Chapter 17

PC Troubleshooting

Learning Outcomes

17.1 Identify common-sense practices when troubleshooting a PC.
17.2 List the most likely causes of boot failure at each boot stage.
17.3 Recognize common problems or failures and identify their causes.
17.4 Compare Windows diagnostic utilities.
17.5 Recall the Windows boot sequence.
17.6 Describe preventive computer maintenance.
17.7 List the CompTIA A+ troubleshooting steps.

A+ Certification Exam Objectives

The following A+ Certification Exam Objectives are covered in this chapter.

Exam 220-1101

5.0 Hardware and Network Troubleshooting

- 5.1 Given a scenario, use the best practice methodology to resolve problems.
- 5.2 Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power.
- 5.3 Given a scenario, troubleshoot and diagnose problems with storage devices and RAID arrays.
- 5.4 Given a scenario, troubleshoot video, projector, and display issues.
- 5.5 Given a scenario, troubleshoot common issues with mobile devices.

Exam 220-1102

1.0 Operating Systems

- 1.2 Given a scenario, use the appropriate Microsoft command line tool.
- 1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system.
- 1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

3.0 Software Troubleshooting

- 3.1 Given a scenario, troubleshoot common Windows OS problems.

4.0 Operational Procedures

- 4.3 Given a scenario, implement workstation backup and recovery methods.
- 4.5 Summarize environmental impacts and local environmental controls.

Key Terms

archive bit
blue screen error
differential backup
hive
incremental backup
Microsoft Dynamic Link Library (DLL)
POST card
registry key
startup problem
system image

Overview

Troubleshooting a PC requires a combination of a technician's knowledge, intuition, and experience. Microsoft Windows operating systems include many diagnostic tools as standard programs, and there are many diagnostic tools available from third-party vendors that can assist in the troubleshooting process. Third-party vendor programs range from freeware and shareware to systems costing several thousands of dollars, with the more expensive programs including a diagnostic board that plugs into the PC's expansion slots.

Most problems can be diagnosed without expensive diagnostic tools, but the value of these tools is their ability to save time and money when trying to identify problems that may be caused by two or more components. For example, it can be difficult to determine if a problem is caused by a troublesome CPU or a bad motherboard. When this situation arises, a simple solution is to substitute a known or good CPU for the suspect CPU. However, this substitution alone can be very expensive.

A+ Note

The A+ Certification places a great deal of weight on knowing the basics of troubleshooting. You need to become familiar with the limitations and purpose of various diagnostic tools, and the best way to become familiar with troubleshooting tools is by using them.

17.1 Common-Sense Practices

When troubleshooting and repairing PCs, remember that "time is money." This means you should always strive to take the quickest, most efficient path first. Adhering to the following common-sense practices can help tremendously:

- Determine the major area at fault
- Determine what action occurred just prior to failure or problem
- Proceed carefully
- Write down settings before you change them
- Think the problem through

Determining the Major Fault Area

The first step is to try to determine what major area is the most likely source of the fault. There are four major fault areas to be considered:

- Hardware failure
- Software failure
- User-generated problems
- Internet and network connection failure

User-generated problems tend to be the most common error or problem encountered. Some users like to tinker with Control Panel, and others will try to solve their problems alone. In some cases, this is probably fine, but most users are unlikely to possess the appropriate technical knowledge, and users with little technical knowledge can be the most dangerous. They often attempt to fix a problem before calling the technician, so it is vital that technicians understand that a user's permissions can either be augmented or diminished via the User Account Settings in Control Panel and apply the principle of least privilege. Nevertheless, technicians will experience issues with a personal computer, regardless of the administrative and safety practices they implement on their machines.

When this happens, you may be faced with more than one problem. First, the original problem likely still exists, and then there may be additional problems created by the user. Repairing computers in a school setting can be the most frustrating, as some students love to experiment with the settings on a school's computer before trying the activity on their home computer. Nevertheless, technicians can observe and troubleshoot these issues more efficiently and effectively than a user will when implementing fixes in their personal computers.

Figure 17-1 illustrates the Control Panel from the Windows 10 operating system, and its functionality and features. There are three different views for Control Panel: **Large icons**, **Small icons**, and **Category**, which is shown in Figure 17-1. From Control Panel, a technician can determine if all drivers are installed and up to date, observe the computer's firewall, verify software that is installed, document whether remote access has been granted for external computers inside and outside of the user's network, obtain service logs, and confirm the machine is working to its fullest capability with its hardware. Technicians can also determine the current and recent functionality of the machine for their documentation purposes.

By default, a user's network settings update automatically when their personal computer is powered on, and a network is detected via its network adapter. However, if a network requires the personal computer to input the network information manually, technicians may do so via the Control Panel. Nevertheless, it is rare that networks do not allow automatic configuration and most networks broadcast their network updates to the connected computers automatically.

It is also a good practice to begin by considering what reasonably could have caused the problem. For example, if a solid-state drive will not boot, likely causes include operating system failure and drive corruption. By contrast, network connectivity is highly unlikely to be related to the issue.

Goodheart-Willcox Publisher

Figure 17-1 Control Panel houses several functional utilities and features in one location.

What Happened Last?

1102: 3.1 A+

It is critical to determine from the computer user what the last action on the computer was prior to the problem occurring or before computer failure. Often, the last action taken by the user can lead the technician directly to the problem. For example, the installation of new hardware or software can possibly lead to operational malfunctions, as can a recent download from the Internet. Ask the user as many questions as possible because obtaining as much information as possible can save valuable time later. It is also important to verify requirements before installing new hardware or software. If the system does not have all the requirements, you can experience a wide range of problems. All commercial software lists the specific requirements for installation. For example, the following represents the minimum requirements for Windows:

- 1 GHz or faster processor with two or more cores
- 4 GB of RAM
- 64 GB of storage
- UEFI Secure Boot
- Trusted Platform Module 2.0
- Graphics Card with Direct X 12 or later with WDDM 2.0 driver

Suppose you install Windows 11 on a computer that meets all the requirements except the graphics card. You will likely experience a wide range of display problems that will be difficult to diagnose.

Tech Tip

Some problems can be intermittent and related to a loose hardware connection or excessive heat. For example, partially blocked airflow could cause heat to build slowly inside a computer and the memory modules to overheat. Once the memory module has overheated, the system locks up. Always be aware of "what happened last" when troubleshooting a computer.

Proceed Carefully

Take your time when diagnosing problems; rushing through a diagnosis or operating in a hurry will likely lead to sloppy work, create new problems, or cause you to overlook something important. In contrast, proceed in a methodical yet constant pace. Customers will not appreciate a technician who is standing around talking, socializing, or any other activity that appears to be a nonproductive use of time, because they are typically paying a premium price for service and losing the use of their computers while they are inoperable. Do not waste the customer's time or money, or they will likely call someone else next time there is a problem.

Write Things Down

Do not rely on your memory alone while troubleshooting. Take note of current settings before changing them as well as file names before deleting them. You can make the problem much harder to determine if you create another problem along the way. If a problem is not cleared after changing a setting or deleting a file, you should return the system file or setting to the way you found it. Do not simply move on and try something else.

Think the Problem Through

Do not try operations out of desperation. Desperate technicians will often run the same test twice knowing the results from the first test were valid. These are acts of desperation, and they occur when a technician is stumped. While it might seem an odd recommendation for a professional, it is often a good idea to perform an online search for the specific problem you are encountering. It is quite likely that others have encountered a similar problem and may have published their resolution, saving you a significant amount of time in the long run.

When you run out of tests, *stop and think* about the situation. It can be helpful to create two lists: one listing items you know are *not* the problem and other listing potential issues that could still exist. Then, check the website of the manufacturer of the PC, BIOS, and operating system for corrections that have been posted for the exact symptoms you are encountering. Many times, a problem is discovered that affects a particular setup or combination of hardware and software programs and solutions are posted. Again, if you are experiencing this issue, it is likely someone else also has.

Do not hesitate to contact the manufacturer of the hardware or software in question by e-mail with a description of the problem. Most questions will be answered in 24 to 48 hours at no cost for the service. You can get much faster replies by calling, but that service is seldom free.

Your fellow technicians are another important source of information. As you progress in the PC repair world, you will make many friends, and it is a standard practice to share information with a colleague who may have encountered a similar problem. A peer may have a quick and easy answer to a problem that you have not encountered before. Other times, simply discussing the problem with a peer can be quite helpful, as explaining the problem forces you to summarize the situation and describe it in logical terms. Just the act of verbalizing the problem may allow you to solve it. Never be embarrassed to ask for help.

