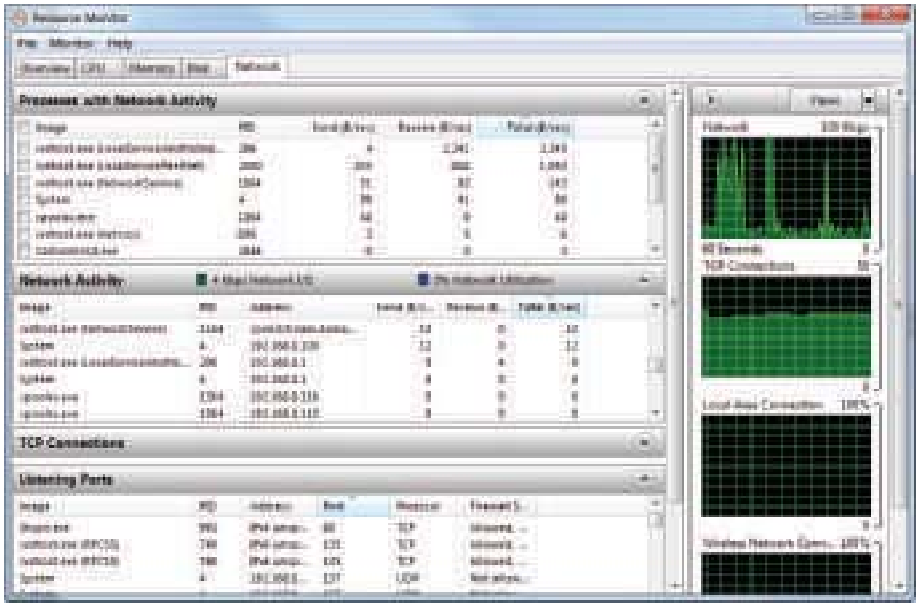
Source: Microsoft Windows 7

Figure 11-40 The Resource Monitor shows how memory is currently used

The easiest way to find out if a system would benefit from a memory upgrade (adding more memory to the system) is to watch this memory bar as a user does her work. If you consistently see Free memory disappear from this graph, the system would benefit from more installed memory.

Notes To best gauge the performance of a system, ask the user to watch the Resource Monitor throughout the workday and note what the monitor shows when the system is busiest.

The Network tab of the Resource Monitor is useful if you suspect a program is hogging network resources. If you suspect a worm or other process is slowing down the network with excessive activity, look for the process in the Processes with Network Activity group on the Network tab (see Figure 11-41). (A worm is malware that can bring down a network by overwhelming it with activity.)

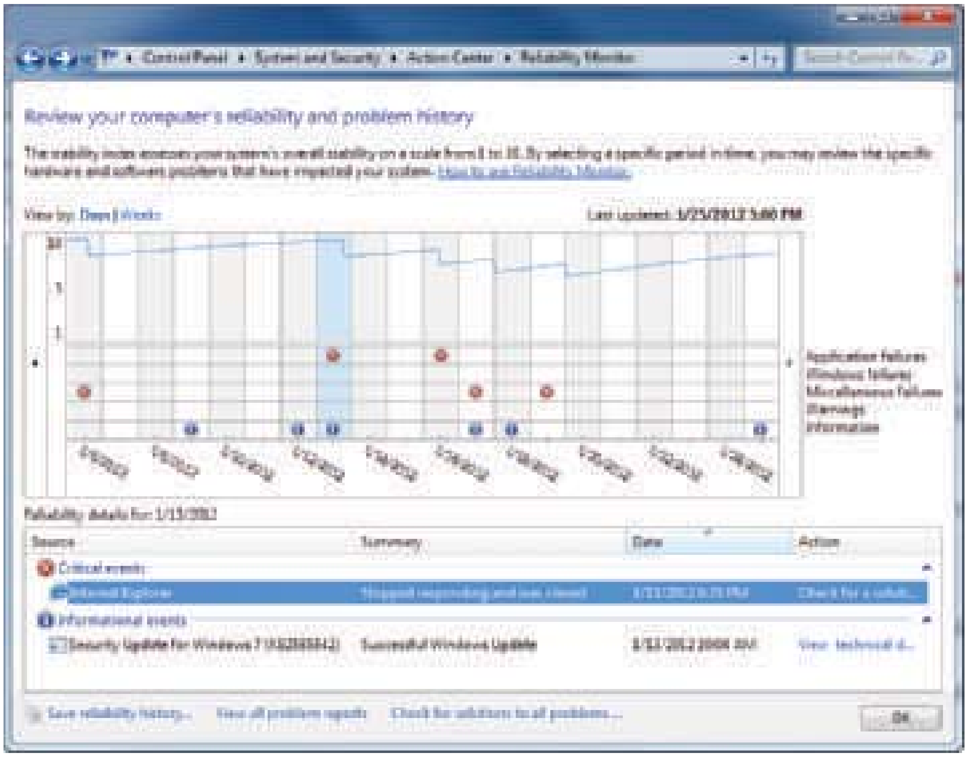

Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
Processes with Network Activity
Image PID Send (B/sec) Receive (B/sec) Total (B/sec)
Network Activity
Image PID Address Send (B/s... Receive (B... Total (B/sec)
TCP Connections
Listening Ports
Image PID Address Port Protocol Firewall S...
Views
Network
60 Seconds
TCP Connections
Local Area Connection 100%
Wireless Network Conn... 100%

Source: Microsoft Windows 7

Figure 11-41 Look for a process using excessive networking resources

WINDOWS 7 RELIABILITY MONITOR

The Windows **Reliability Monitor** gives information about problems and errors that happen over time. Unless someone has cleared its history log, it reports problems since Windows was installed. To open the Reliability Monitor, open the **Action Center**, click the down arrow to open the Maintenance group, and click **View reliability history**. (You can also enter **Reliability** in the search box.) The Reliability Monitor window is shown in Figure 11-42.



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system. How to use Reliability Monitor

View by: Days | Weeks

Last updated: 1/25/2012 5:00 PM

Reliability details for: 1/13/2012

Source	Summary	Date	Action
Critical events			
Internet Explorer	Stopped responding and was closed	1/13/2012 [illegible] PM	Check for a soluti...
Informational events			
Security Update for Windows 7 ([illegible])	Successful Windows Update	1/13/2012 [illegible] AM	View technical d...

Save reliability history... View all problem reports Check for solutions to all problems...

Source: Microsoft Windows 7

Figure 11-42 Use the Reliability Monitor to search for when a problem began and what else happened about that time

When you click an error in the column graph, the error and other events that happened the same day appear at the bottom of the window. Double-click one of these errors or events to see more information about it.

One important step in troubleshooting a problem is to ask what changes were made to a system at the time a problem began. If you can find out about when a performance problem started, use the Reliability Monitor to find out what happened about that same time. For example, suppose Internet Explorer locks up and the problem started around the day selected in Figure 11-42. You can see from this window that Windows received a security update on this day. The next task would be to research this security update on the Microsoft web site to see if it might be the source of the problem.

WINDOWS 7 PERFORMANCE MONITOR

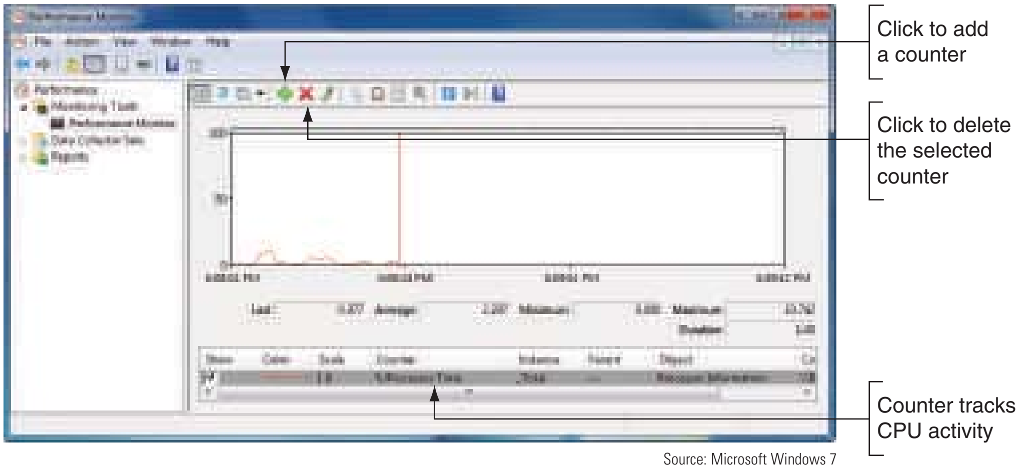
Windows 7 **Performance Monitor** is a Microsoft Management Console snap-in (Perfmon.msc or Perfmon.exe) that can track activity by hardware and software to measure performance. Whereas Resource Monitor monitors activities in real time, Performance

A+
220-802
1.1, 1.4

Monitor can monitor in real time and can save collected data in logs for future use. Software developers might use this tool to evaluate how well their software is performing and to identify software and hardware bottlenecks.

Use one of these methods to open the Performance Monitor window shown in Figure 11-43:

- Click **Start**, enter **perfmon.msc** in the search box, and press **Enter**.
- In the Performance Information and Tools window, click **Advanced tools**, and click **Open Performance Monitor**.
- In the Computer Management window in the System Tools, Performance, Monitoring Tools group, click **Performance Monitor**.


Click to add a counter
Click to delete the selected counter
Counter tracks CPU activity

Source: Microsoft Windows 7

Figure 11-43 Performance Monitor uses counters to monitor various activities of hardware and software

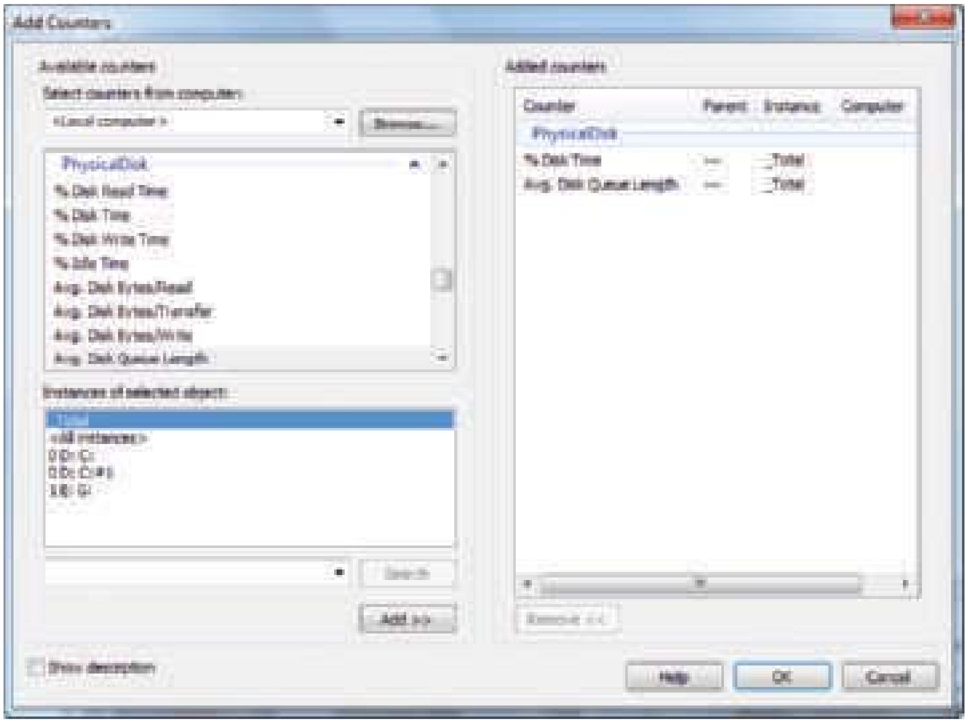
Performance Monitor offers hundreds of counters used to examine many aspects of the system related to performance. The Windows default setting is to show the %Processor Time counter the first time you open the window (see Figure 11-43). This counter appears as a red line in the graph and tracks activity of the processor.

To keep from unnecessarily using system resources, only use the counters you really need. For example, suppose you want to track hard drive activity. You first remove the %Processor Time counter. To delete a counter, select the counter from the list so that it is highlighted and click the red **X** above the graph.

