Configuring Windows Operating Systems

Windows includes several configuration settings you can manipulate as a PC techni-
cian. Many of these are configured by default, so you won't need to make changes
to them. However, it's very possible that users will manipulate these settings, and you'll
need to recognize what has been changed so that you can return the system to normal.
Additionally, many of the tools you use to configure a system can also be valuable when
troubleshooting Windows-based systems.

Exam 220-802 objectives in this chapter:

- 1.2 Given a scenario, install, and configure the operating system using the most
  appropriate method.
  - Driver installation, software and windows updates
- 1.4 Given a scenario, use appropriate operating system features and tools.
  - Administrative
    - Device manager
    - System configuration
  - MSCONFIG
    - General
    - Boot
    - Services
    - Startup
    - Tools
- 1.5 Given a scenario, use Control Panel utilities (the items are organized by "classic
  view/large icons" in Windows).
  - System
    - Performance (virtual memory)
    - Remote settings
    - System protection

- 1.7 Perform preventive maintenance procedures using appropriate tools.
  - Best practices
    - Schedules backups
    - Windows updates
    - Patch management
    - Driver/firmware updates
  - Tools
    - Backup
    - System Restore
- 4.6 Given a scenario, troubleshoot operating system problems with appropriate tools.
  - Tools
  - MSCONFIG

REAL WORLD   PREVIOUS VERSIONS CAN SAVE THE DAY

I was recently helping a small business owner with her Windows 7–based computer, and she mentioned that she had accidentally deleted a file. To say that she was disappointed is a huge understatement. It had valuable data, and she didn't know how she was going to be able to re-create it.

Thinking of previous versions and shadow copy, I asked her whether she used restore points. She didn't know what I was talking about, which was good news. They're enabled by default on Windows 7, and they keep copies of previous versions of files.

We took a quick look, and with just a couple of clicks, we were able to retrieve her file. She had no idea that this feature was there and must have said "Thank you" more than a dozen times. Even though users don't know about this, A+ technicians should. You can use it to help users get their data back or to retrieve a lost file of your own.

Using System Configuration

The *System Configuration* tool is one of the tools you can use to view and manipulate the configuration of your system. It has changed a little between Windows XP and Windows Vista but is the same in Windows Vista and Windows 7.

You can start the System Configuration Tool by entering *msconfig* (short for Microsoft Configuration) at the command prompt or a run line and pressing Enter. It's also accessible via the Administrative Tools group from the Control Panel on Windows Vista and Windows 7.

General

Figure 15-1 shows the System Configuration Tool with the General tab selected on Windows 7 (on the left) and Windows XP. You can see that msconfig in Windows XP includes three additional tabs that allow you to easily configure three different initialization files: System.ini, Win.ini, and Boot.ini. Windows Vista and Windows 7 use different methods for these settings, so these files are not needed. However, the Boot tab on Windows 7 provides some of the same functionality as the Boot.ini tab in Windows XP.
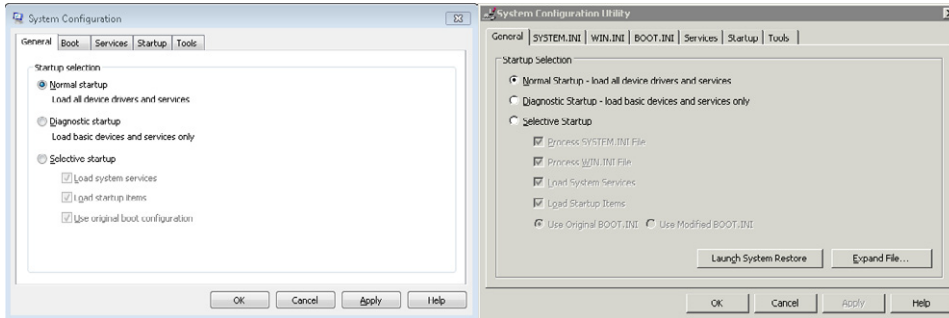

FIGURE 15-1 General tab of System Configuration tool.

The Startup Selection option is normally set to Normal Startup as shown. You can select Diagnostic Startup and restart the system, and it will start Windows using only basic services and drivers. If you modify any of the settings in the Services or Startup tab, it will automatically change to Selective Startup.

> **MORE INFO** **CHAPTER 17, "TROUBLESHOOTING WINDOWS OPERATING SYSTEMS"**
>
> Diagnostic startup is similar to starting the system in safe mode. Safe mode options are covered in Chapter 17.

Windows XP also includes a button to open System Restore, to create restore points, or to revert a system to a previously created restore point. The "System Protection" section later in this chapter covers restore points in greater depth.

Boot

The Boot tab allows you to control how a system starts. This can be useful if you want to change the behavior of a dual-boot system. For example, if you have a dual-boot system that currently starts Windows 7 by default but you want it to start Windows 8, you can use this tab to change it. Figure 15-2 shows the options for a dual-boot system configured with Windows 7 and Windows 8.
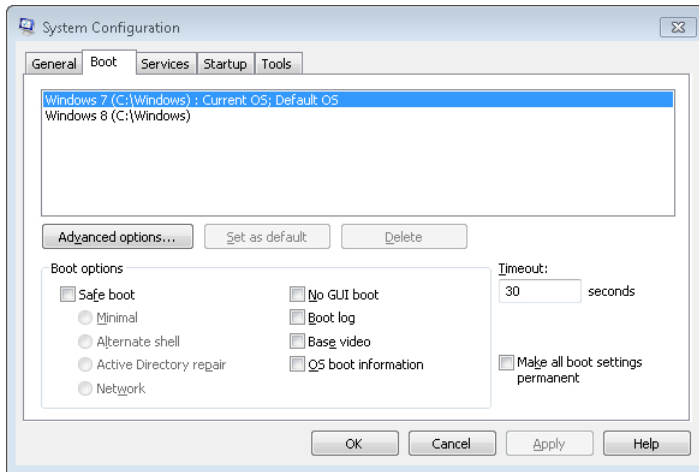
FIGURE 15-2 Boot tab of System Configuration.

Windows 7 is currently the default operating system. The system will start, show the dual-boot options for 30 seconds (based on the Time-Out setting), and start Windows 7 if the user doesn't take any action. You can select Windows 8 and click the Set As Default button to cause it to start Windows 8 by default instead. You can also change the Time-Out setting on this tab.

> *MORE INFO* **CHAPTER 17, "TROUBLESHOOTING WINDOWS OPERATING SYSTEMS"**
>
> Chapter 17 covers the Boot options available on this tab in the context of the different safe modes you can use while troubleshooting a system.

Services

The Services tab lists all the services that are available on the system and their current status, such as Running or Stopped. If the service has been disabled, it lists the date and time when it was disabled. Figure 15-3 shows this tab with the Windows Backup service disabled. You can deselect any check box to disable the service.

You can use this as a quick way to view the status or disable a service, but your choices are limited. The Services applet (covered in Chapter 13, "Using Windows Operating Systems," within the "Administrative Tools" section) provides you with many more options.
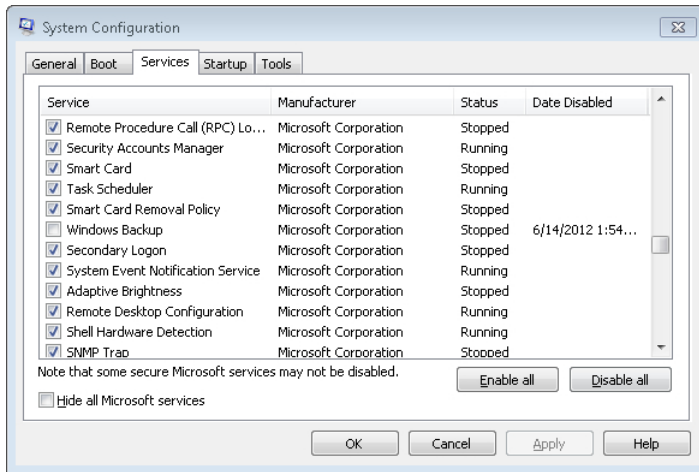
FIGURE 15-3 Services tab of System Configuration tool.