17.2 Troubleshooting by Boot Stage

There is no one foolproof method to troubleshooting. There are too many variables that can cause a computer to fail, but there are recommended procedures that can be used to help you organize your approach to solving a computer problem. The causes of failure discussed are not all-inclusive and should be interpreted as a guide to solving a computer-related problem or complete system failure.

When troubleshooting computer problems, the first thing you must do is isolate the problem to determine whether it is a hardware, software, or user-generated problem. This is easier said than done, but the best way to go about this is to determine at what stage of computer operation the problem is occurring. The three general stages of computer operation are

- the POST;
- the loading of operating system files and initialization of hardware; and
- the loading of startup programs and running of applications and services after logon.

First Stage

A+ 1102: 3.1

If the problem occurs during POST, it is most likely a hardware failure since no operating system software or application software has been loaded at this stage. The POST may fail to complete if a damaged hardware device fails POST or its own diagnostic routine. For example, a modem that has been damaged during a thunderstorm may cause the computer to lock up during or immediately after the POST.

If you just built the computer system and it fails to boot successfully the first time during POST, you may have improperly installed the RAM, CPU, or CPU cooling device. A high-speed CPU with an improperly installed cooling fan or heat sink may generate excessive heat in seconds, causing the computer to freeze while performing the POST. Improperly seated RAM may also cause the computer to fail during POST, but the computer will typically issue a beep code indicating a problem with the RAM. Go back, reinstall these devices, remove all devices not required for system operation, and reboot the system. If the problem continues to persist, you can either substitute parts to determine which hardware device is causing the failure or use a third-party utility that uses a POST card to diagnose the problem.

Firmware POST Codes

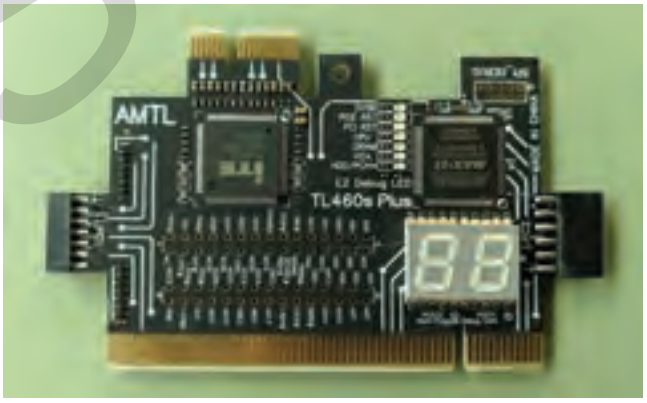
A+ 1101: 5.2

The firmware (BIOS or UEFI) produces specific error codes, known as *beep codes* or *POST codes*, which can be used diagnostically. POST codes are not universal and can vary significantly depending on the manufacturer of the computer, motherboard, or firmware. A beep code is used to indicate failures before the video system is initialized when there is no display on which to print screen messages. After the video is enabled, a message will appear on the screen during or immediately after the POST indicating the problem by either an alphanumeric code or short message.

Some computers indicate a successful POST with a single beep while others do not, and some BIOS/UEFI firmware allow the single beep to be disabled because it annoys some users. To identify a problem via beep code, you must consult the computer, motherboard, or firmware manufacturer. For example, a series of short and long beeps on a Dell computer indicates a problem that does not necessarily match the same series of beeps on an ASUS computer. One thing you can be sure of is if you hear a series of beeps, it is an indication of a major hardware failure.

POST Cards

A **POST card** is an expansion card that plugs into a motherboard and displays error codes generated during a computer's power-on self-test (POST). These cards are extremely helpful in troubleshooting computers that do not start up. POST cards include some type of digital readout, as shown in Figure 17-2, that displays hexadecimal digits that correspond to startup errors, much like diagnostic trouble codes



Markus Kuhn/Public Domain

Figure 17-2 A POST card is an expansion card that plugs into a motherboard and displays error codes generated during a computer's power-on self-test (POST).

(engine codes) in automobiles. A very popular third-party utility suite used by repair centers is PC-Doctor Service Center Kits, which has historically been used by Dell Computers to perform computer diagnostics in the service department.

The POST card is inserted into any PCI slot and used to diagnose errors during POST caused by hardware failure such as the CPU, RAM, or the motherboard. A POST error code is displayed on the LEDs, and the technician can then match the code to the diagnostic chart in the user manual. Without a POST card, a technician would have to rely on beep codes or substitute the CPU, RAM, and motherboard with a known good component, which can be time-consuming and expensive. The technician also runs the risk of damaging a part during the substitution process.

As motherboards have improved, the need for POST cards has lessened, but they still have a valuable place in a PC technician's tool kit. Be aware that every manufacturer is different, so the problem associated with a given code for one motherboard may not be the same issue on a different motherboard. Additionally, ensure that the POST card is compatible with the motherboard before using it. For example, not all motherboards broadcast their POST codes to the PCI slots. In these cases, you will have to rely on the beeps.

For more information on problems that can occur during the POST stage, see the following chapter sections: Typical Startup Problems, Hard Drive Failures, Additional Mechanical Problems, and Boot Sequences.

A+ 1101: 5.3
1102: 3.1

Second Stage

If the problem occurs during the second stage—operating system loading and initialization—the problem is most likely related to a corrupt operating system file or a driver. Many computer systems display the results of the POST as it occurs, so you can often identify when stage two starts simply by observing the screen display. For example, you will see the RAM check verified and the hard disk drive and other devices that are present identified on the screen, and soon after the POST turns the loading of the operating system to the bootstrap program, you will see a progress bar appear on the screen. When you see the progress bar, you know that the second stage has begun, and the operating system has successfully loaded the system kernel. The operating system then initializes the hardware devices.

A+ 1102: 3.1

Failure during the second stage is usually the result of a corrupt system file such as ntldr or failure to properly detect and initialize a piece of hardware. It can also be caused by a corrupt hardware driver. The fastest way to repair a system failure that occurs during the loading and initialization of the operating system is by reinstalling required system files. Simply insert the installation CD/DVD and then reboot the computer. When the installation CD/DVD boots, follow the screen prompts. If your computer does not have an optical drive, you should be able to download the necessary files to a USB flash drive and boot from it the same way as you would boot from an optical drive.

For more information on problems caused by hard drive failure that can occur during the second stage, see the Hard Drive Failures section. Detailed troubleshooting methods for this stage are covered in a later chapter.

Third Stage

System logon marks the end of the second stage. Keep in mind that not all operating systems require a logon, so the third stage truly begins when the desktop first appears. During the third stage, startup programs, services, and applications are loaded. The most common problems that can occur during this time are usually due to corrupt or incompatible drivers and files.

File Corruption

1101: 5.3 A+

Files can be corrupted in various ways, such as by virus attacks and hardware failures. For example, an intermittent RAM failure can also corrupt files if the file contents are transferred or copied during the time of RAM failure. File corruption can occur when data is stored in an area of the hard drive that has a bad sector; all data saved to the bad sector is lost, thus corrupting the contents of the complete file. Files can also be corrupted by an unexpected power outage or shutting down the computer system while installing updates.

Overwritten DLL File

Certain files, such as a DLL file, can cause a system failure when inappropriately applied in a software program or when they become corrupt. A **Microsoft Dynamic Link Library (DLL)** file is an executable file that can be called and run by Microsoft software applications or by third-party software programs. Rather than write code from scratch each time a new software application is written, programmers can simply call a DLL from within the program they have written and run the needed function automatically. One DLL can be used by more than one software program at the same time, and by reusing the same code contained in the DLL, a programmer saves time and uses less memory and disk space. The term *dynamic* is used because the file can be loaded, run, and then unloaded from computer memory when no longer needed.

One of the major software problems in the past occurred when a user loaded a software application from a disc that contained the necessary DLL files to run a software application. All too often, the DLL file on the software disc overwrote the existing DLL residing on the computer, and if the overwritten file were newer than the file on the disc, an error would occur when the user started an application other than the one just loaded. A classic example is when a user loaded an old version of a software game on a computer that had other games requiring a similar DLL file. While the older game ran perfectly, one or more of the other games ran incorrectly or not at all.

DLL files usually have a **.dll** file extension, for example **mon.dll**, though the DLL will sometimes have an **.exe** file extension. Look at Figure 17-3 to see the search results for files with the **.dll** extension. There are over 62,000 files that have a **.dll** extension on this particular computer. As you can see, there are thousands of possible DLL files that can be used as part of multiple software applications and hardware drivers.

Goodheart-Willcox Publisher

Figure 17-3 DLL files are called by software applications to perform common tasks.