Next add two counters: % Disk Time counter and Avg. Disk Queue Length counter. The % Disk Time counter tracks the percentage of time the hard drive is in use, and the Avg. Disk Queue Length counter tracks the average number of processes waiting to use the hard drive. To add a counter, click the green **plus sign** above the graph. Then, in the Add Counters box, select a counter and click **Add**. Figure 11-44 shows the Add Counters box with two counters added. After all your counters are added, click **OK**.

Allow Performance Monitor to keep running while the system is in use, and then check the counters. The results for one system are shown in Figure 11-45. Select each counter and note the average, minimum, and maximum values for the counter.

A+
220-802
1.1, 1.4



Add Counters

Available counters

Select counters from computer:

<Local computer> ▾ Browse...

PhysicalDisk
% Disk Read Time
% Disk Time
% Disk Write Time
% Idle Time
Avg. Disk Bytes/Read
Avg. Disk Bytes/Transfer
Avg. Disk Bytes/Write
Avg. Disk Queue Length

Instances of selected object:

_Total
<All instances>
0 D: C:
0 D: C:#1
1 E: G:

Search

Add >>

Added counters

Counter	Parent	Instance	Computer
PhysicalDisk			
% Disk Time	---	_Total	
Avg. Disk Queue Length	---	_Total	

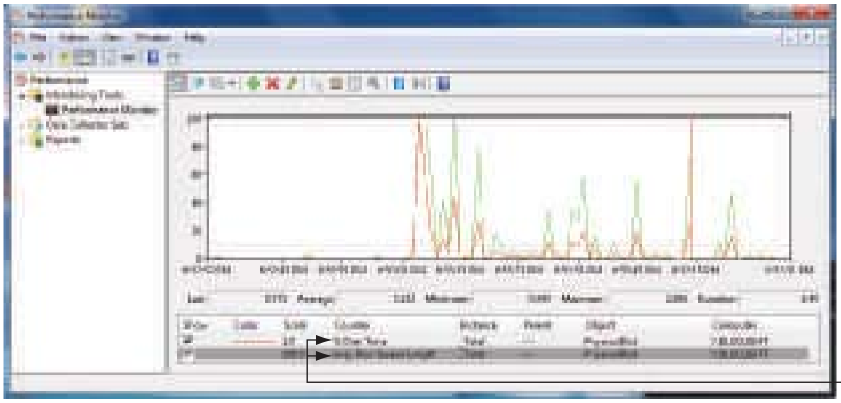
Remove <<

□ Show description

Help OK Cancel

Source: Microsoft Windows 7

Figure 11-44 Add counters to set up what Performance Monitor tracks



Two counters to track hard drive activity

Source: Microsoft Windows 7

Figure 11-45 Two counters can measure hard drive performance

If the Avg. Disk Queue Length is above two and the % Disk Time is more than 80 percent, you can conclude that the hard drive is working excessively hard and processes are slowed down waiting on the drive. Anytime a process must wait to access the hard drive, you are likely to see degradation in overall system performance.

Performance Monitor also offers several data collector sets. A **data collector set** is a set of counters that you can use to collect data about the system and save this data in a report or log file for future use. You can also create your own data collector sets by selecting counters to use in the set and you can decide where to save the log file when you run your customized data collector set. Data collector sets are started, stopped, and customized using the Data Collector Sets group in the left pane of the Performance Monitor window. If you want to know more about using data collector sets, click the Help button in the Performance Monitor window or search the Microsoft web site at *technet.microsoft.com*.

A+
220-802
1.1, 1.4

Vista Differences The Windows Vista **Reliability and Performance Monitor (Perfmon.msc)** is an earlier version of three separate Windows 7 tools: Windows 7 Resource Monitor, Reliability Monitor, and Performance Monitor. To find out more about the Vista Reliability and Performance Monitor, see Appendix B.

XP Differences The Windows XP Performance Monitor is also called the **System Monitor**. To find out more about this tool, see Appendix C.

Hands-on | Project 11-6 Find Windows Utilities

List the program filename and path for the following utilities. (*Hint*: You can use Windows Explorer or Search to locate files.) Use Windows 7 to find the first 11 utilities listed.

1. Task Manager
2. Vista Software Explorer
3. System Configuration
4. Services Console
5. Computer Management
6. Microsoft Management Console
7. Event Viewer
8. Performance Monitor
9. Resource Monitor
10. Reliability Monitor
11. Registry Editor
12. Vista Reliability and Performance Monitor
13. XP Performance Monitor

Now let's turn our attention to the step-by-step procedures using the tools you just learned about to improve Windows performance.

IMPROVING WINDOWS PERFORMANCE

A+
220-802
4.3

In this part of the chapter, you'll learn to search for problems affecting performance and to clean up the Windows startup process. These step-by-step procedures go beyond the routine maintenance tasks you learned about in Chapter 10. We're assuming Windows starts with no errors. If you are having trouble loading Windows, it's best to address the error first

A+
220-802
4.3

A+ Exam Tip The A+ 220-802 exam expects you to know how to troubleshoot and solve problems with slow system performance.

rather than to use the tools described here to improve performance. How to handle errors that keep Windows from starting is covered in Chapter 14.

Now let's look at 10 steps you can take to improve Windows performance.

STEP 1: PERFORM ROUTINE MAINTENANCE

It might seem pretty mundane, but the first things you need to do to improve performance of a sluggish Windows system are the routine maintenance tasks that you learned in Chapter 10. These tasks are summarized here:

- ***Verify critical Windows settings.*** Make sure Windows updates are current. Verify that antivirus software is updated and set to routinely scan for viruses. Make sure the network connection is secured. If the system is experiencing a marked decrease in performance, suspect a virus and use up-to-date antivirus software to perform a full scan of the system.
- ***Clean up, defrag, and check the hard drive.*** Make sure at least 15 percent of drive C: is free. For Windows 7/Vista, make sure a magnetic hard drive is being defragged weekly. If you suspect hard drive problems, use Chkdsk to check the hard drive for errors and recover data.
- ***Uninstall software you no longer need.*** Use the Windows 7/Vista Programs and Features window or the XP Add or Remove Programs window to uninstall programs you no longer need.

As always, if valuable data is not backed up, back it up before you apply any of the fixes in this chapter. You don't want to risk losing the user's data.

STEP 2: CLEAN WINDOWS STARTUP

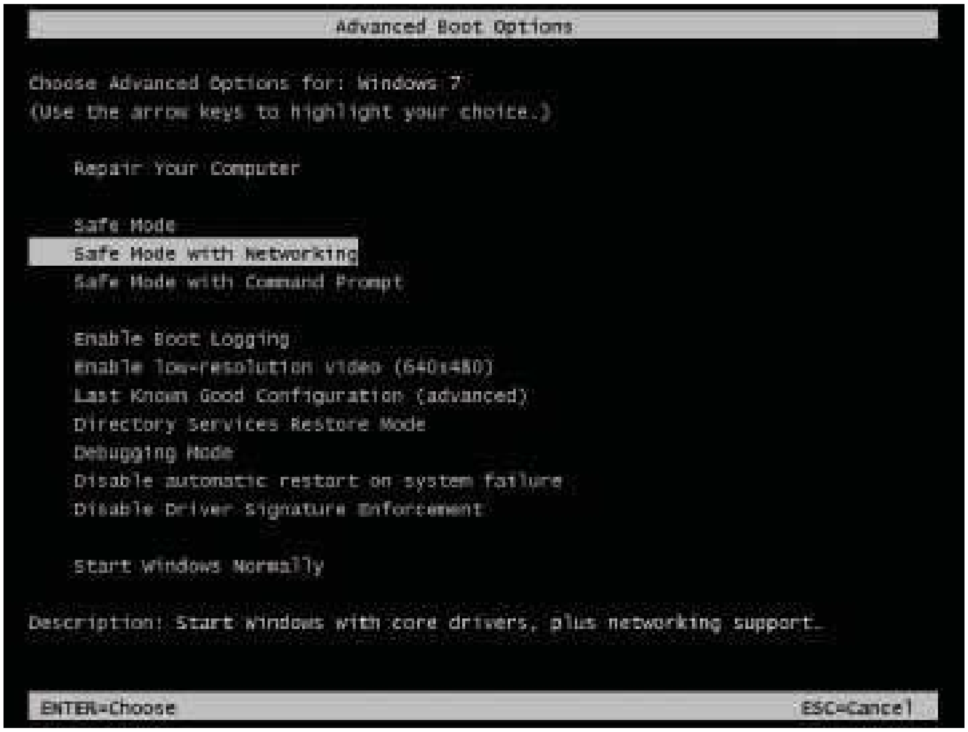
The most important step following routine maintenance to improve performance is to verify that startup programs are kept to a minimum. Before cleaning Windows startup, you can use Safe Mode to set a benchmark for the time it takes to start Windows when only the bare minimum of programs are launched.

OBSERVE PERFORMANCE IN SAFE MODE

To find out if programs and services are slowing down Windows startup, boot the system in Safe Mode and watch to see if performance improves. Do the following:

1. Use a stopwatch or a watch with a second hand to time a normal startup from the moment you press the power button until the wait icon on the Windows desktop disappears.
2. Time the boot again, this time using Safe Mode. To boot the system in Safe Mode, press **F8** while Windows is loading and then select Safe Mode with Networking from the boot options menu (see Figure 11-46).

A+
220-802
4.3



```
                       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: Start Windows with core drivers, plus networking support.

 ENTER=Choose                                              ESC=Cancel
```

Source: Microsoft Windows 7

Figure 11-46 Windows Advanced Boot Options Menu allows you to launch Safe Mode

If the difference is significant, follow the steps in this part of the chapter to reduce Windows startup to essentials. If the performance problem still exists in Safe Mode, you can assume that the problem is with hardware or Windows settings and you can proceed to *Step 3: Check If the Hardware Can Support the OS.*

INVESTIGATE AND ELIMINATE STARTUP PROGRAMS

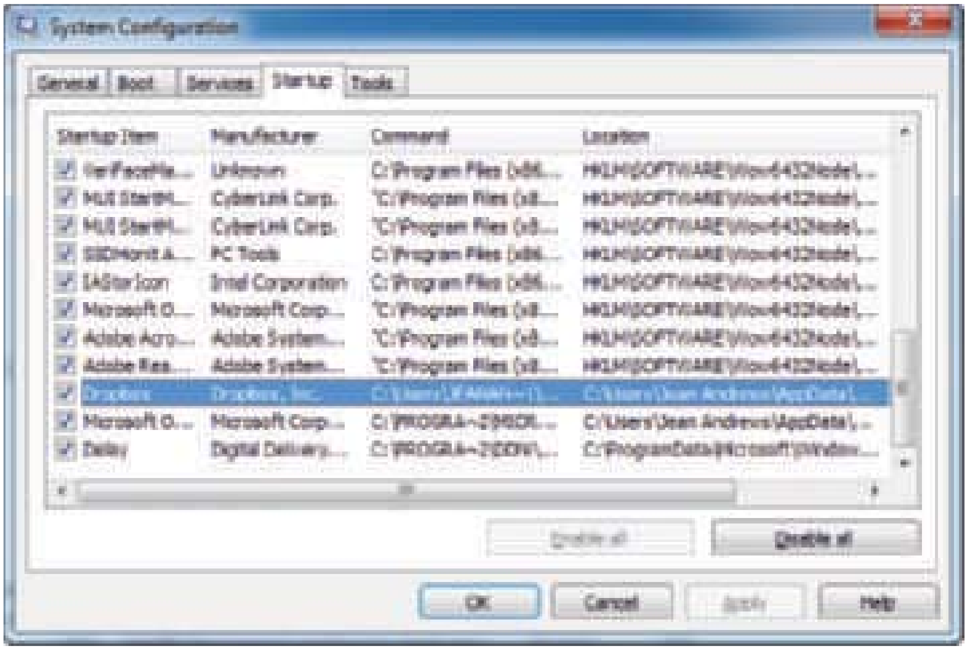
To speed up startup, search for unnecessary startup programs you can eliminate. Tools that can help are System Configuration (Msconfig.exe), startup folders, and Task Manager. Follow these steps to investigate startup:

1. Open Msconfig, select the **Startup** tab, and look for a specific startup program you don't want. If you're not sure of the purpose of a program, scroll to the right in the Command column to see the name of the startup program file (see Figure 11-47). Then search the web for information on this program. Be careful to use only reliable sites for credible information. Use the Location column to find out how the program was launched. In Figure 11-47, notice the last three items are launched from startup folders.