NOTE **SYSTEM INFORMATION TOOL**

System Information is another tool that allows you to view services. Chapters 2, "Understanding Motherboards and BIOS," and 3, "Understanding RAM and CPUs," introduced the System Information tool and showed how you can use it to get a quick overview of the system. Within the Software Environment group, you can select Services to view all the Services, their current state, the start mode, and more. You can start it by typing **msinfo32** from the command prompt or a run line.

Startup

The Startup tab shows all the applications that are configured to start when Windows starts. After using your computer for a couple of years, you'll have installed many different applications, and you might notice that the startup cycle is very slow. Many applications configure themselves to start automatically.

Figure 15-4 shows the Startup tab for a relatively new installation. The only two applications I've added are Virtual Machine User Services and Snagit. Compare this to your system. How many applications are configured to start automatically?
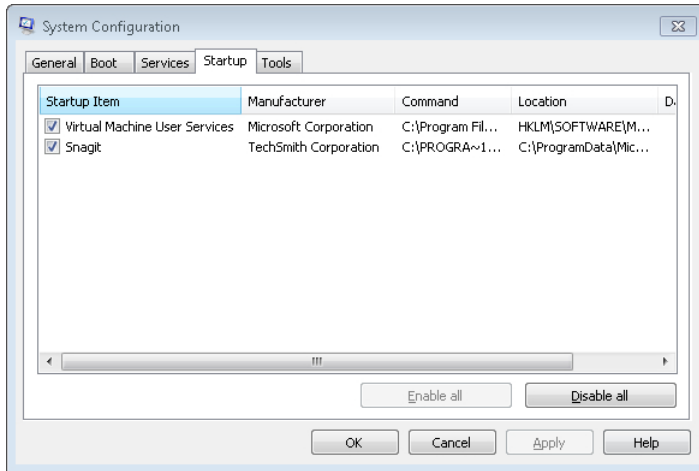
FIGURE 15-4 Startup tab of System Configuration tool.

You can deselect the check box for any of the items to prevent it from starting the next time Windows starts.

EXAM TIP

Manipulating the Startup applications is useful when troubleshooting infected computers or problem applications. You can use this to prevent an application from loading at startup.

The Windows Startup folder (available by clicking Start, All Programs, Startup) shows applications that are configured to start for the current user's profile. However, this does not show all the applications that will start when Windows starts. The Startup tab of the System Configuration applet shows all the applications.

Tools

The Tools tab provides a launching pad for many tools that are available on your system. These tools are covered in different areas of this book, but as an exercise, it's worth your time to open them. Select any of the tools and click Launch to start it.

✔ **Quick Check**

　　1. What is the command used to open the System Configuration tool?

　　2. How can you change the default operating system in a dual-boot system?

Quick Check Answers

　　1. Msconfig.

　　2. Modify the settings on the Boot tab of the System Configuration tool.

Using the System Applet

The *System* applet provides a quick snapshot of your system and includes some useful links to other tools. Figure 15-5 shows the System applet opened on a Windows 7–based system on the left and on Windows XP on the right. The Windows 7 version includes several active links in the left pane, and the middle pane provides some information about the system, such as the operating system version and the hardware.
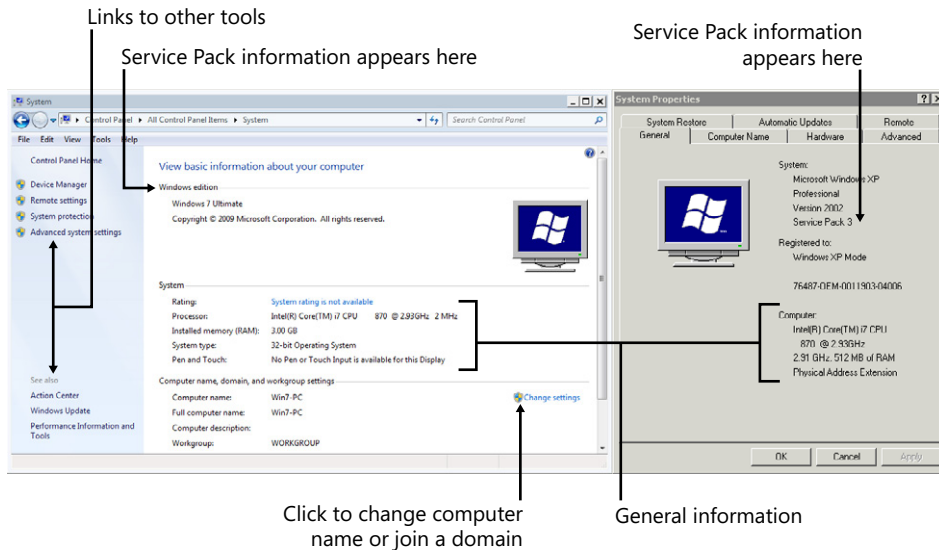

FIGURE 15-5 System applet on Windows 7 (left) and System Properties on Windows XP (right).

Windows XP includes some of the same information. You can see that Windows XP has Service Pack 3 installed, but Windows 7 is blank in that area, indicating a service pack has not been installed. Instead of active links, Windows XP includes multiple tabs.

For example, you can click the Device Manager link in the Windows 7 version to open the Device Manager. On Windows XP, you can select the Hardware tab and click the Device Manager button. Device Manager is covered later in this chapter.

Remote Settings

The Remote Settings tab includes settings that allow or block remote connections for a system. Two types of remote connections are Remote Assistance and Remote Desktop.

- **Remote Assistance.** This is used to allow a remote helper to provide assistance to a user. For example, a friend of yours might be having computer problems and send you a remote assistance request. When you respond, you'll be able to see his desktop on your computer. If he approves, you can take control of his desktop to fix a problem. While you're fixing, he can observe all your actions and learn in the process.

- **Remote Desktop.** Administrators use this to take full control of a remote system. With Remote Desktop, users do not see what the administrator is doing.

You can use the following steps to enable Remote Assistance and Remote Desktop on a Windows 7–based system.

1. Start the System applet from the Control Panel.

2. Click Remote Settings. The System Properties dialog opens with the Remote tab selected. You'll see something similar to the following graphic. Remote Assistance is enabled by default.
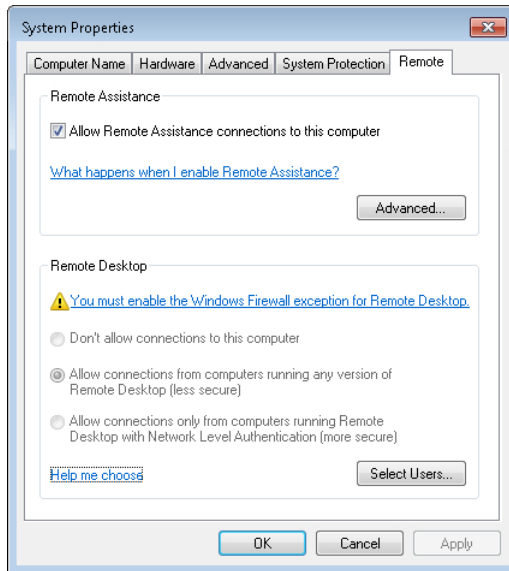
3. By default, the Windows Firewall blocks Remote Desktop connections. Use the following steps to configure the firewall:

   A. Click You Must Enable The Windows Firewall Exception For Remote Desktop. This starts Help.

   B. Select Click To Open Windows Firewall within the Help file.

   C. In the left pane, click Allow A Program Or Feature Through Windows Firewall.

   D. Click Change Settings. If you're prompted by User Account Control, click Yes to continue.

   E. Scroll down to Remote Desktop. Select the check box on the left to enable it. Ensure the check box for Home/Work (Private) is selected. This allows Remote Desktop to operate when it's connected in a home or work network. Your display will look similar to the following graphic.
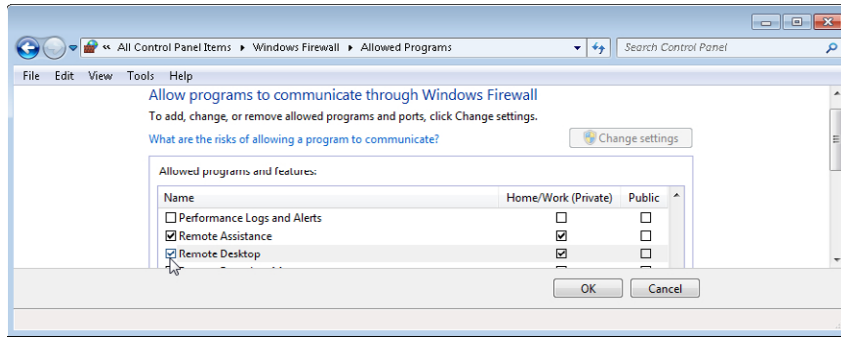
F. Click OK to make the change.