A+ 1101: 5.2
1102: 3.1

Blue Screen Error

During the third stage of booting, the system may experience a blue screen error commonly referred to as the *Blue Screen of Death (BSoD)*. A **blue screen error** is a blue screen that appears with an error code and then freezes the system. Microsoft also refers to blue screen errors as *fatal errors*, *stop errors*, and *stop error messages* because the system is not recoverable at the time of the error and must be restarted before you can attempt to remedy the problem. Some of the most common causes for blue screen errors include

- defective hardware;
- corrupt files on the hard drive;
- system BIOS settings that are beyond the capabilities of the hardware;
- third-party software containing bad code; and
- bad code in the Windows operating system.

The error codes displayed on the blue screen can be quite cryptic. You should copy the error code and use it as a reference when searching Microsoft's Support website.

The most appropriate utility for diagnosing a problem after the logon is the System Configuration Utility (**msconfig.exe**). This and other utilities for diagnosing problems during this stage are covered in the Windows Diagnostic Utilities section, as well as in a later chapter. You may also check out Microsoft TechNet for detailed information and articles.

Tech Tip

A malicious software program can attack a computer at any time, not just after the system logon. For example, if the MBR is corrupted by a virus, the computer will fail before switching from text mode to graphic mode.

17.3 Commonly Encountered Problems

While every computer system is unique, they all have similar components, which all have similar lifespans. For example, many system failures stem from startup, mechanical failures, and intermittent issues. This section presents an overview of commonly encountered problems categorized by problem type. In general, four common problem types include

- startup problems;
- hard drive failure;
- mechanical problems; and
- system and intermittent device failure.

Remember that these are not the only types of problems one may encounter while working on computers in the field. Rather, these are generalized categories to describe some of the most common problems.

Tech Tip

When troubleshooting a PC, always attempt the simplest tests first before moving on to the more complex and labor-intensive tests.

Typical Startup Problems

A **startup problem** causes the computer to lock up during the boot process. Startup problems are difficult to diagnose because they occur too early in the PC operation to be solved by system diagnostic tools. Each of the following problems is described as a symptom, and possible solutions are provided as a guide, similar to the troubleshooting symptoms you encountered in in Chapter 13. The list of symptoms centers on the problems encountered before the boot process is completed. Keep in mind that there are hundreds of possible computer symptoms, and this section only details some of the most common, catastrophic boot problems you may encounter.

Think about the boot process and the steps involved. System boot failures involve the power supply, CPU, boot device (often a hard drive or SSD), RAM, BIOS, CMOS, system configuration, loading of drivers, and the loading of the operating system. Now consider some of the most common hardware problems and their symptoms during the boot process.

When reading the list that follows, assume that there is one hard drive labeled C: and a disc drive labeled D:. Note that these are recommended procedures, not absolute procedures. Also, be aware that viruses can imitate some of the described symptoms, so you should always check for the presence of a virus on the hard drive.

Symptom 1:

1101: 5.2, 5.3 A+

There is no power light, no fan running, and no sound of boot operation. It appears that the PC is completely dead.

Items to check:

Before you open the case, make sure the PC is plugged in. Next, check the power from the wall outlet, power strip, or both to ensure there is power to the unit. If you have power, then the likely problem is the computer's power supply. Open the case and test the power supply outputs. Replacing the power supply is generally more cost-effective than fixing a broken one.

Most computers include indicator lights to identify activity such as hard drive activity, the presence of power, or data transfer activity. These lights can help troubleshoot basic issues. For example, a red LED indicator light indicates a substantial problem, a yellow light indicates a warning, and a green light indicates everything is running normally. There are also LED lights associated with network interface cards, for which a solid green or yellow light indicates proper functionality, while a blinking light indicates actual network activity.

Symptom 2:

1101: 5.2, 5.3 A+
1102: 3.1

The power light (LED) is on, the fan is running, but there is no activity. The system appears dead.

Items to check:

Check the power supply for a power good signal. The power good signal is sent to the BIOS system to signal that the power supply is on and ready.

If the power supply passes the power test, try reseating the RAM and the CPU. The CPU or RAM may not be making a good electrical connection in their sockets. Try reseating the RAM first because it is significantly faster and easier than reseating the CPU. Both components operate on very low voltages, so even a slight oxidation buildup on one of the device pins operating at 3.3 volts or less is sufficient to render the CPU or RAM dead. Cleaning the oxidation will bring it back.

If you perform all the listed operations and the system still fails to activate, you may have defective components. If you have RAM modules or a CPU that is known to be good, you can use those to eliminate defective parts as a possibility. In that event, you may have a defective motherboard.

Symptom 3:

1101: 5.2, 5.4 A+
1102: 3.1

The system tries to boot, and you hear two or more beeps, and then nothing (no video). The fan is running, and there is a power light.

Items to check:

Make sure the monitor is plugged in correctly, both to the PC and the power source. There are a number of different cables used with video, so it is also important to ensure you are using the correct cable. HDMI is quickly becoming the most widely used, but many monitors still connect via SVGA, DisplayPort, or other connection type. The first thing to look for is any frays or wearing in the cable. If you see any degradation along the cable jacket or connectors, replace the cable. If the cable appears to be in working order, test its functionality by plugging it into a monitor that is

known to be in working condition. If the video still fails, you can operate with the knowledge that the cable is likely bad and needs to be replaced. If the cable appears to be working, check the monitor source. Many modern monitors allow for multiple sources, so you might simply have the monitor set to the incorrect data source.

In the event the cable and monitor are found to be functional, the next logical step is to check and reseat the video card; then do the same to the RAM. If those actions do not help, try to decode the beep error code by consulting the manufacturer literature. Newer manuals often come as a PDF file on disc as opposed to the traditional paper booklet. If there is no manual, look up the BIOS chip manufacturer on the Internet. First, copy all information from the BIOS chip or motherboard and then consult the manufacturer's website.

In some cases, a technician can access information from the Event Viewer Log regarding when a monitor has been turned off or the display of an image was interrupted. The Event Viewer will advise when the monitor experiences errors, along with potential warning indicators as to what actions need to be taken to resolve the error. However, monitor access must be available to obtain information regarding the Event Viewer Log.

A+ 1102: 3.1

Symptom 4:

A setup error is indicated on the screen.

Items to check:

This is probably a CMOS setup problem. Access the BIOS setup utility by using the key combination indicated on the screen. If no key combinations are given, try those with which you are familiar, such as those listed in Figure 3-43 from Chapter 3. You can also look up the keystroke combination for accessing the BIOS at the BIOS manufacturer's website.

A+ 1101: 5.2

Normally, CMOS settings do not change. However, the settings sometimes change when you install a new hard drive that is automatically detected. Also, if the battery used to hold the CMOS data is going bad, you could lose the settings. The date and time not matching the true date and time is a good indication that your battery is going bad.

Be sure to write down the existing CMOS settings before making any changes. This is extremely important if you are going to try something like the **Return to default settings** option. When that option is selected, many settings will change instantly, and you will not be able to tell which settings have changed or what they changed from. Check the manufacturer's website for the correct CMOS settings for your particular model of PC. Having baseline CMOS settings on hand can save you a tremendous amount of time. Sometimes people get curious and go into the setup utility to see what it looks like. They also make changes either intentionally or accidentally. If you know what the settings *should* be, it is much faster to restore them.

A+ 1101: 5.3

Symptom 5:

The PC powers on, but there is no drive activity.

Items to check:

Check the system CMOS settings, and make sure the correct drive is identified. The drive and the number of cylinders, heads, and sectors should be identified in the setup utility, and the hard drive manufacturer and hard drive model number will often flash on the screen when the BIOS detects it during the boot process. If the drive is not detected during the boot, the screen will flash something similar to *No hard disk drive*.

You should also check the connections between both the power supply and the hard drive and the motherboard and the hard drive to ensure they are tight. If all that checks out, boot the system with a recovery disc or the operating system installation disc, and see if you can access the hard drive from the command prompt.

Symptom 6:

1101: 5.3 A+

The computer attempts to boot to the wrong device.

Items to check:

This can be caused by several issues. The device boot order is controlled by the BIOS/UEFI setup configuration, and an inexperienced user may have changed the boot order while trying to install a program from disc and never returned the boot order to the correct sequence. Another possible reason is the computer had an external storage device, such as a hard disk drive attached to a USB port, and was configured to boot from this device. The device has been removed and now the computer is looking for the device during a normal boot. Inspect the setup utility configuration and correct as necessary.

Symptom 7:

The computer continually reboots on failure.