> **Caution** A word of caution is important here: many web sites will tell you a legitimate process is malicious so that you will download and use their software to get rid of the process. However, their software is likely to be adware or spyware that you don't want. Make sure you can trust a site before you download from it or take its advice.

2. If you want to find out if disabling a startup entry gives problems or improves performance, temporarily disable it using Msconfig. To permanently disable a startup item, it's best to uninstall the software or remove the entry from a startup folder. See Appendix G for a list of startup folders.

A+
220-802
4.3



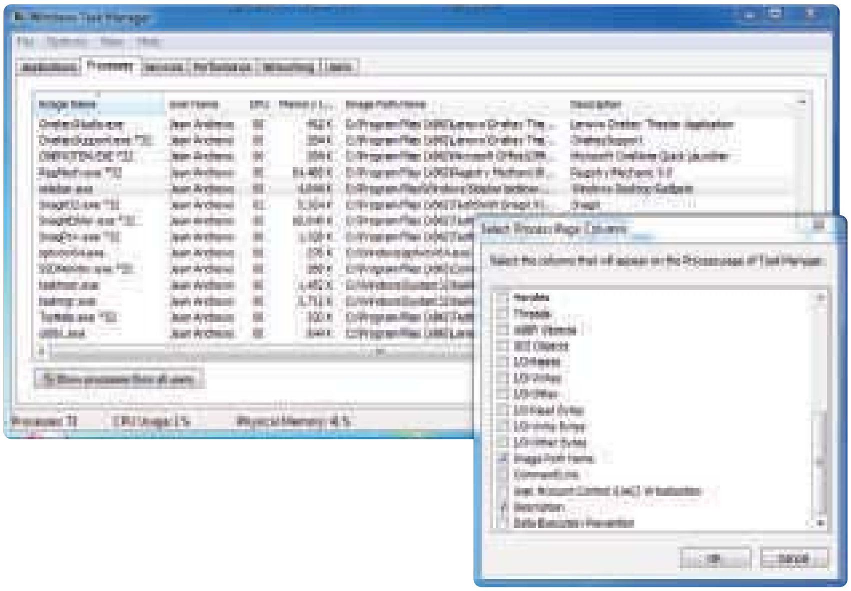
Startup Item	Manufacturer	Command	Location
☑ VerifaceMe...	Unknown	C:\Program Files (x86...	HKLM\SOFTWARE\Wow6432Node\...
☑ MUI StartM...	CyberLink Corp.	"C:\Program Files (x8...	HKLM\SOFTWARE\Wow6432Node\...
☑ MUI StartM...	CyberLink Corp.	"C:\Program Files (x8...	HKLM\SOFTWARE\Wow6432Node\...
☑ SSDMonit A...	PC Tools	C:\Program Files (x86...	HKLM\SOFTWARE\Wow6432Node\...
☑ IAStorIcon	Intel Corporation	C:\Program Files (x86...	HKLM\SOFTWARE\Wow6432Node\...
☑ Microsoft O...	Microsoft Corp...	"C:\Program Files (x8...	HKLM\SOFTWARE\Wow6432Node\...
☑ Adobe Acro...	Adobe System...	"C:\Program Files (x8...	HKLM\SOFTWARE\Wow6432Node\...
☑ Adobe Rea...	Adobe System...	"C:\Program Files (x8...	HKLM\SOFTWARE\Wow6432Node\...
☑ Dropbox	Dropbox, Inc.	C:\Users\JEAN~1\...	C:\Users\Jean Andrews\AppData\...
☑ Microsoft O...	Microsoft Corp...	C:\PROGRA~2\MICR...	C:\Users\Jean Andrews\AppData\...
☑ Delay	Digital Delivery...	C:\PROGRA~2\DDVI...	C:\ProgramData\Microsoft\Windo...

Source: Microsoft Windows 7

Figure 11-47 Find the path and name of the program file in the Command column of System Configuration

Notes The startup folder for all users is hidden by default. In Chapter 3, you learned how to unhide folders that are hidden.

3. As you research startup processes, Task Manager can tell you what processes are currently running. Open Task Manager and select the **Processes** tab. If you see a process and want to know its program file location, click **View** and click **Select Columns**. In the Select Process Page Columns, check **Image Path Name** and click **OK**. The Image Path Name column is added (see Figure 11-48).



Select the columns that will appear on the Process page of Task Manager.

□ Handles
□ Threads
□ USER Objects
□ GDI Objects
□ I/O Reads
□ I/O Writes
□ I/O Other
□ I/O Read Bytes
□ I/O Write Bytes
□ I/O Other Bytes
☑ Image Path Name
□ Command Line
□ User Account Control (UAC) Virtualization
☑ Description
□ Data Execution Prevention

Source: Microsoft Windows 7

Figure 11-48 Use the Image Path Name column on the Processes tab to locate a program file

A+
220-802
4.3

For extremely slow systems that need a more drastic fix, do the following:

- Using Msconfig, disable all startup items on the Startup tab. Then restart the system and see what problems you get into with a program disabled that you really need. Then enable just the ones you decide you need.
- An even more drastic approach for extremely slow startups is to disable all non-Microsoft services. On the Services tab, check **Hide all Microsoft services**, and then click **Disable all**.

Regardless of the method you use, be sure to restart the system after each change and note what happens. Do you get an error message? Does a device or application not work? If so, you have probably disabled a service or program you need.

Has performance improved? If performance does not improve by disabling services or startup programs, go back and enable them again. If no non-Microsoft service or startup program caused the problem, then you can assume the problem is caused by a Microsoft service or startup program. Start disabling them one at a time.

Caution You might be tempted to disable all Microsoft services. If you do so, you are disabling Networking, Event Logging, Error Reporting, Windows Firewall, Windows Installer, Windows Backup, Print Spooler, Windows Update, System Protection, and other important services. These services should be disabled only when testing for performance problems and then immediately enabled when the test is finished. Also, know that if you disable the Volume Shadow Copy service, all restore points kept on the system will be lost. If you intend to use System Restore to fix a problem with the system, don't disable this service. If you are not sure what a service does, read its description in the Services console before you change its status.

Remember that you don't want to permanently leave MSconfig in control of startup. After you have used MSconfig to identify the problem, use other tools to permanently remove them from startup. Use the Services console to disable a service, use the Programs and Features window to uninstall software, and remove program files from startup folders. After the problem is fixed, return MSconfig to a normal startup.

Don't forget to restart the computer after making a change to verify that all is well.

CHECK FOR UNWANTED SCHEDULED TASKS

When applications install, they often schedule tasks to check for and download their program updates, and malware sometimes hides as a scheduled task. Scheduled tasks might be unnecessary and can slow a system down. The best way to uninstall a scheduled task is to uninstall the software that is responsible for the task. Open the Task Scheduler window and search through tasks looking for those you think are unnecessary or causing trouble. Research the software the task works with and then you might decide to uninstall the software or disable the task.

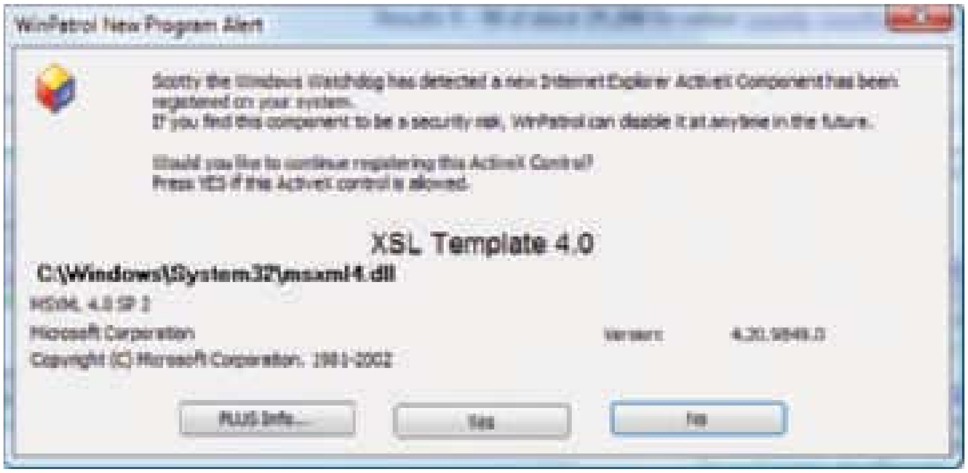
Don't forget to restart the system to make sure all is well before you move on.

MONITOR THE STARTUP PROCESS

Now that you have the startup process clean, you will want to keep it that way. You can use several third-party tools to monitor any changes to startup. A good one is WinPatrol by BillP Studios (*www.winpatrol.com*). Download and install the free version of the

A+
220-802
4.3

program to run in the background to monitor all sorts of things, including changes to the registry, startup processes, Internet Explorer settings, and system files. In Figure 11-49, you can see how WinPatrol gave an alert when it detected an Internet Explorer plug-in is placing an entry in the registry. WinPatrol displays a little black Scotty dog in the notification area of the taskbar to indicate it's running in the background and guarding your system. Also, many antivirus programs monitor the startup process and inform you when changes are made.



WinPatrol New Program Alert

Scotty the Windows Watchdog has detected a new Internet Explorer ActiveX Component has been registered on your system.
If you find this component to be a security risk, WinPatrol can disable it at anytime in the future.

Would you like to continue registering this ActiveX Control?
Press YES if the ActiveX control is allowed.

XSL Template 4.0

C:\Windows\System32\msxml4.dll

MSXML 4.0 SP 2

Microsoft Corporation Version: 4.20.9849.0

Copyright (C) Microsoft Corporation. 1981-2002

Source: WinPatrol

Figure 11-49 WinPatrol by BillP Studios alerts you when a program is making a system change

Hands-on Project 11-7 Monitor Startup Items with WinPatrol

1. Using System Configuration (MSconfig), disable all the non-Windows startup items. Restart your computer.
2. Download and install WinPatrol from *www.winpatrol.com*.
3. Using System Configuration, enable all of the disabled startup items and restart the computer.
4. Are the startup programs able to start? What messages are displayed on the screen?

STEP 3: CHECK IF THE HARDWARE CAN SUPPORT THE OS

The system might be slow because the OS does not have the hardware resources it needs. Use the Windows 7/Vista Windows Experience Index to quickly zero in on a hardware component that might be a bottleneck. If you suspect that the processor, hard drive, or memory is a bottleneck, consider using the Windows 7 Resource Monitor, the Vista Reliability and Performance Monitor, or the XP Performance Monitor to get more detailed information. If the bottleneck appears to be graphics, the problem might be solved by updating the graphics drivers or by updating Windows.

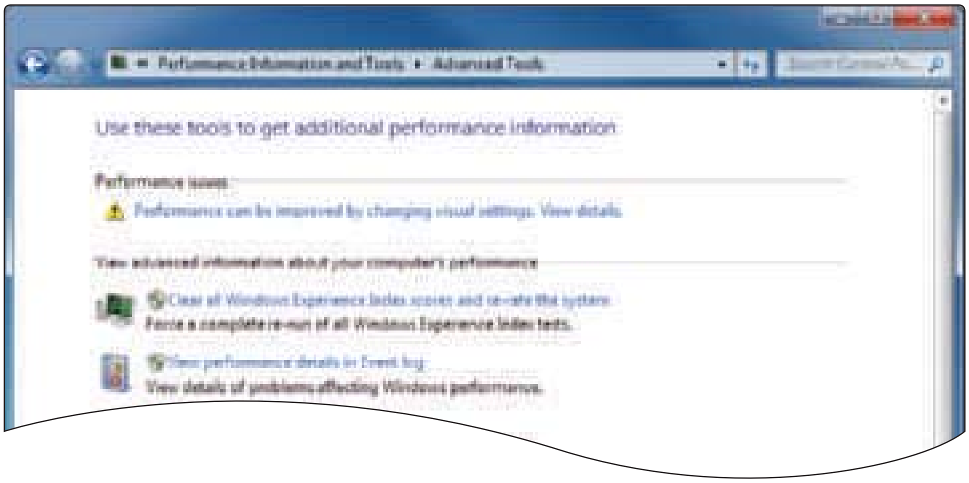
A+
220-802
4.3

Notes Use the System Information Utility (msinfo32.exe) to find information about the installed processor and its speed, how much RAM is installed, and free space on the hard drive. Compare all these values to the minimum and recommended requirements for Windows listed in Chapter 7.