> **MORE INFO**   **CHAPTER 20, "UNDERSTANDING PROTOCOLS"**
>
> Chapter 20 shows how to use the Remote Desktop Connection (opened with the mstsc command) to connect with another computer. Chapter 22, "Network Security Devices," covers the Windows Firewall and exceptions in more depth.

System Protection and System Restore

System Protection includes System Restore and previous versions capabilities. System Restore is a Windows feature that allows you to restore your system to a previous state. For example, if you installed an application and find that it's causing problems with your system, you can use System Restore to undo the changes by applying a previously created *restore point*.

> **EXAM TIP**
>
> System Restore can uninstall applications, roll back drivers, and remove Windows Updates. You can also uninstall applications by using Add/Remove programs in Windows XP or Programs and Features in Windows Vista or Windows 7. Similarly, there are other tools to modify device drivers and updates. A restore point can modify all at the same time.

If you click the System Protection link from the System applet, it opens the System Properties page with the System Protection tab selected as shown in Figure 15-6. Click the System Restore button and click Next to access the System Restore dialog. Windows shows recent restore points that you can choose. If you want to view more options, select the Show More Restore Points check box.

On Windows XP, click Start, All Programs, Accessories, System Tools, and select System Restore to access restore points.

Windows automatically creates restore points every seven days and prior to certain events, such as a system update, an application installation, or a driver update. You can also manually create a restore point at any time by clicking the Create button.
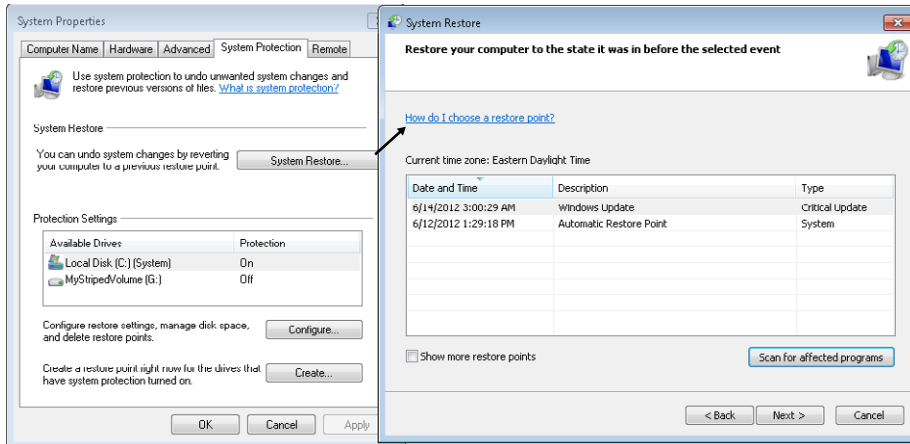
FIGURE 15-6 Accessing restore points on Windows Vista and Windows 7.

By default, System Restore will use up to 5 percent of the disk space to store restore points. You can click the Configure button to enable or disable System Protection or to modify how much disk space it will use. You can also delete the restore points to free up some disk space.

System Restore does not modify any user files, such as documents or pictures, when a restore point is applied. It restores only system files, applications, and drivers. However, when restore points are created, they do save previous versions of files that can be restored by using a feature called previous versions.

Shadow Copy (Previous Versions)

Previous versions are copies of files and folders that are automatically saved when a restore point is created. It's available in Windows Vista and Windows 7 and sometimes referred to as *shadow copy*, or shadow copies.

To use previous versions, your system must be configured to use restore points or have backups available. You can use Windows Explorer to right-click any file or folder, select Properties, and click the Previous Versions tab.

Figure 15-7 shows the properties of a file named A+ Study Notes with the Previous Versions tab selected. There is one previous version for this file, but it's possible for multiple versions to be available. When you select a previous version, you can select Open, Copy, or Restore.

- **Open.** This opens the file so that you can view the contents before actually restoring the file.
- **Copy.** You can create a copy of the file and store it in another location.
- **Restore.** Use this to overwrite the current version with the previous version.
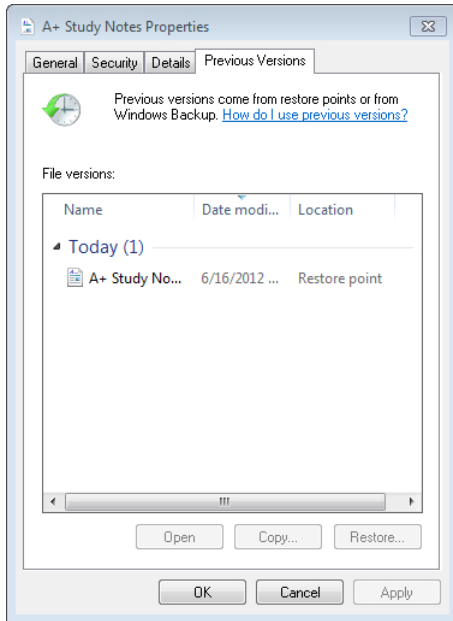
FIGURE 15-7 Using Previous Versions tab.

It's also possible to retrieve a previous version of a file that has been deleted, but the procedure is slightly different. If the file is deleted, you can't right-click it. Instead, use the following steps:

1. Open Windows Explorer by clicking Start, Computer.

2. Locate the folder where the file existed before it was deleted.

3. Right-click the folder and select Properties.

4. Click the Previous Versions tab.

5. Select a version of the folder that includes your file and click Open.

6. Double-click the file to open it. You can then save it.

Advanced System Settings

If you click on Advanced System Settings, it opens the System Properties page with the Advanced tab selected. There are three sections on this page: Performance, User Profiles, and Startup And Recovery.

The Performance section gives you options for viewing and configuring the paging file (covered in the next section). The User Profiles section is sometimes used by administrators to copy user profiles. Chapter 17 covers the Startup And Recovery options.

Understanding Paging

Computers use both physical memory and virtual memory. The physical memory is the random access memory (RAM) installed in the system, and the virtual memory is a file on the hard drive called a *paging file*. Virtual memory allows a system to use a paging file as an extension of RAM and operate as if it had more physical memory.

Paging Overview

Imagine that you're working on a computer and you have Internet Explorer (IE) and Microsoft Outlook running. The operating system takes up some RAM, and both IE and Microsoft Outlook take up the rest. For this scenario, imagine that the operating system and your two apps take up all the physical RAM.

Without virtual memory, you wouldn't be able to open up another application. If you tried to open up Microsoft Word, the operating system could refuse or, worse, crash. With virtual memory, the system swaps information between the physical RAM and a file on the hard drive. This allows you to work on more applications even if you've run out of physical RAM.

Figure 15-8 provides an overview of how this works. On the left, you can see that the operating system, IE, and Microsoft Outlook are in RAM. When you start Microsoft Word, the operating system looks to see what you haven't used recently and swaps it to the paging file on the hard disk. In the figure, it moved IE to the paging file on the hard disk to make room for Microsoft Word.