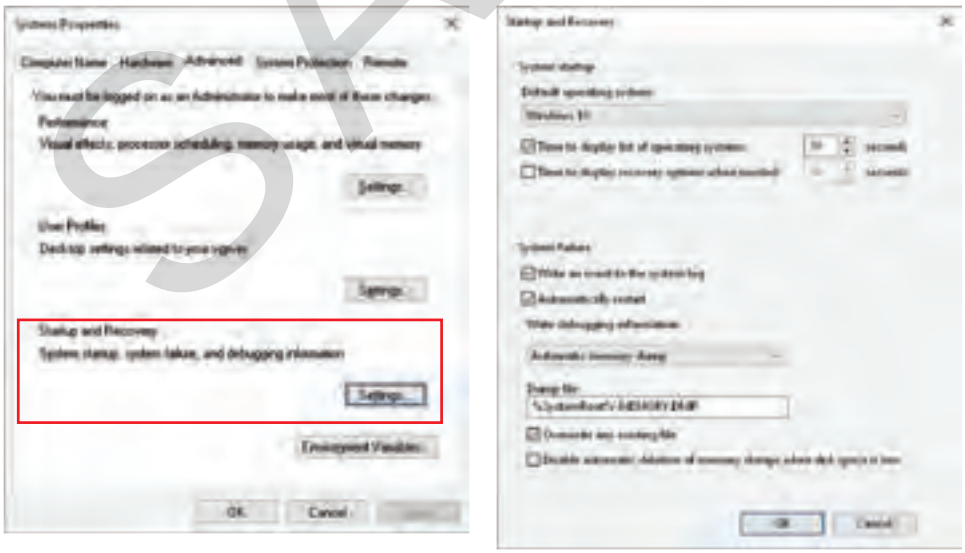
Items to check:

Some computers can be configured to reboot on a detected error. However, this may cause the system to continuously reboot, so you will have to disable this option to stop the continuous reboots and diagnose the cause of the failure. Windows also provides an option in the **Startup and Recovery** dialog box that can configure the way the computer reacts when encountering an error. The **Startup and Recovery** dialog box is accessed through **Control Panel**>**System and Security**>**System**>**Advanced system settings**>**Settings**. The option to restart the computer automatically is the default setting in Windows. Figure 17-4 shows the **Automatically restart** option enabled.

Symptom 8:

1101: 5.2 A+
1102: 3.1

The system crashes or reboots for no apparent reason.



Goodheart-Willcox Publisher

Figure 17-4 The **Startup and Recovery** dialog box is set by default to reboot continuously when a system error is encountered.

Items to check:

Check the power supply and cables to ensure they are all tightly connected. Check for excessive heat on the CPU and memory chips, and make sure all DIMMs are seated properly. Additionally, try reseating the CPU. Finally, check the BIOS/UEFI configuration to verify the correct amount of RAM.

A+ 1101: 5.2

Symptom 9:

A burning smell or smoke is coming from the computer.

Items to check:

This is most likely the result of a defective power supply. While not required, a power supply suspected of severe electrical damage can be easily removed from the computer to be opened and inspected. Severe electrical damage is very easy to identify, as shown by the power supply in Figure 17-5, which exhibits the following signs of severe damage caused by a failed capacitor:

- An imperfection in the side of the capacitor that appears like a dent or bulge.
- A smoke stain on the clear plastic insulation cover that protects the electrical parts from the metallic cover.
- A deposit of ash from the electrical fire created by the defective capacitor.

You do not have to be an electrical engineer to tell this power supply is bad.

If the power supply hardware appears okay, the motherboard is most likely defective or there is a problem with the hard drive. Swapping the hard drive with one you know is working should show where the problem lies. If the hard drive is causing the problem, check for a virus or a corrupt operating system. Always think about the last thing that occurred on the PC before the problem developed. Hard drive failures will be discussed in detail in a later section.

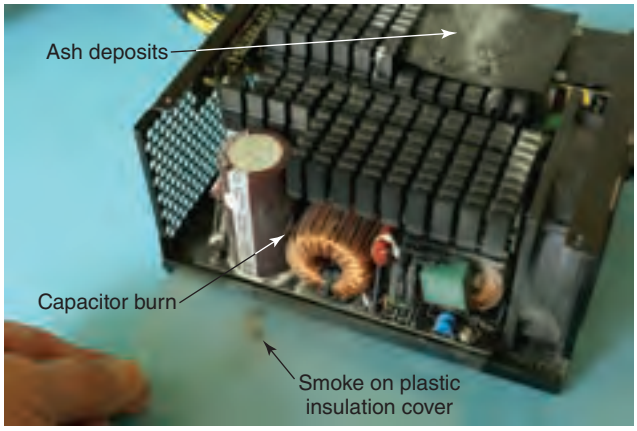
A+ 1102: 3.1

Symptom 10:

The computer fails to start services.

Items to check:

When a technician experiences a service that will not run, they can use the Windows Services utility for their troubleshooting strategies. The Windows Services utility displays all the properties and information about the services that run on the Windows operating system. Once the technician has found the service that is not working properly, they can right-click on the service and either pause or restart it.



Goodheart-Willcox Publisher

Figure 17-5 Typically, a suspected damaged power supply can be verified by a visual inspection.

Symptom 11:

A+ 1102: 3.1

The user's profile loads slowly.

Items to check:

Depending on the content of a user's profile, a user may experience an ample amount of time for their account to load as they are logging in to their personal computer. Technicians confronted by this issue should first delete any unneeded documents and programs that are on the user's computer and conduct a virus scan to search for any malicious software that might be causing the profile to deem faulty via the user's perception. However, if problems with a user's account persist, it is recommended that a new profile be generated for the user, or an attempt made to rebuild their profile via Safe Mode to eliminate any malicious or unneeded data and programs.

When a technician boots a Windows operating system into Safe Mode, the Windows operating system only runs the minimal number of resources necessary to allow the operating system to function. Furthermore, a technician can decide what programs will or will not operate and in what order the boot sectors and drives will operate. Therefore, technicians can rebuild or modify a user's profile with minimal interference and operating system resources.

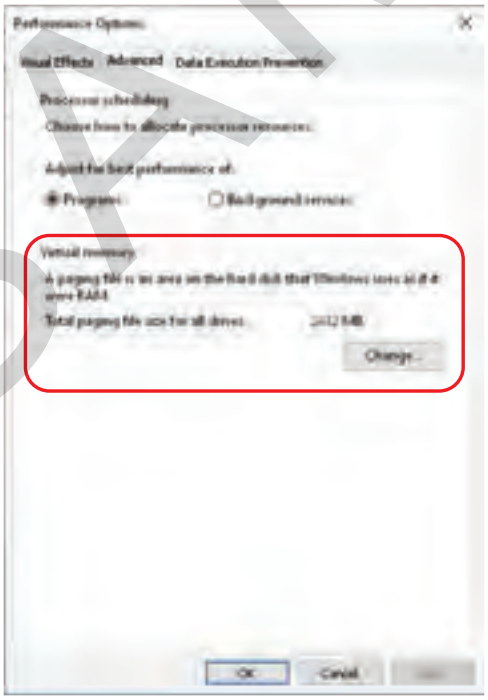
Symptom 12:

A+ 1102: 3.1

The computer generates a low memory warning.

Items to check:

One of the first things to check on a Windows 10 or 11 computer is the virtual memory. The easiest way to do this is to conduct a search using the keyword System and select the **System** option from the list of results. From there, select **Advanced system settings** to open the System Properties dialog box; then select **Settings** from the Performance section of the **Advanced** tab. This will open the Performance Options dialog box, from which you should select the **Advanced** tab, as shown in Figure 17-6.



Goodheart-Willcox Publisher

Figure 17-6 Virtual memory should account for one-and-one-half times the size of your physical memory.

From this screen, you can not only change the Virtual Memory, but you can also adjust programs and services for best performance. Virtual memory should normally be one-and-one-half times the size of your physical memory. Workstations should generally be optimized for program performance, whereas servers should be optimized for background services.

It may also simply be that you have unnecessary programs running, so examining your startup programs and services may lead to you being able to remove some unneeded services, freeing up more RAM for other programs. If nothing else corrects the problem, you may run the Windows Memory Diagnostics Tool. You can access this tool by searching for memory and selecting **Windows Memory Diagnostics** from the list of results. This will launch a dialog box from which you can restart the computer to check for problems or defer the diagnostics until the next time the computer is booted, as shown in Figure 17-7.

A third solution is to simply add more resources. If your system is notifying you of low RAM, adding more RAM is a viable solution to this problem, but it is best to first ensure that more RAM is needed. By performing the previously discussed troubleshooting steps, you should be able to confirm the amount of RAM needed and present in the computer. If adjusting the virtual memory and Windows Memory Diagnostics do not alleviate the problem, then adding resources is the next logical step.