If you find that the system is slow because of a hardware component, discuss the situation with the user. You might be able to upgrade the hardware or install another OS that is compatible with the hardware that is present. Upgrading from Vista to Windows 7 can often improve performance in a computer that has slow hardware components. Better still, perform a clean installation of Windows 7 so that you get a fresh start with installed applications, plug-ins, and background services that might be slowing down the system.

STEP 4: CHECK FOR PERFORMANCE WARNINGS

Windows 7/Vista tracks issues that are interfering with performance. To see these warnings, open the Performance Information and Tools window and click **Advanced tools**. The Advanced Tools window appears, as shown in Figure 11-50. If Windows knows of performance issues, they are listed at the top of this window. Click an issue to see a recommended solution.



Use these tools to get additional performance information

Performance issues

Performance can be improved by changing visual settings. View details.

View advanced information about your computer's performance

Clear all Windows Experience Index scores and re-rate the system
Force a complete re-run of all Windows Experience Index tests.

View performance details in Event log
View details of problems affecting Windows performance.

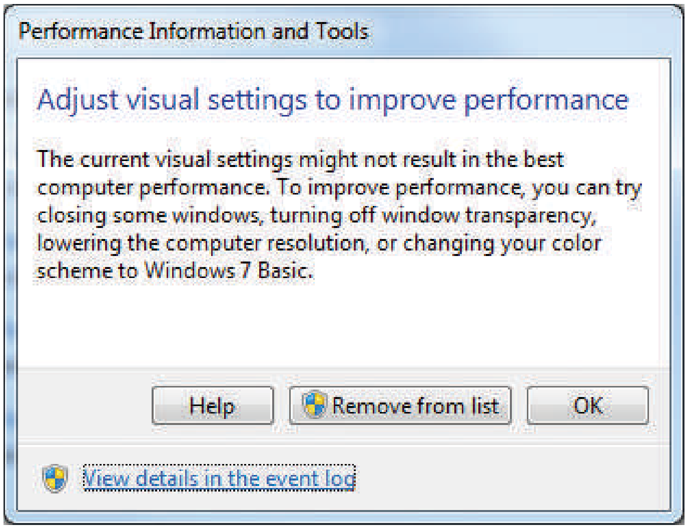
Source: Microsoft Windows 7

Figure 11-50 Windows 7/Vista provides performance warnings and tools to improve Windows performance

For example, when you click the one issue reported in Figure 11-50, a box appears describing the problem and offering solutions (see Figure 11-51). If you make a change to the system while resolving the issue, restart Windows before tackling the next fix or issue. After you have resolved an issue or have decided to live with it, you can click **Remove from list** so that it will no longer appear in the list of issues. If you need more information about an issue, click **View details in the event log** and Event Viewer opens, displaying the appropriate logs.

Windows XP does not offer the Advanced Tools window. For XP, open Event Viewer and view the System log. Look for events that might indicate a performance problem.

A+
220-802
4.3



Performance Information and Tools

Adjust visual settings to improve performance

The current visual settings might not result in the best computer performance. To improve performance, you can try closing some windows, turning off window transparency, lowering the computer resolution, or changing your color scheme to Windows 7 Basic.

Source: Microsoft Windows 7

Figure 11-51 Windows reports that current visual settings are affecting performance.

STEP 5: CHECK FOR A HISTORY OF PROBLEMS

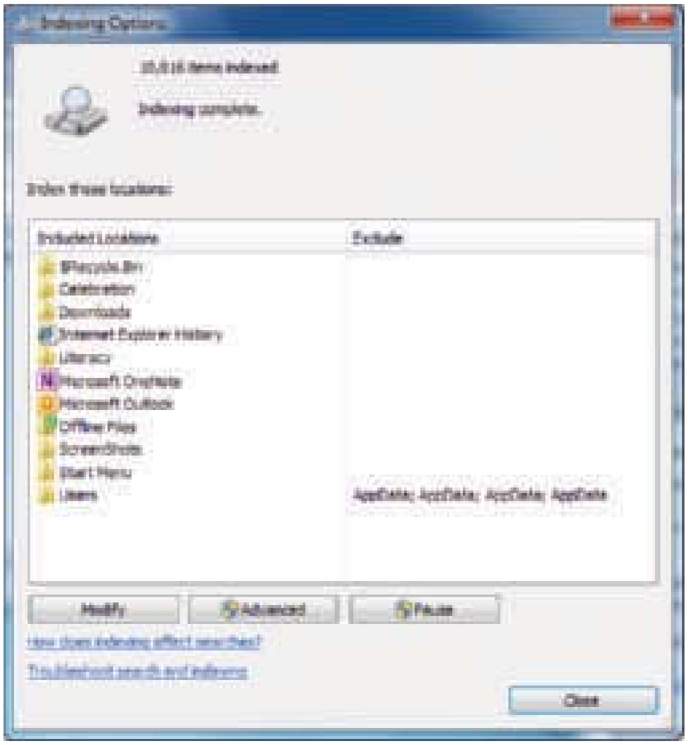
Try to identify when the slow performance problem began, and then use the Windows 7 or Vista Reliability Monitor to find out what changes were made to the system around that time and what other problems occurred. If you don't know when the problem started, skim through the line graph at the top of the Reliability Monitor window and look for drops in the graph. Also look for critical events indicated by a red X (refer to Figure 11-42).

STEP 6: DISABLE THE INDEXER FOR WINDOWS SEARCH

The Windows 7/Vista indexer is responsible for maintaining an index of files and folders on a hard drive to speed up Windows searches. The indexing service has a low priority and only works when it senses that the hard drive is not being accessed by a service with a higher priority. However, it might still slow down performance. Do the following to find out if this service is causing a performance problem:

1. Find out if the indexing service is currently indexing the system. To do that, click **Adjust indexing options** in the left pane of the Performance and Information Tools window. (You can also enter **Indexing Options** in the search box.) The Indexing Options box appears (see Figure 11-52).
2. If you see *Indexing speed is reduced due to user activity* at the top of the box, wait while indexing is in progress and the status changes to *Indexing complete*. You can now stop the indexing service.
3. To stop the indexing service, open the Services console. Then stop and disable the **Windows Search** service (see Figure 11-53).

A+
220-802
4.3


Indexing Options
Modify
Advanced
Pause
How does indexing affect searches?
Troubleshoot search and indexing
Close

15,616 items indexed

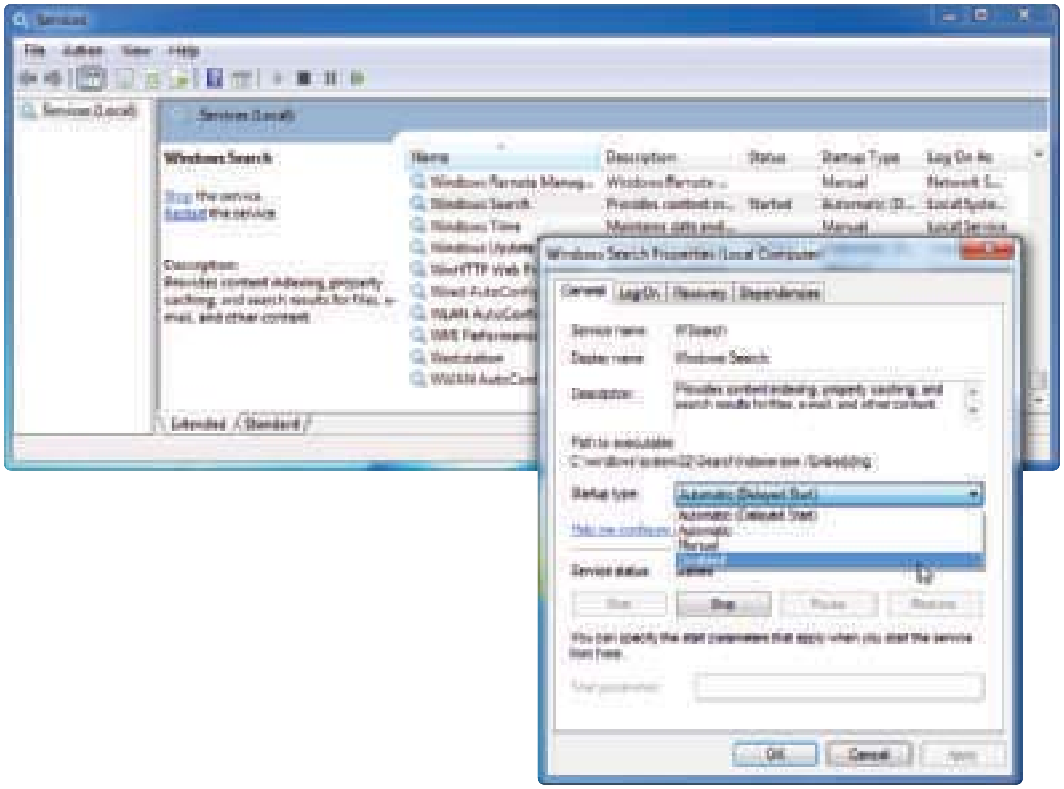
Indexing complete.

Index these locations:

Included Locations	Exclude
$Recycle.Bin	
Celebration	
Downloads	
Internet Explorer History	
Literacy	
Microsoft OneNote	
Microsoft Outlook	
Offline Files	
ScreenShots	
Start Menu	
Users	AppData; AppData; AppData; AppData

Source: Microsoft Windows 7

Figure 11-52 Indexing is enabled on this system



Windows Search

Description:
Provides content indexing, property caching, and search results for files, e-mail, and other content.

Name	Description	Status	Startup Type	Log On As
Windows Remote Manag...	Windows Remote ...		Manual	Network S...
Windows Search	Provides content in...	Started	Automatic (D...	Local Syste...
Windows Time	Maintains date and...		Manual	Local Service
Windows Update				
WinHTTP Web Pr				
Wired AutoConfig				
WLAN AutoConfig				
WMI Performance				
Workstation				
WWAN AutoConf				

Service name: WSearch

Display name: Windows Search

Description: Provides content indexing, property caching, and search results for files, e-mail, and other content.

Path to executable:
C:\windows\system32\SearchIndexer.exe /Embedding

Startup type: Automatic (Delayed Start)

Automatic (Delayed Start)
Automatic
Manual
Disabled

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Source: Microsoft Windows 7

Figure 11-53 Disable the Windows Search service

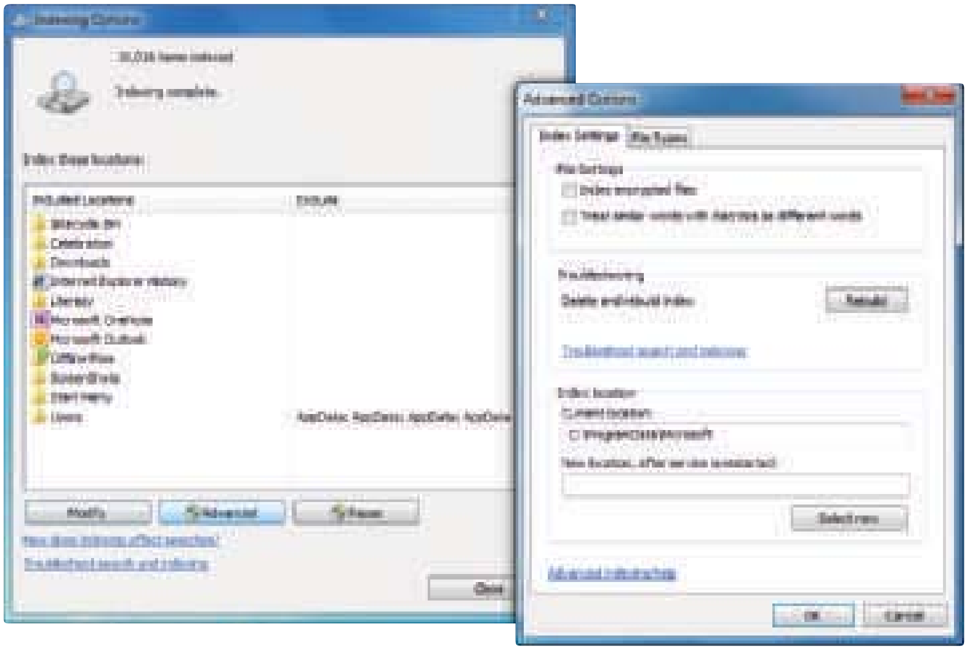
A+
220-802
4.3

4. Restart the computer. Run the system for a while and see if performance improves.

5. If performance does not improve, restart the indexing service. To do that, use the Services console to set the status of the Windows Search service to **Automatic** (**Delayed Start**) and start the service. Then move on to the next section of this chapter, *Step 7: Plug Up Any Memory Leaks*.