If you later go back to IE, the operating system looks for what hasn't been used recently. It could move Microsoft Outlook to the paging file and IE into physical RAM. You can then work with IE.
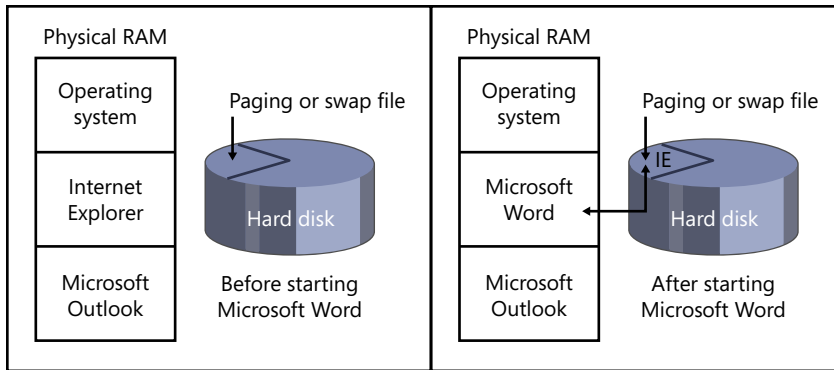
FIGURE 15-8 Using a paging file.

64-KB Pages

The preceding section provides a simplified explanation of paging, but it needs some clarification. RAM is organized in 64-KB pages, and the operating system works on these pages when swapping information back and forth between RAM and the hard disk. That is, when it needs to move something out of RAM, it looks for the 64-KB pages that haven't been used recently and swaps these page to the hard disk. If IE is consuming 500 MB of RAM and the operating system needs 128 KB of RAM, it swaps two 64-KB pages. It doesn't swap the entire 500 MB used by IE.

> **NOTE   PAGING FILE OR SWAP FILE**
>
> This file has been called the swap file because it swaps information back and forth. It's called the paging file in Windows XP, Windows Vista, and Windows 7, referring to how it moves pages of memory. You're likely to hear both terms, but they are the same.

Excessive Paging

If a system doesn't have enough RAM for what a user is doing, it will experience excessive paging. Data will be constantly swapped back and forth between the hard disk and RAM, and the overall performance will slow to a crawl.

One solution is for the user to close some applications to free up some RAM. When the system has enough free RAM, there will be very little swapping. Another solution is to add more RAM. If a system has enough RAM, there will be very little paging.

How much is enough? That depends on what the user is doing. I'm currently working on a system that has 16 GB of RAM. I'm running three virtual PCs (one for Windows XP, one for Windows Vista, and one for Windows 7) and have several applications open for writing and

to create graphics. Some paging is occurring, but my system isn't slow. Therefore, 16 GB is enough for me on this system. If I was only using IE to surf the Internet, 2 GB might be enough.

EXAM TIP

Disk thrashing is a symptom of a disk not having enough RAM. You'll be able to hear the disk constantly seeking as it reads and writes data, the disk LED on the front panel will be constantly blinking, and the system will be very slow. Disk thrashing can also occur if a drive is fragmented. Chapter 16, "Understanding Disks and File Systems," covers disk fragmentation, including how to check and resolve it.

Performance (Virtual Memory) Settings

You can configure the paging file from the System menu, but as a best practice, it's best to let Windows manage the size of the paging file on desktop systems. It sets the minimum and maximum size and grows the paging file as needed. If you do set the size of the paging file, you should ensure that the Maximum Size (MB) is at least 1.5 times the physical RAM.

One reason to modify the paging file settings is to move it. It is configured on the same drive as the operating system by default, but you can squeeze some performance gains out of the system by moving it to a different internal physical drive. This way, the operating system and paging file don't compete with each other for disk access.

You move the paging file location by creating a paging file on a different internal drive and then selecting No Paging File for the original drive.

> **NOTE** **VIRTUAL MEMORY ADDRESSED AS DISK LOCATIONS**
>
> One of the valuable features of virtual memory is that it is not tied to addressable memory space of the system. For example, a 32-bit system can address only 4 GB of physical RAM. The virtual memory is addressed as disk locations, so you can go beyond 4 GB.

The following steps show how you can view and modify the paging file settings on a Windows 7–based system.

1. Click Start, Control Panel. If necessary, change the view to Large icons.

2. Select System. Click Advanced System Settings. The System Properties page opens with the Advanced tab selected.

3. Click the Settings button in the Performance area.

4. Click the Advanced tab on the Performance Options page. You'll see a display similar to the following graphic. Automatically Manage Paging File Size For All Drives is selected by default.

Change button
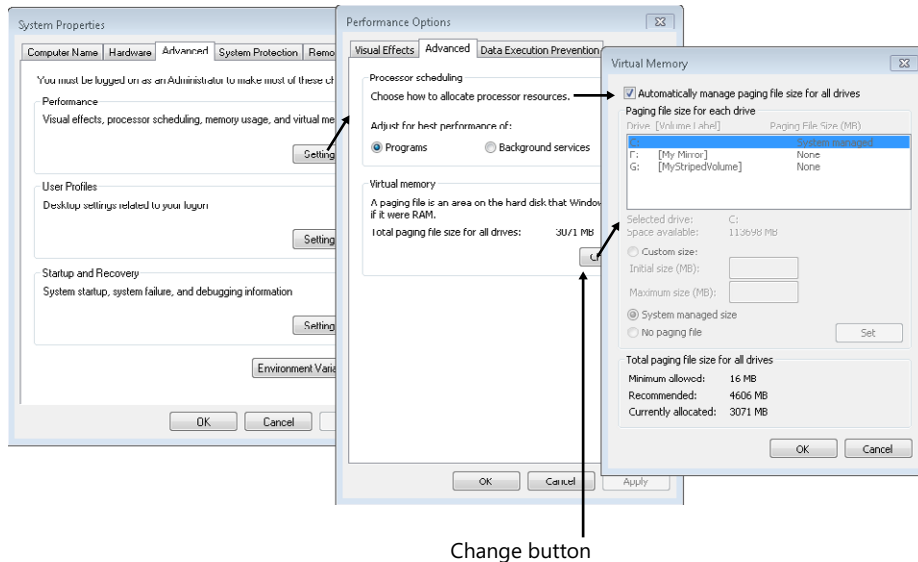
If you deselect the check box, you can select Custom Size and enter the Initial Size and Maximum Size values for the file. If your system has multiple internal disks, you can select a different disk and configure the file for this disk. When moving the paging file, you need to configure it for a different disk and then select No Paging File for the current disk holding the paging file. When you are done, click the Set button.

EXAM TIP

If you have more than one internal hard drive, you can increase the performance by moving the paging file to a different internal hard drive. You cannot move the paging file to an external drive. Set the maximum size to at least 1.5 times the amount of physical RAM.

✔ Quick Check

1. What allows Windows to use disk space as an extension of memory?

2. If you manually configure the paging file, how large should it be?

Quick Check Answers

1. Paging file.

2. At least 1.5 times the amount of RAM.

Working with Device Manager

A common task for any A+ technician is installing and upgrading device drivers. The primary tool that you'll use is *Device Manager*. Chapter 5, "Exploring Peripherals and Expansion Cards," introduces device drivers in the context of installing peripheral devices. Devices will often work without any user intervention, but sometimes a technician needs to get involved.

Starting the Device Manager

Device Manager works similarly in Windows XP, Windows Vista, and Windows 7, but there are different methods of starting it.

To start Device Manager on Windows XP, click Start, Run. Type in **devmgmt.msc** and click OK.

To start Device Manager on Windows Vista or Windows 7, click Start, Control Panel. If necessary, change the view to Classic View on Windows Vista or to Large icons on Windows 7. Select Device Manager.

> *NOTE* **MANY PATHS**
>
> **These methods show a couple of ways to start Device Manager, but as with many tasks, there are many methods you can use. For example, you can also click Start, right-click Computer (or My Computer on Windows XP), and select Properties to start System Properties and access it from there. You can also access it from Computer Management.**

Viewing Device Manager

When you open Device Manager, it displays the devices by type in groups such as disk drives, network adapters, and so on. If all the devices in a group are working, the group is collapsed. If there's an issue with any device, the group is expanded.

For example, Figure 15-9 shows the Device Manager on Windows 7. Two groups (Floppy Disk Drive and Other Devices) are expanded, indicating a possible problem. If a device has an issue, you can right-click it and select Properties and the Device Status section provides information about the error. In this case, the error is clear. The device is disabled, and you can click the Enable Device button to enable it.