A+ 1102: 3.1

Symptom 13:

The computer generates a USB controller resource warning.

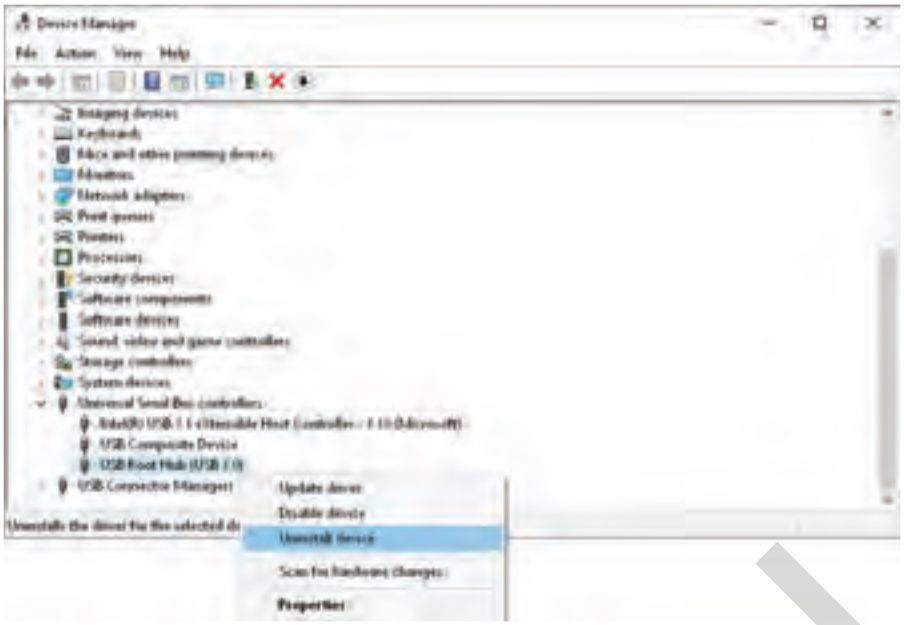
Items to check:

When plugging in a USB device, one might see an alert such as USB controller resource warning or perhaps Not Enough USB Controller resources, both of which relate to an issue common to USB 3.0 ports called *endpoint limitation*. In general, a system can manage up to 16 USB-in and 16 USB-out devices, even though addressing allows for up to 127 devices. One way to attempt to solve this is to reinstall the USB host controllers via Device Manager. Launch Device Manager by conducting a search for devmgmt and select **Device Manager** from the list of results. Once in Device Manager, extend the Universal Serial Bus controllers category, right-click the USB 3.0 controller, and select **Uninstall device** from the shortcut menu, as shown in Figure 17-8. Once the device has been uninstalled, reinsert the device to reinstall the controller.

You can also attempt to run the device diagnostic tool in Windows 10 or 11. Open command prompt with administrator-level permissions and execute the following command syntax: msdt.exe -id DeviceDiagnostic. This command launches the Windows device diagnostic process, as shown in Figure 17-9.

Figure 17-7 The Windows Memory Diagnostic Tool can help determine why a computer is generating low memory warnings.

Goodheart-Willcox Publisher



Goodheart-Willcox Publisher

Figure 17-8 Uninstalling and reinstalling the USB 3.0 controller may help solve USB controller issues.

Goodheart-Willcox Publisher

Figure 17-9 The Hardware and Devices troubleshooter can be launched with the command syntax msdt.exe -id DeviceDiagnostic.

If neither of these solutions alleviates the problem, a more drastic option is to go into the UEFI settings and disable the XHCI mode option. This has the effect of downgrading USB 3.0 ports to USB 2.0. As stated, this is a rather drastic measure and should only be used as a last resort.

Symptom 14:

The system seems unstable.

1102: 3.1 A+

Items to check:

This is a broad symptom that includes any indicators that the operating system is itself unstable, including system crashes, the system hanging, and services failing to start, among many others. System instability can be caused by a number of

underlying issues. For example, using a beta version of Windows can lead to instability. Additionally, if you have recently upgraded the version of Windows, there might be an issue with hardware drivers being incompatible with your version of Windows. Having recently edited the registry manually can also be a source of the issue. It is also possible that there is a failure in underlying hardware.

A+ 1102: 3.1

One step is to remove recent updates, as it is possible that the update is incompatible with some other software on your system. Windows 10 and 11 both offer a number of options to repair Windows, including System Repair, which can be launched with the following steps:

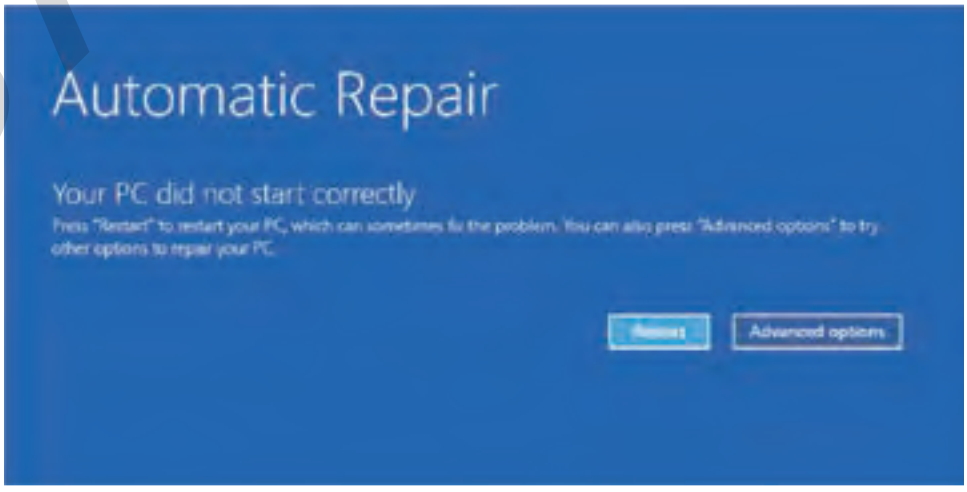
1. Hold down the power button for 10 seconds to turn off your device.
2. Press the power button again to turn on your device.
3. On the first sign that Windows has started (for example, some devices show the manufacturer's logo when restarting) hold down the power button for 10 seconds to turn off your device.
4. Press the power button again to turn on your device.
5. When Windows starts again, hold down the power button for 10 seconds to turn off your device.
6. Press the power button again to turn on your device.
7. This time, allow your device to fully start up.
8. Select **Advanced options.**

If performed correctly, you should see a screen similar to that shown in Figure 17-10. Choose **Advanced options**, and select **Troubleshoot** on the following screen. From here, you can reach screens to perform tasks such as **Startup Repair**, **System Restore**, and **Uninstall Updates**, among others, as shown in Figure 17-11.

A final option is to reset your PC by navigating to **Settings**>**Update & Security**>**Recovery**. This launches the **Recovery** screen, from which you can perform a reset or take other troubleshooting steps, as shown in Figure 17-12.

Hard Drive Failures

Hard drives fail more often than one would think. Any component that combines electrical and mechanical components will fail after a period of time, and hard drives can also fail because of software issues. As an example, a corrupt MBR can cause hard drives to become unresponsive. It is important for you to determine if more than a



Goodheart-Willcox Publisher

Figure 17-10 Performing several hard resets of your device will launch the Windows Automatic Repair option.

Goodheart-Willcox Publisher

Figure 17-11 The Windows Advanced boot options include actions such as **Startup Repair**, **System Restore**, and **Uninstall Updates**, among others.

Goodheart-Willcox Publisher

Figure 17-12 The Windows Recovery menu allows you to perform a system reset or launch other troubleshooting measures.

hard drive is bad, but it is equally important that you also determine *why* it is bad. A bad hard drive or a corrupt MBR will generate a screen message, such as

- invalid partition table;
- error loading operating system; or
- missing operating system.

If any of these error messages appear, you likely have a hard drive problem. To check, try booting the system from a bootable CD/DVD or USB drive. If the system boots normally, you can confirm a hard drive problem.

Mechanical Hard Drive Failure

While solid-state drives are far more common today than the older platter-based hard drives, both are still mechanical and, as you are aware, mechanical parts wear out. A sure sign of an upcoming mechanical hard drive failure is an unusual sound coming from inside the computer when it is being accessed (a read or write

operation is being performed), such as a high-pitched whining or clanking. Strange sounds coming from the hard drive are mechanical in origin and likely cannot be repaired, making replacement the only solution.