6. If performance does improve, it is possible that the problem was caused by a corrupted index database. To rebuild the database, first use the Services console to set the Windows Search service status back to **Automatic** (**Delayed Start**) and to start the service.

7. Open the Indexing Options box and click **Advanced**. The Advanced Options box opens (see Figure 11-54).



Source: Microsoft Windows 7

Figure 11-54 Rebuild the indexing database

8. To rebuild the indexing database, click **Rebuild**. A dialog box appears warning you that this can take some time. Click **OK**. Close the Indexing Options box.

9. After running the system for a while, if the performance problem returns, you can disable the Windows Search service and leave it disabled. However, know that searching will not be as fast without indexing.

STEP 7: PLUG UP ANY MEMORY LEAKS

If you notice that performance slows after a system has been up and running without a restart for some time, suspect a memory leak. A memory leak is caused when an application does not properly release memory allocated to it that it no longer needs and continually requests more memory than it needs.

To see how much memory an application has allocated to it that is not available to other programs, open Task Manager and click the **Processes** tab. In the menu bar, click **View**, **Select Columns**. Verify that the Memory Private Working Set, Handles, and Threads

A+
220-802
4.3

columns are checked and click **OK**. If you observe that the values in these three columns increase over time for a particular program, suspect the program has a memory leak. To sort the data by one column, click the column label. For example, the Task Manager window shown in Figure 11-55 is sorted by Memory. It shows the memory-hungry applications on this system are Eudora (an email client) and Skype (an Internet voice and video program).

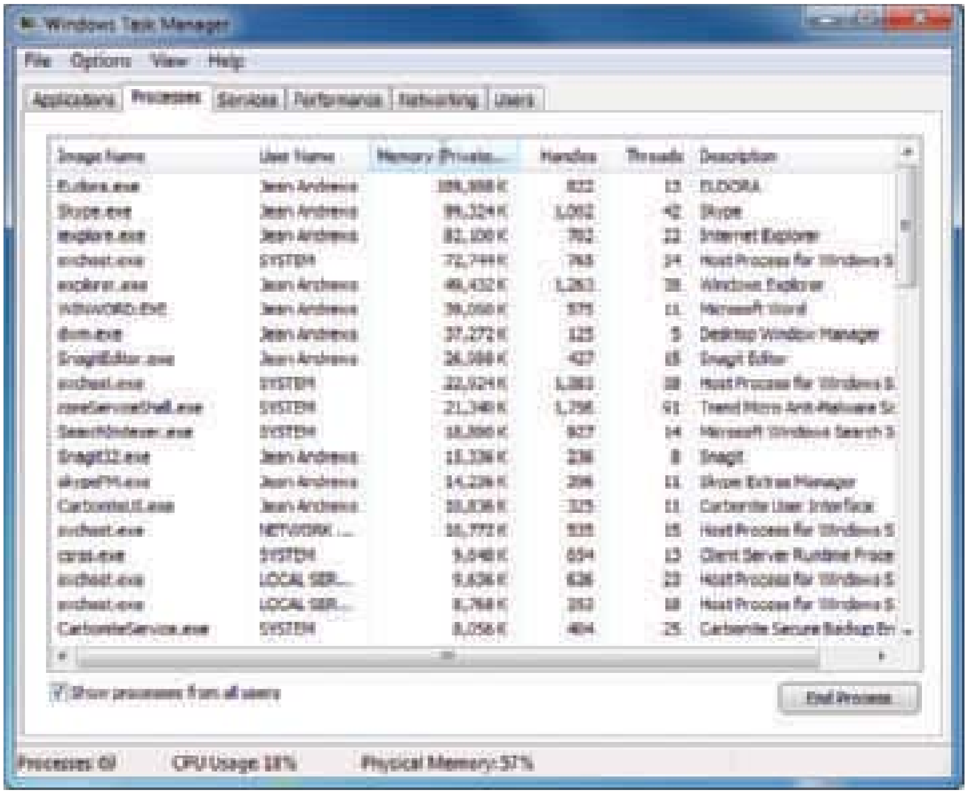

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
☑ Show processes from all users
End Process

Image Name	User Name	Memory (Private...	Handles	Threads	Description
Eudora.exe	Jean Andrews	109,908 K	822	13	EUDORA
Skype.exe	Jean Andrews	99,324 K	1,062	42	Skype
iexplore.exe	Jean Andrews	82,100 K	782	22	Internet Explorer
svchost.exe	SYSTEM	72,744 K	768	34	Host Process for Windows S
explorer.exe	Jean Andrews	49,432 K	1,263	38	Windows Explorer
WINWORD.EXE	Jean Andrews	39,056 K	575	11	Microsoft Word
dwm.exe	Jean Andrews	37,272 K	125	5	Desktop Window Manager
SnagitEditor.exe	Jean Andrews	26,088 K	427	15	Snagit Editor
svchost.exe	SYSTEM	22,624 K	1,083	38	Host Process for Windows S
coreServiceShell.exe	SYSTEM	21,340 K	1,758	91	Trend Micro Anti-Malware S
SearchIndexer.exe	SYSTEM	18,800 K	927	14	Microsoft Windows Search I
Snagit32.exe	Jean Andrews	15,336 K	236	8	Snagit
skypePM.exe	Jean Andrews	14,236 K	398	11	Skype Extras Manager
CarboniteUI.exe	Jean Andrews	10,836 K	325	11	Carbonite User Interface
svchost.exe	NETWORK ...	10,772 K	535	15	Host Process for Windows S
csrss.exe	SYSTEM	9,848 K	654	13	Client Server Runtime Proce
svchost.exe	LOCAL SER...	9,636 K	628	23	Host Process for Windows S
svchost.exe	LOCAL SER...	8,768 K	252	18	Host Process for Windows S
CarboniteService.exe	SYSTEM	8,056 K	404	25	Carbonite Secure Backup En

Processes: 69 CPU Usage: 18% Physical Memory: 57%

Source: Microsoft Windows 7

Figure 11-55 Task Manager shows how memory is allocated for an application

Note that the Windows 7 Resource Monitor and the Vista Reliability and Performance Monitor give similar information about how memory is used. If you decide a program has a memory leak, try to get an update or patch from the program manufacturer's web site.

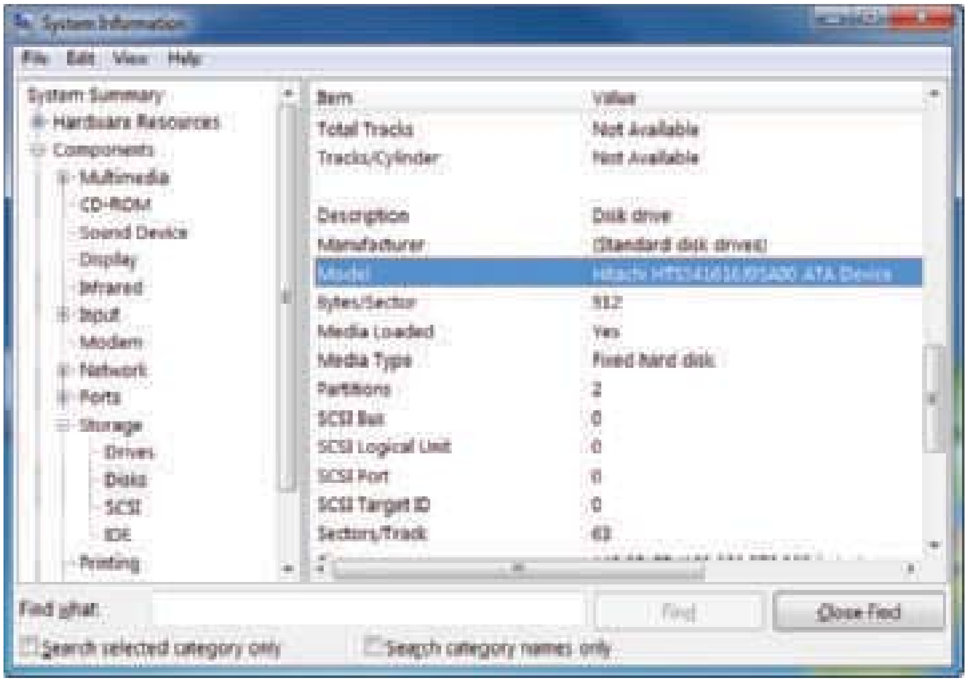
A+
220-802
1.1, 4.3

STEP 8: CONSIDER USING READYBOOST

Windows 7/Vista **ReadyBoost** uses a flash drive or secure digital (SD) memory card to boost hard drive performance. The faster flash memory is used as a buffer to speed up hard drive access time. You see the greatest performance increase using ReadyBoost when you have a slow magnetic hard drive (running at less than 7200 RPM). To find out what speed your hard drive is using, use System Information (Msinfo32.exe) and drill down into the Components, Storage group, and select Disks (see Figure 11-56). The model of the hard drive appears in the right pane. Use Google to search on this brand and model; a quick search shows this drive runs at 5400 RPM. It's, therefore, a good candidate to benefit from ReadyBoost.

A+ Exam Tip The A+ 220-802 exam expects you to know how to use ReadyBoost to improve performance.

A+
220-802
1.1, 4.3



System Information

File Edit View Help

- System Summary
  - Hardware Resources
  - Components
    - Multimedia
    - CD-ROM
    - Sound Device
    - Display
    - Infrared
    - Input
    - Modem
    - Network
    - Ports
    - Storage
      - Drives
      - Disks
      - SCSI
      - IDE
    - Printing

Item	Value
Total Tracks	Not Available
Tracks/Cylinder	Not Available
Description	Disk drive
Manufacturer	(Standard disk drives)
Model	Hitachi HTS541616J9SA00 ATA Device
Bytes/Sector	512
Media Loaded	Yes
Media Type	Fixed hard disk
Partitions	2
SCSI Bus	0
SCSI Logical Unit	0
SCSI Port	0
SCSI Target ID	0
Sectors/Track	63

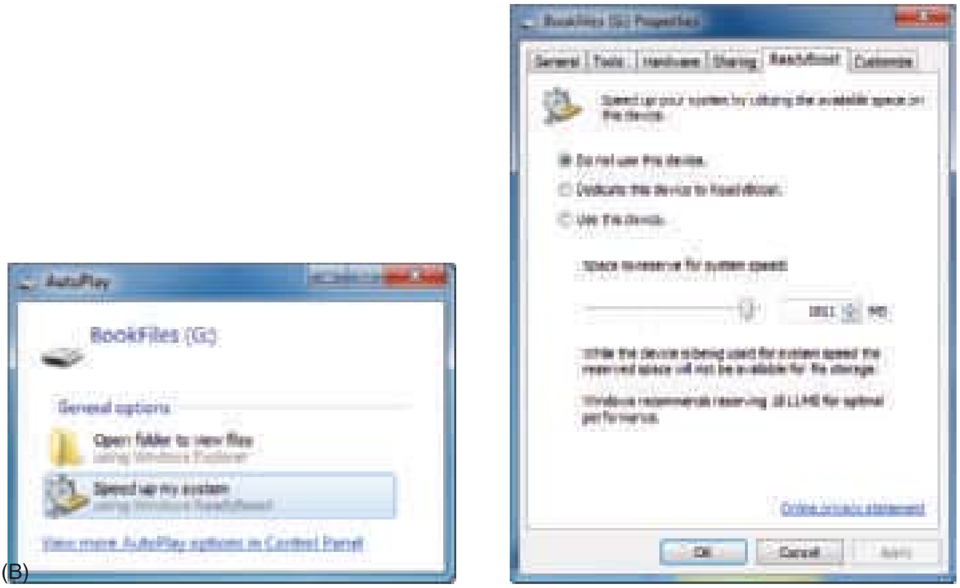
Find what: Find Close Find

□ Search selected category only □ Search category names only

Source: Microsoft Windows 7

Figure 11-56 Use the System Information window to find out the brand and model of your hard drive

When you first connect a flash device, Windows will automatically test it to see if it qualifies for ReadyBoost. To qualify, it must have a capacity of 256 MB to 4 GB with at least 256 MB of free space, and run at about 2 MB/sec of throughput. If the device qualifies, Windows displays a dialog box that can be used to activate ReadyBoost (see Figure 11-57a). When you click **Speed up my system,** the device properties box appears with the ReadyBoost tab selected (see Figure 11-57b). Here you can decide how much of the device memory to



AutoPlay

BookFiles (G:)

General options

Open folder to view files
using Windows Explorer

Speed up my system
using Windows ReadyBoost

View more AutoPlay options in Control Panel

BookFiles (G:) Properties

General | Tools | Hardware | Sharing | ReadyBoost | Customize

Speed up your system by utilizing the available space on this device.