> *NOTE* **ERROR CODES**
>
> **The errors aren't always so clear. The Microsoft knowledge base article at *http://support .microsoft.com/kb/310123* includes explanations for many error codes, in addition to steps you can take to resolve them. The article is geared towards Windows XP, but the same codes are used in Windows Vista and Windows 7.**
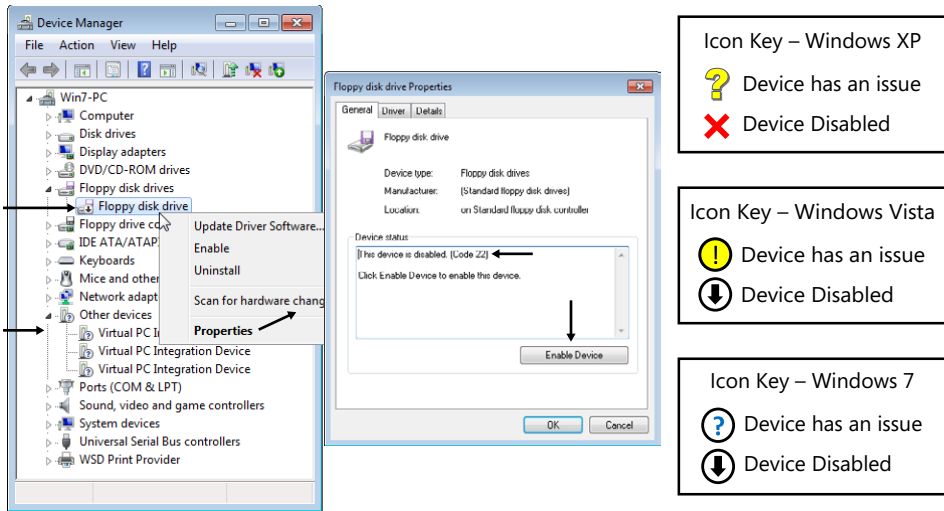
FIGURE 15-9 Device Manager.

The icons are slightly different on different operating systems, and Figure 15-9 has a partial key to show you some of the icons. The colors don't show up in the book, but for Windows XP, the question mark is yellow and the *X* is red. On Windows Vista, the exclamation mark is black on a yellow background. On Windows 7, the question mark is blue on a white background.

Additionally, the issues can be somewhat different. For example, a black exclamation mark on a yellow background usually indicates that the device driver for a device is missing. It could also indicate that the driver is corrupted or not the correct driver for the device.

EXAM TIP

A down arrow in Windows Vista and Windows 7 indicates that a device is disabled. A black exclamation mark on a yellow background often indicates that the device driver is missing.

Updating Drivers

You can replace the existing driver with a new one by updating it. This is required if the existing driver is missing or not working properly. At other times, you might realize that all the features of the device are not enabled. By installing a new driver, you'll enable all the features.

If you right-click the device, select Properties, and select the Driver tab, you'll see a display similar to Figure 15-10.
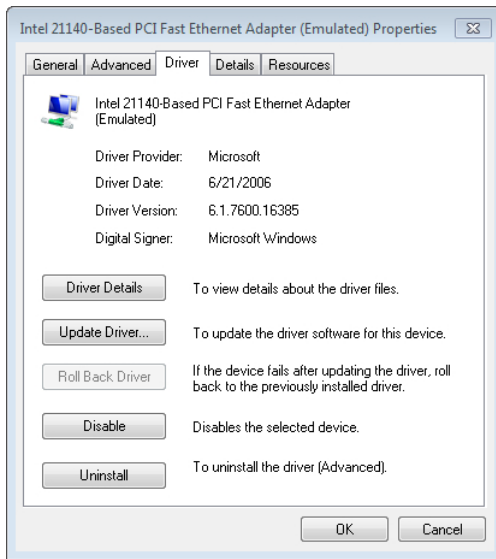
FIGURE 15-10 Driver tab.

> **NOTE ADVANCED TAB**
>
> If you compare Figure 15-9 to Figure 15-10, you can see that the Properties page for the Ethernet adapter in Figure 15-10 has more tabs than the Properties page for the floppy drive shown in Figure 15-9. It includes an Advanced tab and a Resources tab. The availability of additional tabs is primarily determined by the driver.

This tab has some basic information about the driver, such as the date it was released and its version. You can click the Driver Details button to get a listing of each of the files used by the driver and their location on the hard drive.

Clicking the Update Driver button shows a display similar to Figure 15-11. The easiest way to update the driver is to click Search Automatically For Updated Driver Software. If the driver is available, Device Manager will automatically locate and install it.

If a driver isn't functioning properly, all the features aren't working, or there is an updated driver you want to install, you can update it. The Update Driver Software is available from the right-click menu. You'll be prompted to allow Windows to search for the driver, or you can browse to the specific location.

Often the manufacturer will submit the driver to Microsoft, and it is available through this method. Sometimes you'll have to do a little more work. For example, if you've recently installed a new graphics card, the most up-to-date driver might not be available on Microsoft's site.
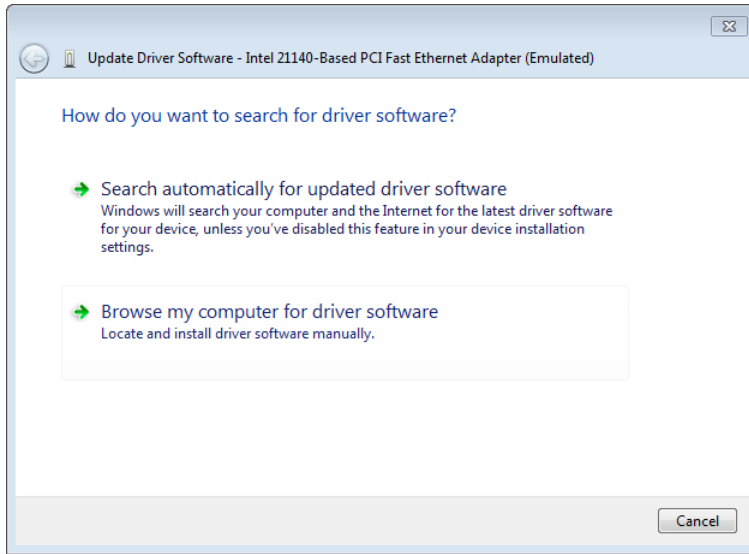
FIGURE 15-11 Updating a driver.

You can download a new driver from the manufacturer's website and select Browse My Computer For Driver Software. You can then browse to the location where you saved the driver. When you select the correct location, Device Manager will install it.

Disabling and Uninstalling

There can be times when you want to disable devices in the operating system. For example, if a computer includes hardware that a company doesn't want employees to use, disabling the unwanted device ensures that it won't be used. Chapter 2 shows how you can disable devices in the Basic Input/Output system (BIOS), but it's also possible to disable devices from within Device Manager.

You can right-click the device from within Device Manager and select Disable, or if you have the device properties page opened and the Driver tab selected, you can click the Disable button. Disabling the driver keeps it disabled even after it restarts.

The Driver tab also includes the Uninstall button, but this can be misleading. It uninstalls the driver, but only temporarily. The next time the system starts, plug and play will detect the device and will reinstall the driver automatically.

EXAM TIP

If you want to prevent users from using a built-in device, disable it from within Device Manager or from BIOS.

Rolling Back Drivers

Ideally, after updating a driver, the device will work better than it did before. Occasionally, that's not the case. Sometimes it's possible to install a driver that results in the device not working at all. However, you can easily undo the change. A great feature available in Device Manager is the ability to roll back the driver to the previous version. If a second driver has been installed, the Roll Back Driver button is enabled, and by clicking this button, you can revert the driver to the previous version.

You can roll back only one version. For example, if you have Driver A installed and you upgrade it to Driver B, you can roll it back to Driver A. However, if you have Driver A installed, and then you install Driver B, and then install Driver C, you cannot roll it back to Driver A. The best you can do is revert it to Driver B.