The only guaranteed method of fully recovering from a hard drive failure is by regularly backing up data. You can always reinstall a collection of software when replacing a hard drive, but the data will be lost unless a recent backup has been made. Users should be instructed to back up data regularly, but it is even more important when a hard drive begins making strange sounds. Data should be backed up immediately, and a technician should be called to prepare for the crash. The technician should have parts on hand and be prepared to replace the hard drive.

MBR Failure and Recovery

Hard drives can also fail because of corrupted files and data. The most important area of the hard drive is the master boot record (MBR), and if it is damaged, the hard drive will not support the booting process. However, you will still be able to boot from a bootable USB or CD/DVD. Once you boot from the USB or CD/DVD, try to look at the hard drive by entering the **dir C:** command at the command prompt, as shown in Figure 17-13. If you can view the files on the hard drive, then you can perform a repair and may be able to remedy the situation. As a precaution, back up all data immediately.

You will not be able to back up the files in every situation, but if you can see files on the hard drive, you should be able to back up important data to some kind of data storage media. Generally, on an older system, you will be forced to copy files to a disc. However, on some newer systems, you may be able to access the drive via an existing network connection.

A computer with a bootable CD/DVD allows for a quicker and easier backup of system files. You can boot the PC using a system restore CD/DVD, which loads all necessary files to boot the PC. In addition, you may load a driver to support the CD/DVD, and once the drivers are loaded, you can copy files that need to be backed up.

Many third-party software systems can repair an MBR, especially if the software is installed before the problem develops. Software recovery systems make a copy of all vital information, including the MBR. When an error occurs, the recovery software can use the copy to recover the damaged system. In addition, third-party software systems can be used to inspect, copy, and modify bytes in each sector of the hard drive. This is a very powerful tool, but using it can be time-consuming.

Windows has built-in utilities to assist with hard drive failures. Previous versions of Windows included the **fsidk** command, which is no longer available as of

Figure 17-13 Users can examine the hard drive through the command prompt. If files are shown, you should be able to repair the drive and save the data.

Goodheart-Willcox Publisher

the release of Windows 7 and **bootrec.exe**, which was removed in Windows 8. For Windows 10 and 11, you should use the **diskpart** command interpreter, which helps manage the drives installed on a computer. When the **diskpart** command is issued at the command prompt, you launch the diskpart prompt, which allows you to issue other **diskpart** commands, such as those shown in Figure 17-14. In Figure 17-15, you can see DiskPart being used to display details about the disk.

A GUID partition has a protected backup of the partition located on the hard drive and automatically rebuilds the GUID partition table on failure. Also, the Windows operating system has an option to create an image of the entire disk, including the GUID partition table, which can be used to recover the entire computer system.

Read and Write Failure

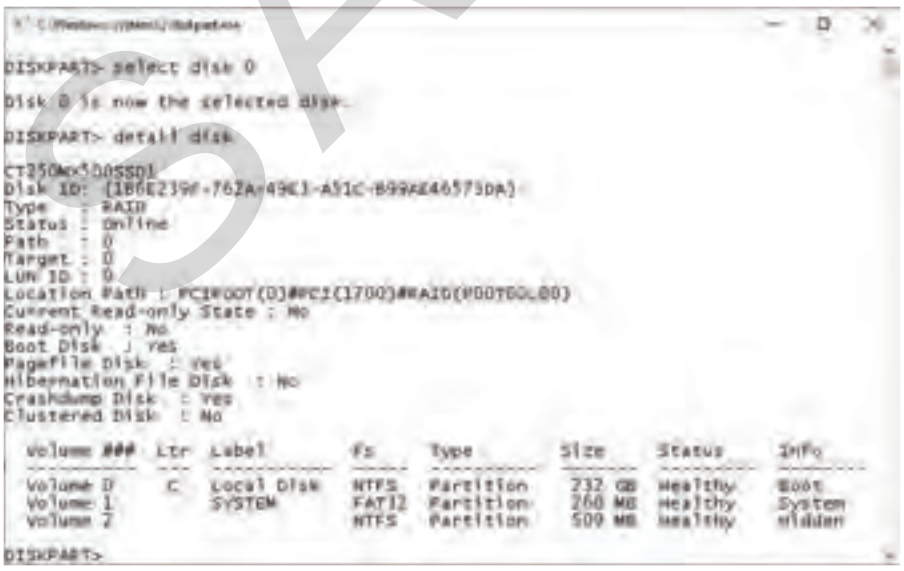
1101: 5.2, 5.3 A+
1102: 3.1

Although there are multiple methods for repairing a hard drive, there is still a possibility that a hard drive may become faulty during its functionality before, during, or after its repair. If the read-write head becomes damaged or impaired, users and

DiskPart Commands	
Command	**Function**
clean	Removes all formatting from the active disk
create	Creates a new partition
delete	Removes an existing partition
detail	Displays detailed information about the selected disk/partition/volume
exit	Exits the diskpart command interpreter
filesystems	Displays information about the file system of the currently selected volume
format	Formats a disk or volume
help	Displays all available commands
repair	Repairs RAID 5 volumes
select	Allows you to select a disk, partition, or volume

Goodheart-Willcox Publisher

Figure 17-14 DiskPart is a command-line interpreter used to manage Windows disks and partitions.



Goodheart-Willcox Publisher

Figure 17-15 The **detail disk** command reveals information about a disk, including the disk ID, disk type, status, path, target, LUN ID, location, and its status as a boot disk, among other facts.

technicians may not be able to retrieve data from the hard drive. Even if the technician *is* able to retrieve data, they will not likely be able to make modifications to it. Lastly, damage to the platters or read-write head of a hard drive may cause the functionality of the hard drive to perform more slowly, along with a noticeable amount of noise, such as grinding or clicking, when the hard drive is not performing to its utmost functionality. To further investigate whether a hard drive is faulty, a technician can utilize a machine's S.M.A.R.T. error screenings.

A+ 1101: 5.3

RAID and S.M.A.R.T. Error Detections

As of the writing of this chapter, the majority of hard drive implementation for a server is utilized via cloud-based technologies; however, technicians may encounter server hard drives such as a *Redundant Array of Independent Disks (RAID)*. RAID implementation can be recognized as a form of hardware and software for its hard drive disk management. The Disk Management tool of a Windows server can be configured to use RAID 0 or RAID 2. For a technician to observe and repair errors via a RAID's functionality, a technician may observe and repair any errors that may have occurred through what is called S.M.A.R.T. Error Detections.

The S.M.A.R.T. Error Detection Tool can be found in Control Panel in both standard Windows and Windows Server. When a technician uses this tool, they can discover when a drive produced an error, was not functioning properly, or if a drive needs to be replaced. Furthermore, the S.M.A.R.T. Error Detection Tool may provide fixes for technicians such as the hard drive needing to be reformatted or if the disk needs to have miscellaneous data removed to utilize the necessary hard drive space needed for present and future files and data.

Disk Management

While the prior-mentioned criteria were based on hardware, other precautions may be taken to adhere to the health of a hard drive. One precaution a technician can utilize is using the Disk Management tool, which can be found easily via a Windows search. From this tool, a technician can defragment, partition, add arrays, and control the amount of storage space allotted to a user. Although this implementation is still in practice, it is important for technicians to understand that hard drive utilization is diminishing for both personal computers and servers, and that data is being stored via cloud-based technologies.

Additional Mechanical Problems

A number of other mechanical faults can cause problems in PCs. Boards, cards, and cables can go bad, but these occurrences are not all that common. You will find that, along with hard drive failure, most other mechanical problems arise from two areas: improper hardware upgrades and accumulation of dust in the system.

Problems after Hardware Upgrades

Many possible system failures can occur after a hardware upgrade. The first thing to check when a system fails to boot is the power and cable connections. While working inside the case, cables are often pulled loose, so look for any free-hanging cables. Take caution when reconnecting the cable so as not to damage any pins, and make sure you connect it to the correct location. There are multiple examples of technicians reconnecting cables to the wrong connection point or reconnecting a cable upside and bending a pin in the process. Additionally, cables can be pinched when systems are reassembled, so ensure cables are tucked away before reassembling the case.

Another major problem occurs when mixing different generation technologies together inside the same PC. When a PC has been upgraded several times, problems do arise. For example, an older BIOS chip may not be able to recognize a new

memory module or see the new hard drive that has been installed. Check the system resources for conflicts using Device Manager or the Microsoft System Information utility.