● Do not use this device.

○ Dedicate this device to ReadyBoost.

○ Use this device.

Space to reserve for system speed:

[illegible] MB

While the device is being used for system speed, the reserved space will not be available for file storage.

Windows recommends reserving [illegible] MB for optimal performance.

Online privacy statement

OK Cancel Apply

(A)(B)

Source: Microsoft Windows 7

Source: Microsoft Windows 7

Figure 11-57 Windows asks permission to use the device for ReadyBoost

A+
220-802
1.1, 4.3

allot for ReadyBoost. You can manually have Windows test a memory card or flash drive for ReadyBoost by right-clicking the device and selecting **Properties** from the shortcut menu. On the device properties window, click the **ReadyBoost** tab.

The best flash devices to use for ReadyBoost are the ones that can take advantage of the faster ports. For example, a SuperSpeed USB (USB 3.0) device and port is about 10 times faster than a Hi-Speed USB (USB 2.0) device and port. Incidentally, when you remove the device, no data is lost because the device only holds a copy of the data.

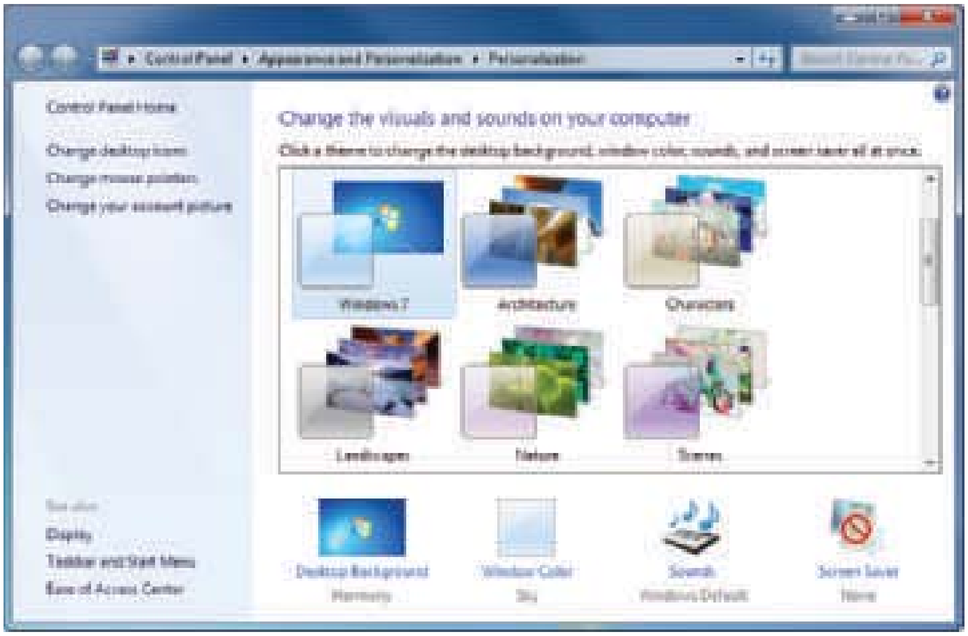
A+
220-802
4.3

STEP 9: DISABLE THE AERO INTERFACE

The Windows Aero interface might be slowing down the system because it uses memory and computing power. Try disabling it. If performance improves, you can conclude that the hardware is not able to support the Aero interface. At that point, you might want to upgrade memory, upgrade the video card, or leave the Aero interface disabled.

To disable the Aero interface using Windows 7, do the following:

1. Right-click the desktop and select **Personalize** from the shortcut menu. The Personalization window opens (see Figure 11-58).
2. Scroll down to and click **Windows 7 Basic** and close the window.



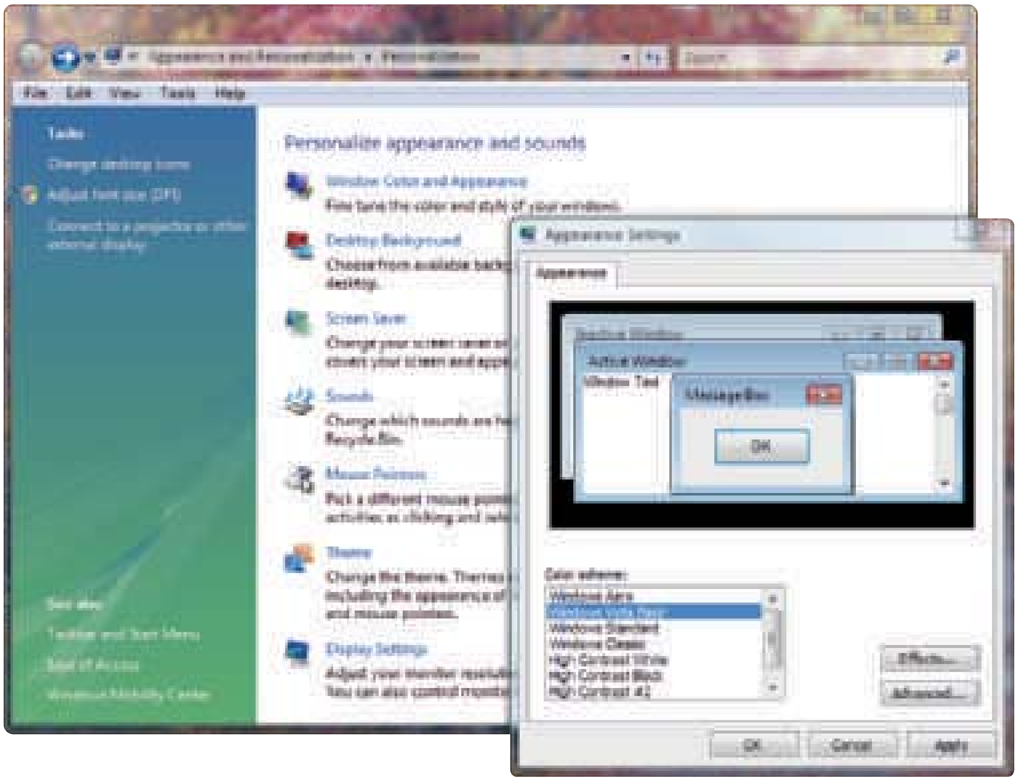
Source: Microsoft Windows 7

Figure 11-58 Disable the Windows 7 Aero interface to conserve system resources

To disable the Aero interface using Windows Vista, follow these steps:

1. Open the Personalization window and click **Window Color**. Then click **Open classic appearance properties for more color options**. The Appearance Settings box opens, shown on the right side of Figure 11-59.
2. Under Color scheme, select **Windows Vista Basic** and click **Apply**. Close the dialog box and window.

A+
220-802
4.3


Appearance and Personalization ▸ Personalization
Search
File Edit View Tools Help
Tasks
Change desktop icons
Adjust font size (DPI)
Connect to a projector or other external display
See also
Taskbar and Start Menu
Ease of Access
Windows Mobility Center
Personalize appearance and sounds
Window Color and Appearance
Fine tune the color and style of your windows.
Desktop Background
Choose from available backg... desktop.
Screen Saver
Change your screen saver or... covers your screen and appe...
Sounds
Change which sounds are he... Recycle Bin.
Mouse Pointers
Pick a different mouse poin... activities as clicking and sele...
Theme
Change the theme. Themes c... including the appearance of... and mouse pointers.
Display Settings
Adjust your monitor resolutio... You can also control monito...
Appearance Settings
Appearance
Inactive Window
Active Window
Window Text
Message Box
OK
Effects...
Advanced...
OK
Cancel
Apply

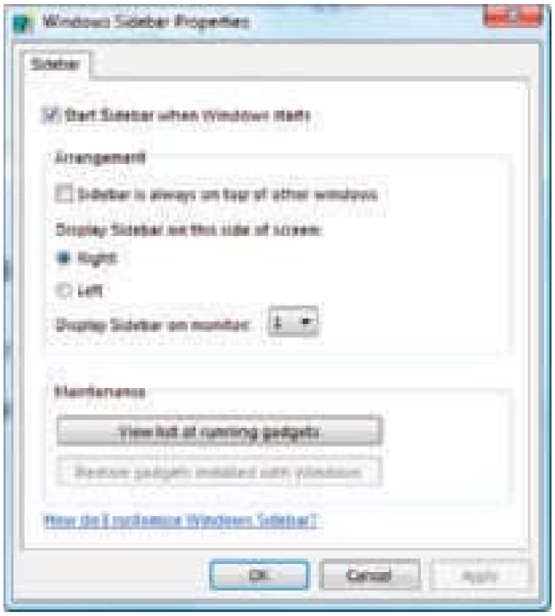
Color scheme:
- Windows Aero
- Windows Vista Basic
- Windows Standard
- Windows Classic
- High Contrast White
- High Contrast Black
- High Contrast #1

Source: Microsoft Vista

Figure 11-59 Disable the Windows Vista Aero interface to conserve system resources

STEP 10: DISABLE THE VISTA SIDEBAR

Recall that the Vista sidebar appears on the Windows desktop to hold apps called gadgets. The sidebar uses system resources and disabling it can improve performance. To do that, right-click the sidebar and select **Properties** from the shortcut menu. The Windows Sidebar Properties box appears (see Figure 11-60). Uncheck **Start Sidebar when Windows starts**. Then click **Apply** and **OK** to close the box.


Windows Sidebar Properties
Sidebar
Arrangement
Maintenance
View list of running gadgets
Restore gadgets installed with Windows
How do I customize Windows Sidebar?
OK
Cancel
Apply

☑ Start Sidebar when Windows starts

☐ Sidebar is always on top of other windows

Display Sidebar on this side of screen:
● Right
○ Left

Display Sidebar on monitor: 1

Source: Microsoft Vista

Figure 11-60 Disable the Vista sidebar to improve performance

MANUALLY REMOVING SOFTWARE

A+
220-802
4.3

In this part of the chapter, we focus on getting rid of programs that refuse to uninstall or give errors when uninstalling. In these cases, you can manually uninstall a program. Doing so often causes problems later, so use the methods discussed in this section only as a last resort after normal uninstall methods have failed.

This part of the chapter discusses the following steps to manually remove software:

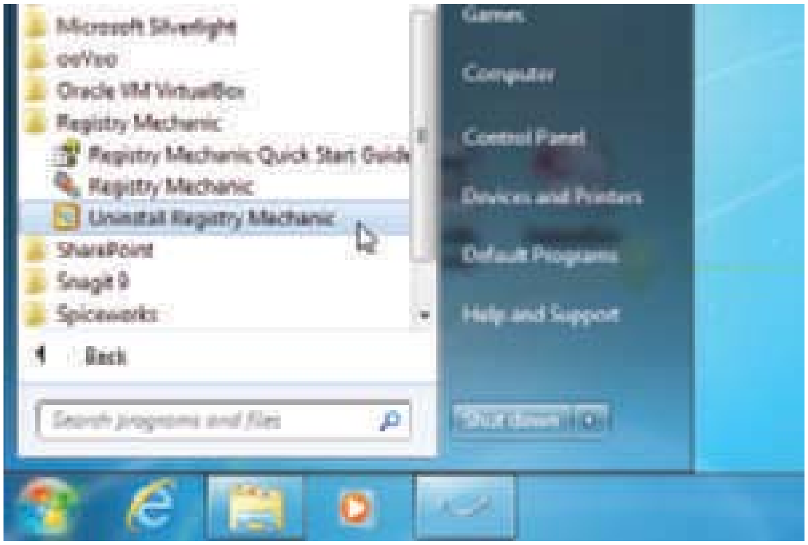
1. First try to locate and use an uninstall routine provided by the software. If this works, you are done and can skip the next steps.
2. Delete the program folders and files that hold the software.
3. Delete the registry entries used by the software.
4. Remove the entries in the Start menu and delete any shortcuts on the desktop.
5. Remove any entries that launch processes at startup.