This brings up an important troubleshooting point: if you make a change to a system and it doesn't correct your problem, return the system to the previous condition. If your system has a problem and you make 10 changes, you might correct the problem but also insert nine additional problems.

Signed Drivers

Most drivers are digitally signed. This is a security feature that provides assurances about who published the driver and that the driver has not been modified since it was released.

With so many criminals looking for ways to infect computers and steal a user's data, a digitally signed driver is valuable. It prevents a criminal from modifying a driver with a virus that would be installed when the driver is installed.

Windows will alert you by default if you try to install an unsigned driver or install a driver that has been altered after it was originally signed. You'll see one of the following errors:

- Windows can't verify the publisher of this driver.
- This driver has been altered.
- Windows cannot install this driver.

Sigverif

If you suspect your system has unsigned drivers that could be causing problems, you can use the File Signature Verification Utility to check it. This tool examines the drivers and system files and verifies that they are digitally signed.

You can open it from the command prompt or a Run line by typing in **sigverif** and pressing Enter. After it opens, click Start. It might take a minute or so to complete, depending on how many files are on your system. When it completes, it a dialog box appears indicating that the files have been scanned.

Sigverif creates a file named Sigverif.txt and stores it in the Public Documents folder. You can easily view it by clicking the Advanced button and then clicking View Log.

Windows Update

Operating systems include millions of lines of code. In a perfect world, all this code would always work. The truth is that, despite extensive testing, problems do appear. Vendors regularly release patches to correct these problems. A *patch* is an update to an operating system or an application and is just a small piece of code that fixes a problem with existing software.

For example, criminals often look for vulnerabilities in software. When they find a vulnerability, they write malicious software (malware), such as viruses, to infect systems. When vendors become aware of vulnerabilities, they develop and release patches. Systems that are patched are not vulnerable to the viruses. The unpatched systems become infected, and often the user is unaware of the problem.

> *MORE INFO* **CHAPTER 26, "RECOGNIZING MALWARE AND OTHER THREATS"**
>
> Chapter 26 presents information about different types of malware and common methods used to protect systems. One method is keeping systems up to date with current patches.

Microsoft uses *Windows Update* to help users keep their systems up-to-date. Additionally, it's very easy to configure a system to automatically check for and install updates when they're available.

Updates available through Windows Update can be related to security, performance, or stability issues. These are classified as important, recommended, and optional updates.

- Important updates improve security, privacy, and reliability of the system. They should be installed as soon as possible and can be installed automatically. These are called high-priority updates on Windows XP.

- Recommended updates target non-critical problems. They can be installed automatically.

- Optional updates provide updates to drivers or new software. They can be installed only through user interaction.

You can access Windows Update on Windows XP, Windows Vista, and Windows 7 by clicking Start, All Programs, and selecting Windows Update. The system checks with a Windows Update site and compares available updates with updates that are currently installed. If updates are available, you'll see a display similar to Figure 15-12. You can then click Install Updates to begin the installation.
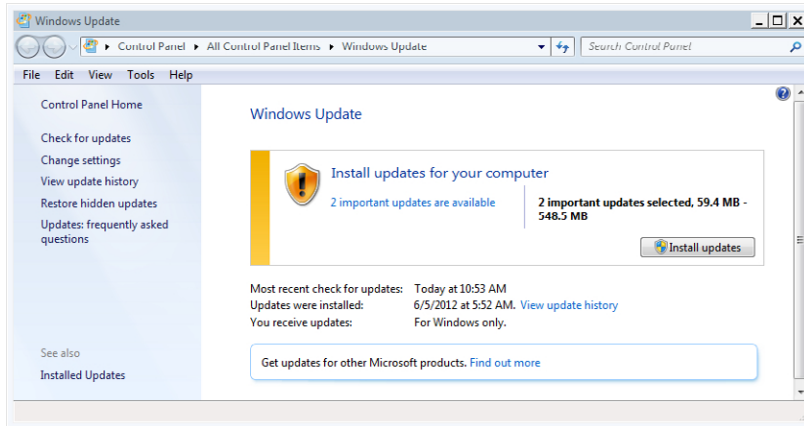

FIGURE 15-12 Windows Update.

EXAM TIP

Systems should be kept up-to-date with current patches and updates to keep them secure. Criminals use a variety of methods to prevent a system from receiving updates. If a system cannot contact Windows Update, it often indicates that the system is infected with malware.

Service Packs

A *service pack (SP)* is a cumulative group of patches and updates. For example, service pack 1 (SP1) for Windows 7 includes all the patches and updates that were released since Windows 7 came out. The next service pack is called SP2, then SP3, and so on. Service packs often include additional features and services.

Automatically Installing Updates

As a best practice, it's recommended that you use *Automatic Updates* to download and install updates automatically rather than manually. When configured this way, Windows periodically checks with Windows Update sites for new updates. When they're available, Windows automatically downloads and installs them.

Figure 15-13 shows the configuration page for Windows Update on a Windows 7–based system. You can get to this page by clicking the Change Settings link in the left column of Windows Update.
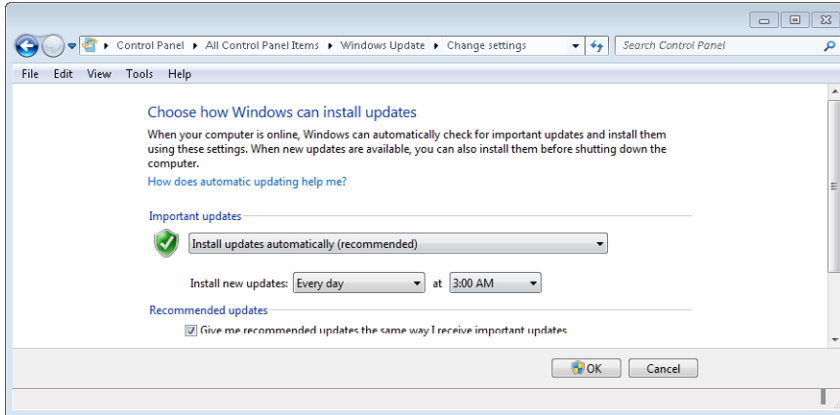

FIGURE 15-13 Windows Update Change Settings page.

NOTE **WINDOWS XP**

Windows XP has similar settings. You can access them on the Automatic Updates tab of the System Properties applet from the Control Panel.

Figure 15-13 shows recommended settings. The system will periodically check for updates and download them when they are available. Then, at 3:00 AM, the system will install the update. The drop-down box provides the following four options:

- **Install Updates Automatically (Recommended).** Most home users and SOHOs will use this.

- **Download Updates But Let Me Choose Whether To Install Them.** Some updates automatically restart the system, and users sometimes select this so that they can control when the update is applied and, therefore, the system is restarted.

- **Check For Updates But Let Me Choose Whether To Download And Install Them.** Users with slow Internet connections use this.

- **Never Check For Updates (Not Recommended).**

Patch Management

Patch management refers to the methods used to keep systems up-to-date. It includes evaluating, testing, and deploying patches, and it also includes periodic testing of systems to ensure that they are up-to-date.

Most home users and small organizations configure systems to automatically download and install updates when they are available. Many large organizations employ detailed change management practices to evaluate and test patches before deploying them. They commonly use tools such as Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM) to automate the deployment of the updates. These can periodically inspect the systems to ensure that they have all the required patches.

Another tool commonly used is the *Microsoft Baseline Security Analyzer (MBSA)*. It can check one or more systems in a network for many security settings in addition to ensuring that they are up-to-date with current patches.

Backup Capabilities

One of the sure things with computers is that if you use them long enough, you will lose data. Files can become corrupted, malicious software can destroy them, and users can accidentally delete their files. Each of these situations can be a major event if a backup isn't available.

Each Windows operating system supports backing up and restoring data, although there are significant differences among the versions of Windows. Windows Vista introduced a new program for backups, and this program was improved and enhanced in Windows 7.

Windows Vista and Windows 7 both support full image backups. A full image backup captures the entire hard drive contents, including the operating system, applications, and all the user's data. If the drive fails, the image backup can restore the system to its state when the image was captured.