Dust Accumulation

1102: 4.5 A+

The accumulation of dust inside a PC is typical, and the type of environment in which the PC operates, as well as its age, determines how much dust has accumulated. Large amounts of dust can cause heating problems by blocking air filters and by collecting on processor heat sink fins and fan components, preventing the proper dissipation of heat. The dust acts like an insulator and holds the heat to the CPU rather than allowing the cooling fans to dissipate it. Dust can also clog air filters and render a fan inoperable.

Remove dust carefully using a can of compressed air or a special vacuum cleaner designed for PC cleaning. Standard vacuum cleaners generate a tremendous amount of static electricity, which is very dangerous to computer chips, so you should only use vacuum cleaners made specifically for electronic equipment.

System and Intermittent Device Failure

The chapter has provided you with excellent troubleshooting tactics by providing information of what criteria and data is needed for a personal computer to boot and access its operating system. However, other symptoms may cause a personal computer to lock up, overheat, cause loud disruptive noises, and other intermittent device failures. When a technician understands that these issues may arise, it also augments their troubleshooting abilities.

System Lockups

Regardless of a personal computer model and its operating system, a technician should always assume that eventually, a user will experience what is called a lockup. *Lockups* are primarily discovered when an operating system cannot be modified and users perceive that the screen has frozen, since they do not see their mouse moving or their applications functioning. In reality, what has happened is that either the RAM has been overutilized or the CPU has been overclocked. Although users are resistant toward the troubleshooting tactics to fix this issue, normally powering the machine off and advising the user not to run as many applications is the best solution to fix a system lockup.

Intermittent Device Failures

Personal computers may experience intermittent device failures, and it is important that a technician understands the warning signs of these failures. Although each model of a personal computer may be vastly different, it should have a serial number or service tag located on the console portion of the machine for a technician to obtain parts and warranty information. Once these numbers are obtained, it is recommended that a technician either call the vendor's customer service line or access its website to ascertain the most common device failures their machines are experiencing. Once this information is obtained, it is still vital that a technician take other precautions than only the common device failures advised by the vendor of the machine.

1101: 5.2, 5.3 A+

A computer will often overheat if it becomes too dusty, has been operating for an ample amount of time, or has a faulty cooling fan. Furthermore, when a machine tends to overheat or internal hardware components of the machine become faulty, it will make an ample amount of noise, such as grinding or clicking. Should a technician experience this, they will need to remove the case of the personal computer and troubleshoot the origin of the problem. Should a technician not be able to find the cause of the faulty hardware, they will then need to either access the system's

BIOS or boot into Windows Safe Mode to obtain the proper error logs and codes to determine which piece(s) of hardware is faulty. Nevertheless, if a technician is not able to repair the hardware needed to make a personal machine functional, they will need to adhere to data recovery techniques.

A+ 1101: 5.5

Mobile Device Issues

If a user is experiencing a mobile device that is not loading applications or is not functioning properly, the first troubleshooting precaution for a technician to take is to make sure the mobile device is not overheating. This is a common factor among mobile device failures, and technicians should always check to see if the battery appears to be swollen if the mobile device feels warm. If the battery appears to be excessively swollen, it is vital that the technician take the mobile device to a cooler area and not attempt to work on the phone until it has cooled down and the battery swelling decreases. Once the mobile device is safe to troubleshoot, technicians may adhere to their troubleshooting implementation.

Other common mobile device errors that users experience include when their mobile devices freeze, or they have forgotten their credentials to log into their devices. If a user's mobile device becomes frozen, the technician will be forced to shut the device down manually, which unfortunately means that any data that was being used at the time will be lost. Furthermore, when a user forgets their login credentials for their mobile device, technicians will have to format the mobile device to its factory state if there is not a second method of entry into the device, such as administrative access via a Google account through an Android device.

Another troubleshooting technique is obtaining application log error files. Assuming the user synchronizes their data to a Windows PC, the technician can find crash reports by locating those reports on the PC, often in the C:\Users\<USERNAME>\AppData\ folder. However, be advised that this information provides details regarding how or why a phone failed when it was running a certain application or applications, not detailed hardware information.

A common hardware issue for mobile devices is a broken screen. Minor cracks are often purely cosmetic, and the device can continue operating in its current state. However, substantial breaking presents a safety issue and should be replaced. These types of screens are generally not field replaceable and often have to be sent back to the manufacturer for repairs. As a result, cases and screen protectors are highly recommended.

17.4 Windows Diagnostic Utilities

Most Microsoft operating systems incorporate the same troubleshooting utilities. You need to become familiar with these utilities to save time when troubleshooting a system problem. Common diagnostic utilities native to Windows include DirectX Diagnostic Tool; System File Checker; Registry Editor; Event Viewer; Problem Steps Recorder; Remote Assistance; Problem Reports and Solutions; Performance, Resource, and Reliability Monitors; Memory Diagnostics Tool; and Component Services.

DirectX Diagnostic Tool

DirectX is a software development tool used for multimedia applications that allows programmers to access many Windows built-in features, but a poorly written program using DirectX can cause severe system hangs or crashes. The DirectX Diagnostic Tool (**dxdiag.exe**) looks at every DirectX program file on the computer, as shown in Figure 17-16. You can look for non-Microsoft-approved program labels here. If a file is Microsoft approved, you should not have a problem. That cannot be said for other programmers' tools.

DirectX program files are abundant and used for game development and all types of multimedia programs. The DirectX Diagnostic Tool is incorporated into all Windows operating systems but has become much more sophisticated.

System File Checker

1102: 1.2, 3.1 A+

The System File Checker (**sfc.exe**) can be run to check for corrupt, changed, or missing files from Windows-based applications and restore system files. You can launch the System File Checker by entering sfc/scannow at the command prompt, but the command prompt must be run as an administrator. This is accomplished easiest by using the [Windows][X] keyboard combination and selecting **Command Prompt (Admin)**. The **sfc/scannow** command scans all protected system files and replaces incorrect versions with correct versions, as shown in Figure 17-17. System

Goodheart-Willcox Publisher

Figure 17-16 The DirectX Diagnostic Tool checks for problems with DirectX files.

Goodheart-Willcox Publisher

Figure 17-17 System File Checker (**sfc.exe**) can be used to check the integrity of system files.

File Checker is also incorporated into the **Advanced Boot Options** menu. When **Repair Your Computer** is selected, the System File Checker is run automatically, and some Windows machines also run the System File Checker after a system failure is detected.

Tech Tip

Microsoft Register Server (**regsvr32.exe**) is a command-line tool used for adding or removing DLLs and ActiveX controls to or from the system registry. Using Microsoft Register Server will avoid generating system error messages.

Registry Editor

Registry Editor is a Microsoft software tool used to view and modify the system registry files. There are several versions of the tool available depending on the operating system installed and whether you are running a 32-bit or 64-bit operating system. The executable file for 32-bit Windows operating systems is **regedit.exe** and **regedt32.exe**, though running **regedt32.exe** will simply run the **regedit.exe** executable file. The default 64-bit version of Registry Editor is launched using **regedit.exe** and is included with 64-bit versions of Windows. When the 64-bit version is launched, it will display both 64-bit keys and 32-bit keys.

The Registry Editor consists of hives and registry keys. A **hive** is one of five major groupings that are displayed in the left pane of the Registry Editor, as seen in Figure 17-18. A **registry key** is a nested folder within a hive. Values for each registry key are displayed in the right pane. Registry Editor is a powerful tool and allows technicians to change the values associated with registry keys. You must use extreme caution when you use it to change registry values, however, as missing or incorrect values in the registry can make Windows unusable. There are times when a technician may need to change the values of registry keys. For example, when a new virus is released and causing a problem with a computer, Microsoft may provide reference material as to how to remove the virus. The information may also contain directions for changing or deleting registry values. Changing the system configuration should be performed through Control Panel or through Microsoft utilities designed for that purpose. In general, you should not make changes to the computer system using the Registry Editor.

You should never attempt to repair the registry files directly. An error made in the registry files can render the computer system inoperable, resulting in your having to reinstall the system onto a clean hard drive. Simply loading the software over the corrupt registry would do no good because the new installation would inherit the previous corrupt settings.