Notes Before uninstalling software, make sure it's not running in the background. For example, antivirus software cannot be uninstalled if it's still running. You can use Task Manager to end all processes related to the software, and you can use the Services console to stop services related to the software. Then remove the software.

Now let's step through the process of manually removing software.

STEP 1: FIRST TRY THE UNINSTALL ROUTINE

Most programs written for Windows have an uninstall routine that can be accessed from the Windows 7/Vista Programs and Features window, the XP Add Remove Programs window, or an uninstall utility in the All Programs menu. For example, in Figure 11-61, you can see in the All Programs menu that an uninstall item is listed for the Registry Mechanic software installation. (Registry Mechanic is utility software that can clean the registry of unused keys.) Click this option and follow the directions on-screen to uninstall the software. Alternately, you can use the Programs and Features window to uninstall the software.



Source: Microsoft Windows 7

Figure 11-61 Most applications have an uninstall utility included with the software

A+
220-802
4.3

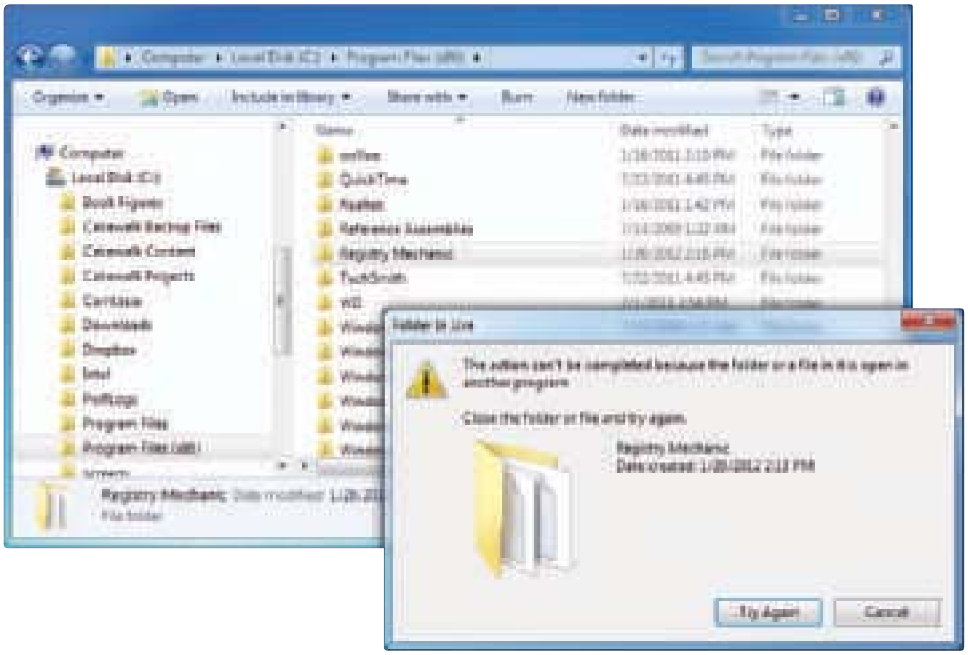
STEP 2: DELETE PROGRAM FILES

If the uninstall routine is missing or does not work, the next step is to delete the program folders and files that contain the software. In our example, we'll delete the Registry Mechanic software without using its uninstall routine.

Look for the program folder in one of these folders:

- C:\Program Files
- C:\Program Files (x86)

In Figure 11-62, you can see the Registry Mechanic folder under the C:\Program Files (x86) folder. Keep in mind, however, the program files might be in another location that was set by the user when the software was installed. Delete the **Registry Mechanic** folder and all its contents.



The action can't be completed because the folder or a file in it is open in another program

Close the folder or file and try again.

Registry Mechanic
Date created: 1/20/2012 2:12 PM

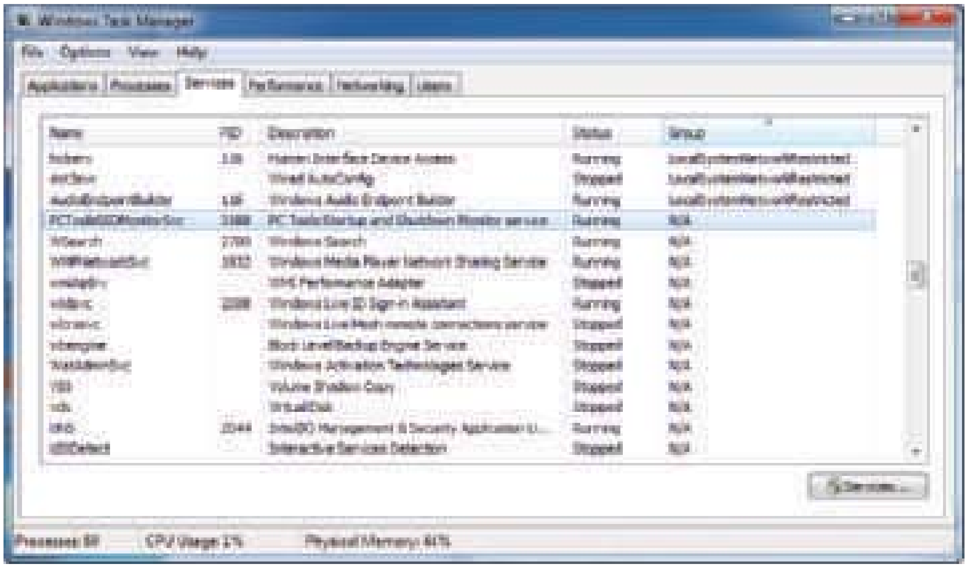
Source: Microsoft Windows 7

Figure 11-62 Program files are usually found in the Program Files or Program Files (x86) folder

As you do, you might see the warning box shown on the right side of Figure 11-62 saying the program is in use. In this situation, do the following:

1. Look for the program file reported on the Processes tab of Task Manager. If you see it listed, end the process. The Command Line column can help you find the right program.
2. If you don't find the program on the Processes tab, check the **Services** tab. If you find it there, select it and click **Services** (see Figure 11-63). The Services console opens where you can stop the service. (Note in the figure the Registry Mechanic software by PC Tools is running under the PC Tools name.)
3. After the program or service is stopped, try to delete the program folder again. If you still cannot delete the folder, look for other running programs or services associated with the software.

A+
220-802
4.3


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Services...

Name	PID	Description	Status	Group
hidserv	328	Human Interface Device Access	Running	LocalSystemNetworkRestricted
dot3svc		Wired AutoConfig	Stopped	LocalSystemNetworkRestricted
AudioEndpointBuilder	618	Windows Audio Endpoint Builder	Running	LocalSystemNetworkRestricted
PCToolsSSDMonitorSvc	3388	PC Tools Startup and Shutdown Monitor service	Running	N/A
WSearch	2700	Windows Search	Running	N/A
WMPNetworkSvc	3832	Windows Media Player Network Sharing Service	Running	N/A
wmiApSrv		WMI Performance Adapter	Stopped	N/A
wlidsvc	2208	Windows Live ID Sign-in Assistant	Running	N/A
wlcrasvc		Windows Live Mesh remote connections service	Stopped	N/A
wbengine		Block Level Backup Engine Service	Stopped	N/A
WatAdminSvc		Windows Activation Technologies Service	Stopped	N/A
VSS		Volume Shadow Copy	Stopped	N/A
vds		Virtual Disk	Stopped	N/A
UNS	2044	Intel(R) Management & Security Application U...	Running	N/A
UI0Detect		Interactive Services Detection	Stopped	N/A

Processes: 69 CPU Usage: 1% Physical Memory: 41%

Source: Microsoft Windows 7

Figure 11-63 Task Manager shows a service is running and needs to be stopped before the program files can be deleted

STEP 3: DELETE REGISTRY ENTRIES

Editing the registry can be dangerous, so do this with caution and be sure to back up first! Do the following to delete registry entries that cause a program to be listed as installed software in the Windows 7/Vista Programs and Features window or the XP Add or Remove Programs window of Control Panel:

1. To be on the safe side, back up the entire registry using one or more of the methods discussed earlier in the chapter.
2. Open the Registry Editor by using the **regedit** command in the search box.
3. Locate a key that contains the entries that make up the list of installed software. Use this criteria to decide which key to locate:
   - For a 32-bit program installed in a 32-bit OS or for a 64-bit program installed in a 64-bit OS, locate this key:
     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
   - For a 32-bit program installed in a 64-bit OS, locate this key:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

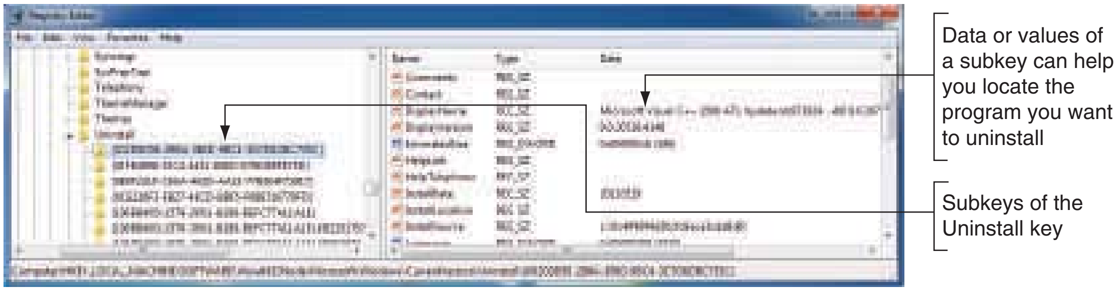
> **Notes** Recall that 32-bit programs are installed the \Program Files (x86) folder on a 64-bit system. These 32-bit programs use the Wow6432Node subkey in the registry of a 64-bit OS.

4. Back up the Uninstall key to the Windows desktop so that you can backtrack, if necessary. To do that, right-click the Uninstall key and select **Export** from the shortcut menu (see Figure 11-34 earlier in the chapter).

A+
220-802
4.3

5. In the Export Registry File dialog box, select the **Desktop**. Enter the filename as **Save Uninstall Key**, and click **Save**. You should see a new file icon on your desktop named Save Uninstall Key.reg.

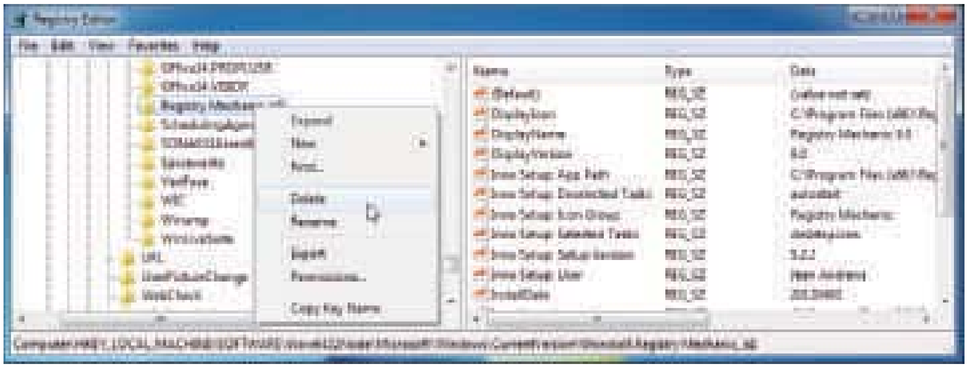
6. The Uninstall key can be a daunting list of all the programs installed on your PC. When you expand the key, you see a long list of subkeys in the left pane, which might have meaningless names that won't help you find the program you're looking for. Select the first subkey in the Uninstall key and watch as its values and data are displayed in the right pane (see Figure 11-64). Step down through each key, watching for a meaningful name of the subkey in the left pane or meaningful details in the right pane until you find the program you want to delete.


Data or values of a subkey can help you locate the program you want to uninstall
Subkeys of the Uninstall key

Source: Microsoft Windows 7

Figure 11-64 Select a subkey under the Uninstall key to display its values and data in the right pane

7. To delete the key, right-click the key and select **Delete** from the shortcut menu (see Figure 11-65) and confirm the deletion. Be sure to search through all the keys in this list because the software might have more than one key. Delete them all and exit the Registry Editor.



Source: Microsoft Windows 7

Figure 11-65 Delete the registry key that lists the software as installed software

8. Open the Windows 7/Vista Programs and Features window or the XP Add or Remove Programs window and verify that the list of installed software is correct and the software you are uninstalling is no longer listed.