Windows XP

Windows XP includes a backup program that you can use to back up and restore data on a computer. You can start the Back Up Or Restore Wizard with the following steps:

1. Click Start, All Programs, Accessories, System Tools, Backup.

2. Follow the directions in the wizard to back up or restore data.

This tool allows users to easily pick and choose what files they want to back up and restore. It includes the ability to back up everything on the computer to external devices and network locations.

Windows Vista

Windows Vista introduced the Backup And Restore Center, which is significantly different from the backup program included with previous editions of Windows. It allows you to back up and restore files, configure automatic backups, and perform a complete PC backup of the entire system. You can open the Backup And Restore center with the following steps:

1. Click Start, Control Panel. If necessary, change the view to Classic View.

2. Double-click Backup And Restore Center. Your display will look similar to Figure 15-14.
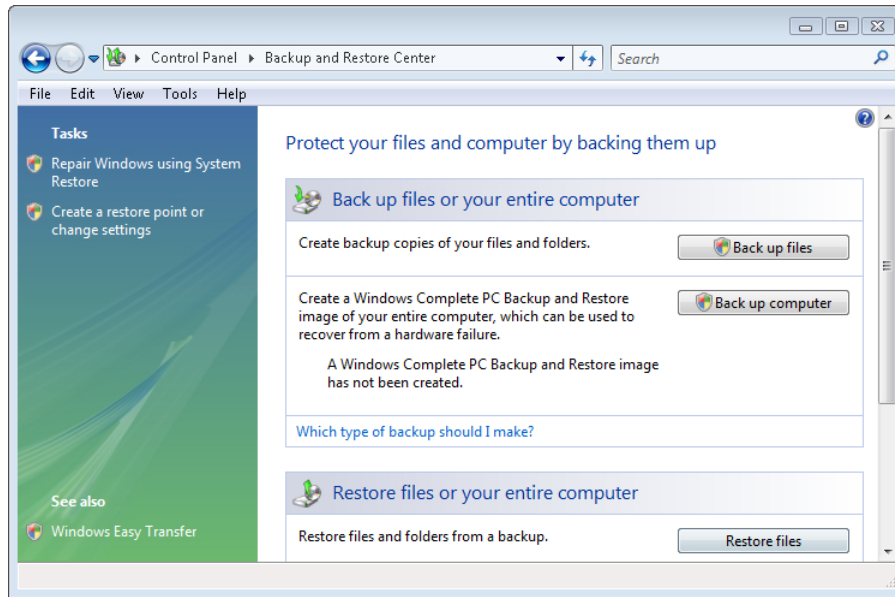

FIGURE 15-14 Windows Vista Backup And Restore Center on Vista Ultimate.

This tool gives you multiple capabilities for backing up and restoring files. You can choose what file types to back up based on categories. For example, you can choose to back up document files and music files. It will then locate all of the files in the category and back them up. You can also back up the entire computer.

The Backup And Restore Center allows you to back up data to multiple locations, including the following:

- **Internal hard drives.** You can't back up data to the same hard drive, but if your system has additional hard drives installed, you can back up data to one of these other drives.

- **External hard drives.** USB hard drives are relatively inexpensive and easy to plug into a system. When they are plugged in, the Backup And Restore program recognizes them and can be configured to back up to these drives.

- **Writable CDs or DVDs.** If your computer includes a CD or DVD burner, you can back up data to writable CDs or DVDs. It might take several CDs or DVDs to complete a backup, and you can't use automatic backups with these discs.

- **Network locations.** Windows Vista Home Premium, Business, and Ultimate editions support backing up to shared folders on network locations. Full image backups cannot be backed up to a network location.

The Windows Complete PC Backup And Restore tool creates an image of your computer. If users do this when they first set up their computer, they can recover the entire computer even if a catastrophic failure prevents the computer from starting. Users can also update the Windows Complete PC Backup image periodically.

EXAM TIP

Automatic backups are not available in the Home Basic edition, and the Windows Complete PC Backup tool is not available in the Home Basic or Home Premium editions. You can back up data to a network location on the Home Premium, Business, and Ultimate edition. You cannot perform a Windows Complete PC Backup (an image backup) to a network location. Windows Vista does not support backing up data to USB flash drives on any edition.

Windows 7

The backup program introduced in Windows Vista was enhanced and improved in Windows 7, making it easier to use and configure. It supports both file backups and image backups, just as Windows Vista does. However, a significant difference is that you can choose what files and folders you want to back up in Windows 7. In Windows Vista, you can choose only the file types to back up based on categories.

You can start the Backup And Restore tool with the following steps:

1. Click Start, Control Panel. If necessary, change the view to Large icons.

2. Double-click Backup And Restore.

You can back up data to multiple locations just as you can with Windows Vista. This includes internal hard drives, external hard drives, writable CDs and DVDs, and network locations.

There are two important differences between the capabilities of Windows Vista and Windows 7 backups. On Windows 7, you can create image backups to a network location, but this isn't possible in Windows Vista. Additionally, you can back up data to USB flash drives as long as they are at least 1 GB in size.

EXAM TIP

All editions of Windows 7 include backup and restore capabilities. However, the Starter and Home Premium editions do not support backing up data to network locations.

Program Compatibility

You might run across an application that works in a previous version of Windows but does not work in the version you're using now. You can use the Application Compatibility tool to configure the application to run by using specific settings from a previous operating system.

You can configure the settings manually by right-clicking the application file, selecting Properties, and clicking the Compatibility tab. You'll see something similar to Figure 15-15.
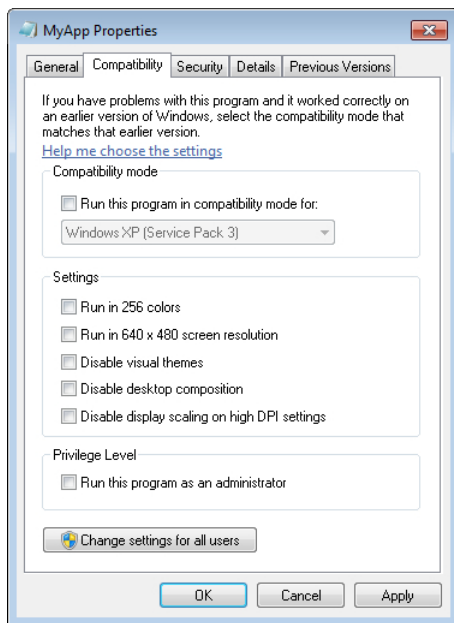

FIGURE 15-15 Manually configuring program compatibility.

You often need to experiment with different settings. For example, if you're having trouble running an application in Windows 7, you can try to run it using a compatibility mode for Windows XP SP3. If this doesn't work, you can try other settings.

An alternative is the Compatibility Wizard. It checks with a Microsoft site to determine whether there is a known setting that works for the application and, if so, will configure the settings. There are different methods of starting this wizard, including the following:

- On Windows XP, click Start, All Programs, Accessories, and select Program Compatibility Wizard.

- On Windows Vista, click Start, Control Panel. Use the Category View by clicking Control Panel Home. Select Programs and select Use An Older Program With This Version Of Windows.

- On Windows 7, Click Start Control Panel. Change the view to Category view if necessary and select Programs. Select Run Programs Made For Previous Versions Of Windows.

After starting the wizard, select the program and follow the wizard's steps.

Modifying Documents Location

User data is often stored in the Documents folder, which is part of a user's profile. In some cases, you might need to move the location of the Documents folder but still keep it as part of the user's profile.

> **MORE INFO**   **CHAPTER 11, "INTRODUCING WINDOWS OPERATING SYSTEMS"**
>
> Chapter 11 covers profile locations. The profile is located in C:\Documents And Settings on Windows XP and C:\Users on Windows Vista and Windows 7.

For example, if a user has stored a significant amount of data in this folder, the C drive can become low on free space. You can move the data to another drive to free up space on the C drive. The following steps show how this is done on different operating systems:

- On Windows XP, click Start, right-click My Computer, and select Explore to start Windows Explorer. Right-click My Documents, and select Properties. Click Move and browse to the new location. Click Select Folder and click OK. Click Yes to confirm the move.