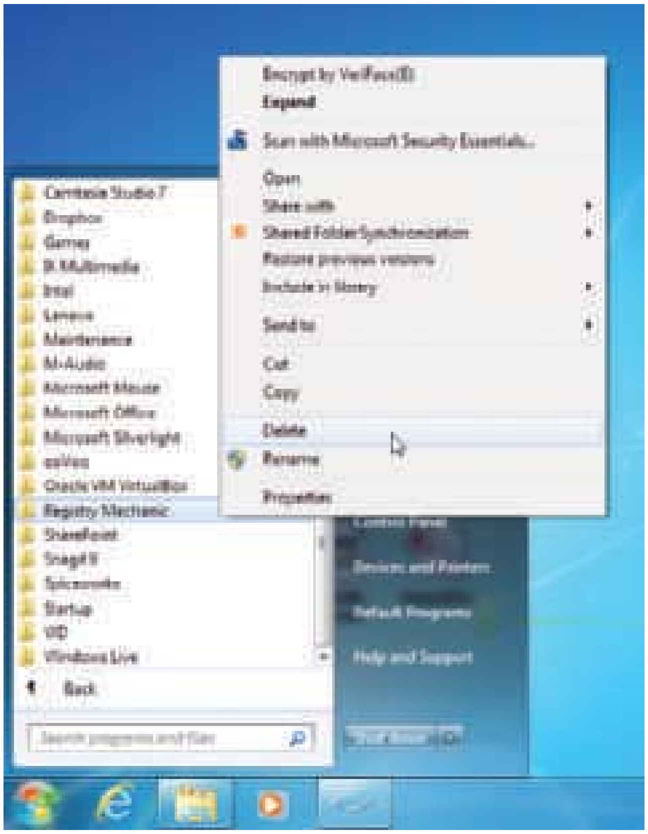
9. If the list of installed software is not correct, to restore the Uninstall registry key, double-click the **Save Uninstall Key.reg** icon on your desktop.

10. As a last step when editing the registry, clean up after yourself by deleting the Save Uninstall Key.reg file on your desktop. Right-click the icon and select **Delete** from the shortcut menu.

A+
220-802
4.3

STEP 4: REMOVE THE PROGRAM FROM THE ALL PROGRAMS MENU AND THE DESKTOP

To remove the program from the All Programs menu, right-click it and select **Delete** from the shortcut menu (see Figure 11-66). If the program has shortcuts on the desktop, delete these.



Source: Microsoft Windows 7

Figure 11-66 Delete the program from the All Programs menu

STEP 5: REMOVE STARTUP PROCESSES

Restart the PC and watch for any startup errors about a missing program file. The software might have stored startup entries in the registry, in startup folders, or as a service that is no longer present and causing an error. If you see an error, use MSconfig to find out how the program is set to start. This entry point is called an orphaned entry. You'll then need to delete this startup entry by editing the registry, deleting a shortcut in a startup folder, or disabling a service using the Services console.

It's unlikely you will be able to completely remove all keys in the registry that the software put there. A registry cleaner can help you find these orphaned keys, but if no errors appear at startup, you can just leave these keys untouched. Also, an installation might put program files in the C:\Program Files\Common Files or the C:\Program Files (x86)\Common Files folder. Most likely you can just leave these untouched as well. Address all error messages you encounter and stop there.

REGISTRY KEYS THAT AFFECT STARTUP AND LOGON EVENTS

You have just seen how you can edit the registry to remove the entries left there by software that you have manually removed. If a system is giving repeated startup errors or you have just removed several programs, you might want to search through registry keys where

A+
220-802
4.3

startup processes can be located. See Appendix G for a list of these registry keys and startup folders. As you read through this list of registry keys to search, know that the list is not exhaustive. With experience, you'll learn that the registry is an ever-changing landscape of keys and values.

Hands-on Project 11-8 Practice Manually Removing Software

To practice your skills of manually removing software, install WinPatrol from *www.winpatrol.com*. (If you did Project 11-2, the software is already installed.) Then, following the directions in the chapter, manually remove the software, listing the steps you used. (Do not use the uninstall routine provided by WinPatrol.) After you have manually removed the software, reboot the system. Did you get any error messages?

>> CHAPTER SUMMARY

Windows Utilities and Tools to Support the OS

- The Windows OS is made up of two main components, the shell and the kernel. The shell provides an interface for users and applications. The kernel is responsible for interacting with hardware.
- A process is a program running under the shell, together with all the resources assigned to it. A thread is a single task that a process requests from the kernel.
- Task Manager (Taskmgr.exe) lets you view services and other running programs, CPU and memory performance, network activity, and user activity. It is useful to stop a process that is hung.
- Tools listed in the Administrative Tools group of Control Panel are used by technicians and developers to support Windows and applications.
- System Configuration (Msconfig.exe) can be used to temporarily disable startup processes to test for performance improvement and find a startup program causing a problem.
- The Services console (Services.msc) is used to manage Windows and application services. When and if a service starts can be controlled from this console.
- The Computer Management console (Compmgmt.msc) contains a group of Windows administrative tools useful for managing a system.
- The Microsoft Management Console (MMC) can be used to build your own custom consoles from available snap-ins.
- The Event Viewer (Eventvwr.msc) console displays a group of logs kept by Windows that are useful for troubleshooting problems with software and hardware. You can also use Event Viewer to view security audits made by Windows.
- The Registry Editor (Regedit.exe) is used to edit the registry in real time. There is no way to use the Registry Editor to undo changes you make to the registry. Therefore, you should always make a backup before editing it.

- The Performance Information and Tools window displays the Windows Experience Index that rates the overall performance of the system. You can reach tools to optimize performance from this window.
- Windows 7 Resource Monitor monitors the performance of the processor, memory, hard drive, and network in real time.
- The Windows 7 Reliability Monitor can be used to get historical data about problems on the computer since Windows was installed.
- The Windows 7 Performance Monitor uses counters to track activity by hardware and software to evaluate performance.
- The Vista Reliability and Performance Monitor (Perfmon.msc) is an earlier version of the three separate tools in Windows 7: the Resource Monitor, Reliability Monitor, and Performance Monitor.
- The XP Performance Monitor (also called the System Monitor) uses counters and is an earlier version of the Windows 7 Performance monitor.

Improving Windows Performance

- The 10 high-level steps to improve Windows performance are (1) routine maintenance, (2) clean Windows startup, (3) check if hardware can support the OS, (4) check for performance warnings, (5) check for a history of problems to find the source of a problem, (6) disable indexing for Windows search, (7) plug up memory leaks, (8) consider using ReadyBoost to improve a slow hard drive's performance, (9) disable the Aero interface, and (10) disable the Vista sidebar.
- Tools that can be used to investigate and clean up the Windows start process include Safe Mode, startup folders, MSconfig, Task Scheduler, Task Manager, and Services console.

Manually Removing Software

- If software does not uninstall using the Windows 7/Vista Programs and Features window or the XP Add or Remove Programs window, you can manually uninstall the software.
- To manually delete software, delete the program files, entries in the Start, All Programs menu, registry keys, and items in startup folders.

>> KEY TERMS

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

Administrative tools
Computer Management (Compmgmt.msc)
console
data collector set
Event Viewer (Eventvwr.msc)
executive services
HAL (hardware abstraction layer)
HKEY_CLASSES_ROOT (HKCR)
HKEY_CURRENT_CONFIG (HKCC)
HKEY_CURRENT_USER (HKCU)
HKEY_LOCAL_MACHINE (HKLM)
HKEY_USERS (HKU)
kernel
kernel mode
Microsoft Management Console (MMC)
Performance Information and Tools
Performance Monitor
process
ReadyBoost
registry
Registry Editor (regedit.exe)
Reliability and Performance Monitor (Perfmon.msc)
Reliability Monitor
Resource Monitor
Services console
shell
snap-ins
System Configuration (Msconfig.exe)
System Monitor
Task Manager (Taskmgr.exe)
Task Scheduler
thread
user mode

>> REVIEWING THE BASICS

1. List four ways to start Task Manager.
2. If a program is not responding, how can you stop it?
3. If a necessary program is using too much of the system resources and bogging down other applications, what can you do to fix the problem?
4. How can you view a list of users currently logged onto the computer?
5. What is the program filename and extension of System Configuration?
6. Which Windows 7 tool can be used to see a history of problems a computer has had since Windows was installed?
7. What tool in Windows Vista, used to temporarily disable a startup program, is not available in Windows 7 or Windows XP?
8. If a nonessential service is slowing down startup, how can you permanently disable it?
9. What should be the startup type of a service that should not load at startup but might be used later after startup? What tool can you use to set a service's startup type?
10. List three snap-ins that can be found in the Computer Management console that are used to manage hardware and track problems with hardware.
11. What is the file extension of a console that is managed by Microsoft Management Console?
12. Name the program filename and file extension for the Microsoft Management Console.
13. Which log in Event Viewer would you use to find out about attempted logins to a computer?
14. Which log in Event Viewer would you use if you suspect a problem with the hard drive?
15. Which three Windows 7 tools are contained in the Vista Reliability and Performance Monitor?
16. What is the path to the Ntuser.dat file in Windows 7?
17. How is the Ntuser.dat file used?
18. Which registry key contains information that Device Manager uses to display information about hardware?
19. Which Windows 7/Vista tool can give you a quick report of the overall performance of the system expressed as a single number?
20. To improve Windows performance, you decide to disable the indexer used for Windows search. Will Windows search still work?
21. What three indicators in Task Manager can be used to find which program has a memory leak?
22. What key do you press at startup to load the system in Safe Mode?
23. If performance improves when Windows is loaded in Safe Mode, what can you conclude?
24. If performance does not improve when Windows is loaded in Safe Mode, what can you conclude?

25. When using MSconfig to stop startup services including Microsoft services, which service should you not stop so that restore points will not be lost?
26. In what folder does Task Scheduler keep scheduled tasks?
27. What are the two folders where, by default, Windows stores installed software?
28. What must you do first before you can delete the program folder containing software that is running in the background?
29. What is the purpose of the Wow6432Node subkey in the Windows registry?
30. What is the name of the window used to uninstall software in Windows 7/Vista?

>> THINKING CRITICALLY

1. You need to install a customized console on 10 computers. What is the best way to do that?
   a. When installing the console on the first computer, write down each step to make it easier to do the same chore on the other nine.
   b. Create the console on one computer and copy the .mmc file to the other nine.
   c. Create the console on one computer and copy the .msc file to the other nine.
2. What is the name of the program that you can enter in the search box to execute Event Viewer? What is the process that is running when Event Viewer is displayed on the screen? Why do you think the running process is different from the program name?
3. When cleaning up the startup process, which of these should you do first?
   a. Use the Registry Editor to look for keys that hold startup processes.
   b. Run Msconfig to see what processes are started.
   c. After you have launched several applications, use Task Manager to view a list of running tasks.
   d. Run the Defrag utility to optimize the hard drive.
4. Using the Internet, investigate each of the following startup processes. Identify the process and write a one-sentence description.
   a. Acrotray.exe
   b. Ieuser.exe
5. Using Task Manager, you discover an unwanted program that is launched at startup. Of the following items, which ones might lead you to the permanent solution to the problem? Which ones would not be an appropriate solution to the problem? Explain why they are not appropriate.
   a. Look at the registry key that launched the program to help determine where in Windows the program was initiated.
   b. Use Task Manager to disable the program.
   c. Search Task Scheduler for the source of the program being launched.
   d. Use Msconfig to disable the program.
   e. Search the startup folders for the source of the program.

>> REAL PROBLEMS, REAL SOLUTIONS

REAL PROBLEM 11-1: Using Registry Mechanic

Registry Mechanic by PC Tools can be downloaded free from the registrycleaner.com web site. Download, install, and run the software. How many orphaned registry keys did it find on your computer? Which software installed on your computer is responsible for these orphaned keys? Do you think your system would benefit from allowing Registry Mechanic to clean your registry? If you decide to use Registry Mechanic to clean the registry, be sure to create a restore point first so you can undo the changes to your registry, if necessary.

REAL PROBLEM 11-2: Cleaning Up Startup

Using a computer that has a problem with a sluggish startup, apply the tools and procedures you learned in this chapter to clean up the startup process. Take detailed notes of each step you take and its results. (If you are having a problem finding a computer with a sluggish startup, consider offering your help to a friend, a family member, or a nonprofit organization.)