- On Windows Vista, click Start, Computer to start Windows Explorer. In the Folders area, expand your user profile (your user name). Right-click Documents and select Properties. Click the Location tab. Click Move and browse to the new location. Click Select Folder and click OK. Click Yes to confirm the move. Click OK.

- On Windows 7, click Start, Computer to start Windows Explorer. Expand the Documents folder within Libraries. Right-click My Documents and select Properties. Click Move and browse to the new location. Click Select Folder and click OK.
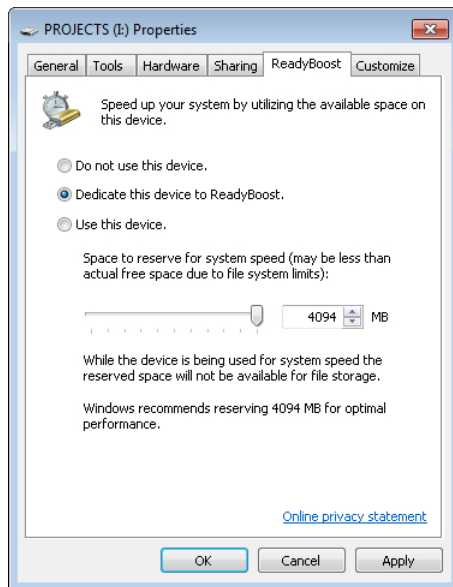
ReadyBoost

ReadyBoost is a feature available in Windows Vista and Windows 7 that can speed up a computer by using storage space on a USB flash drive. Your system can use this extra memory to cache disk content. There are a few basic requirements for this to work:

- Must be USB 2.0 or higher.

- It must have a minimum of 1 GB free space. For best performance, use a flash drive with twice as much RAM as your system has.

- ReadyBoost must be enabled on the drive.

You will usually be prompted if you want to use ReadyBoost when you plug a USB device into your system. You can also enable it manually with the following steps:

1. Start Windows Explorer by clicking Start, Computer.

2. Right-click the USB drive and select Properties.

3. Click the ReadyBoost tab.

4. Select Dedicate this device to ReadyBoost, and adjust the amount of space you want to use for ReadyBoost. Your display will look similar to the following graphic. Click OK.

If you want to see a video and read more about ReadyBoost, check out this link: *http://windows.microsoft.com/en-us/windows7/Turn-ReadyBoost-on-or-off-for-a-storage-device.*

Chapter Summary

- The msconfig command opens the System Configuration tool. This tool has five tabs on Windows Vista and Windows 7: General, Boot, Services, Startup, and Tools.

- You can use msconfig to modify the boot configuration for a dual-boot system, disable services so that they cannot start, and disable applications configured to start when Windows starts.

- The System applet provides a quick snapshot of your system and includes links to change many settings.

- Remote settings are configured to allow remote connections to a computer. You need to configure an exception in the Windows Firewall to enable Remote Desktop.

- System Protection automatically creates restore points. You can apply a restore point to revert system, application, and driver files to a previous state. System Protection also creates copies of previous versions of user files.

- Users can use previous versions (sometimes called *shadow copy* or *shadow copies*) to restore previous versions of files and to restore a deleted file.

- The paging file is a file on the hard disk that is used as an extension of memory. Windows manages the paging file size by default and stores it on the same drive as Windows.

- You can move the paging file to another internal drive to improve performance. If configured manually, the maximum size should be set to 1.5 times the size of physical RAM.

- Device Manager is used to troubleshoot and maintain device drivers. You can use it to disable devices, update drivers, uninstall drivers, and roll back an updated driver.

- If a device or driver has an issue, it will automatically be expanded in Device Manager. Different versions of Device Manager use different icons to identify issues.

- You can locate unsigned drivers with the File Signature Verification utility (sigverif).

- Patches are small pieces of code applied to the operating system or applications and released as updates. They correct problems such as security vulnerabilities.

- Systems are kept up-to-date with Windows Update tools. Automatic updates can be configured to automatically download and install updates on to systems.

- Patch management practices ensure that patches are tested and deployed to all systems within an enterprise. Tools such as MBSA, WSUS, and SCCM help automate these tasks.

- All editions of Windows 7 include backup and restore capabilities. The Professional and Ultimate editions support backing up to network locations.

- Application Compatibility tools allow you to run incompatible applications by using settings that mimic previous versions of Windows.

Chapter Review

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

1. You restarted a system and noticed an error message flash on the screen. You want to identify what applications are configured to start automatically. What can you use?

   A. Shadow copy

   B. Device Manager

   C. Services

   D. Msconfig

2. You are trying to optimize the performance of a computer with two internal hard drives and an external USB drive. Windows is on C, and D is used for data storage. You want to move the paging file. What is the best option?

   A. Move it to the external USB drive.

   B. Move it to the C drive.

   C. Move it to the D drive.

   D. Move it to the boot partition.

3. You are troubleshooting a system and decide to use a restore point from three days ago. You explain to the user that it will revert the system to the state it was in three days ago. The user is concerned that his data will be lost. How would you respond?

   A. Restore points will erase the data, so it should be backed up.

   B. Restore points won't modify user data.

   C. If the data is on the C drive, there is no problem.

   D. If the data is on the D drive, there is no problem.

4. You recently added a graphics card but realize that all the features are not working. What should you do?

   A. Enable System Protection.

   B. Update the driver.

   C. Configure Program Compatibility.

   D. Use Device Manager to disable the device.

5. Your company recently received some computers that include built-in modems, but users shouldn't use them. How can you prevent users from using these modems?

   A. Remove the modems.

   B. Disable them by using Device Manager.

   C. Disable them by using System Configuration.

   D. Enable ReadyBoost.

6. Which of the following tools can be used for patch management? (Choose all that apply.)

   A. WSUS

   B. SCCM

   C. Automatic Updates

   D. System Configuration

Answers

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

1. **Correct Answer:** D

   A. **Incorrect:** Shadow copy helps restore previous versions of files but does not track startup applications.

   B. **Incorrect:** Device Manager is used to troubleshoot and maintain device drivers.

   C. **Incorrect:** The Services applet can be used to identify what services start automatically, but not applications.

   D. **Correct:** The Startup tab of the System Configuration tool (msconfig) shows what applications start automatically.

2. **Correct Answer:** C

   A. **Incorrect:** You can't move the paging file to an external drive.

   B. **Incorrect:** If you're trying to optimize performance, you should move the paging file to a drive other than the operating system drive. The C drive holds the operating system.

   C. **Correct:** For best performance, move the paging file to a drive different than the operating system, which is D.

   D. **Incorrect:** The operating system is on the boot partition.

3. **Correct Answer:** B

   A. **Incorrect:** A backup might be useful, but restore points will not erase the user data.

   B. **Correct:** Restore points won't modify user data.

   C. **Incorrect:** It doesn't matter where the user stored the data.

   D. **Incorrect:** It doesn't matter where the user stored the data.

4. **Correct Answer:** B

   A. **Incorrect:** System Protection is used for restore points.

   B. **Correct:** If all the features of a new device are not working, you should update the driver.

   C. **Incorrect:** Program Compatibility is for applications, not devices.

   D. **Incorrect:** If the device is disabled, it won't work at all.

5. **Correct Answer:** B
   - **A.** **Incorrect:** If the modem is built-in, it cannot be removed.
   - **B.** **Correct:** Devices can be disabled with Device Manager.
   - **C.** **Incorrect:** System Configuration cannot disable devices.
   - **D.** **Incorrect:** ReadyBoost cannot disable devices.

6. **Correct Answer:** A, B, C
   - **A.** **Correct:** Windows Server Update Services (WSUS) is a free server tool used to automate deployment of patches.
   - **B.** **Correct:** System Center Configuration Manager is a server tool used to automate deployment of patches.
   - **C.** **Correct:** Automatic Updates can be configured to automatically install updates.
   - **D.** **Incorrect:** System Configuration does not deploy updates.