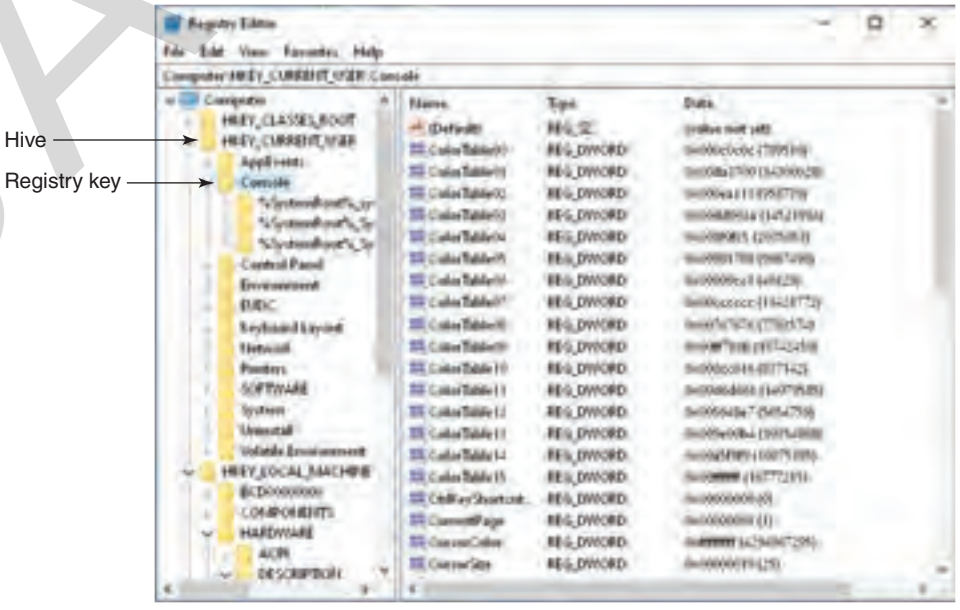


Figure 17-18 Registry Editor is a Microsoft software tool that is used to view and modify the system registry files.

Goodheart-Willcox Publisher

Event Viewer

1102: 1.3 A+

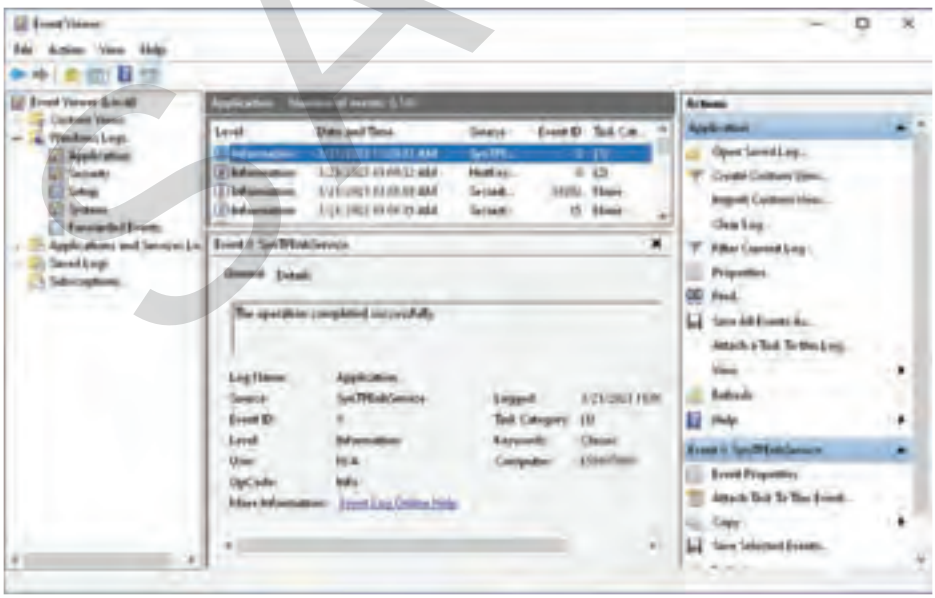
Event Viewer, shown in Figure 17-19, is a centralized depository of various logs relating to system setup and configuration, applications, security, and more. These logs are categorized by event types, including

- *Error*, indicated by a red circle with an exclamation point;
- *Warning*, indicated by a yellow triangle with an exclamation point;
- *Information*, indicated by a white circle with a blue I; and
- *Audit success*, indicated by a key icon.

Each log can be viewed in chronological order or by categories such as event and user. Since the log files in Event Viewer retain a history of events that have occurred on the PC, they are a valuable troubleshooting tool. For example, users typically do not want to reveal information about installed software such as games, especially if gaming software is against company policy. Using Event Viewer, a technician can quickly view a list of software changes and obtain objective data that can be used to identify possible causes of system problems.

Specific types of events can be selected from the list of Windows logs located in the left pane of Event Viewer, and individual events (located in the middle pane of Event Viewer) can be opened to reveal details about the event, as shown in Figure 17-20. Notice that more information about the event can be accessed through the **Event Log Online Help** option. To find more about the extensive capabilities of the Event Viewer, use Windows Help and Support.

There can be many different log files on a computer system, not just the ones discussed in this section. Software and hardware manufacturers write their own log file collection programs to assist them (and you) in determining problems that may have occurred during the installation of their hardware or software package. The log files can be used to relay information to technical support personnel by e-mail or telephone. Sometimes these files can be accessed remotely by technical support personnel.



Goodheart-Willcox Publisher

Figure 17-19 Event Viewer collects information about events that happen relating to the computer system, and it stores a description of the event in a log.

Problem Steps Recorder

Problem Steps Recorder is a screen capture tool to record a problem as it is occurring. A series of screen captures are generated while the utility is running, and once the recording is stopped, comments can be added, and the entire recording session can be saved as a zipped (compressed) file in the MIME HTML (MHTML) format. The file can then be sent by e-mail to a technician or help desk for viewing. The technician can see exactly what problem occurred on the computer. The recorder is launched by entering psr into the **Search** box located off the **Start** menu in Windows 10 or Windows 11 and then selecting **Steps Recorder** from the results.

The Problem Steps Recorder is a very simple and intuitive tool. As you can see in Figure 17-21, it has controls for recording, pausing, or stopping the recording. Saving and naming the file is accomplished similarly to any other program. It should be noted that not all types of problems can be recorded, but most involving software applications can, especially ones that generate cryptic error messages that users cannot interpret.

Remote Assistance

Remote Assistance was first introduced with Windows XP and continues to be a part of all Windows operating systems. It allows a user to invite another user to access their computer and assist in repair. The user needing help sends an e-mail invitation to another person, such as a technical support person, and technical support can then repair the system while chatting with the user.

Remote Assistance should not be confused with Remote Desktop, which allows a user to connect directly to their computer from another location. For example, a user could connect to the office computer from a home computer and have complete control over the office computer just as if they were sitting at its keyboard. Remote Assistance is a temporary connection, and a person must be present at both locations.

Figure 17-22 shows the Remote Assistance and Remote Desktop options listed in the **System Properties** dialog box. Remote Desktop can only be initiated from a computer running Windows Professional and Ultimate editions, but any version

Figure 17-20 Detailed information about an event is shown in the **Event Properties** dialog box, which is accessed by double-clicking the event.

Goodheart-Willcox Publisher

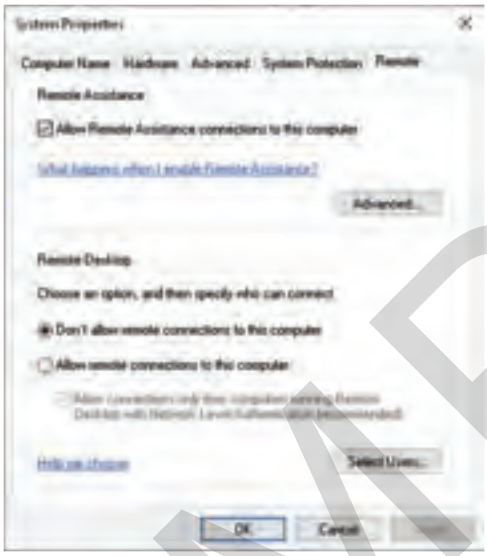
Figure 17-21 The Problem Steps Recorder tool creates a series of screen captures while recording computer problems.

Goodheart-Willcox Publisher

of Windows can return the connection to the computer that starts the Remote Desktop connection. For example, you can start a Remote Desktop connection session from any location running Windows Professional and then access the Windows Professional computer system from another computer running Windows Home Basic. There are no such restrictions for Remote Assistance.

Windows Security and Maintenance

As shown in Figure 17-23, Windows 10 features a utility called Security and Maintenance, which identifies problems as they occur on the system and can be used to automatically find solutions. Problems are automatically reported to



Goodheart-Willcox Publisher

Figure 17-22 Two remote access programs are available in Windows: Remote Assistance and Remote Desktop.

Goodheart-Willcox Publisher

Figure 17-23 The **Security and Maintenance** menu in Windows provides an easy way to assess the security and functionality of a computer.

Microsoft via the Internet, and if a solution is known, it is sent to the computer. A complete history of all problems and solutions can be archived for future use and diagnostics, which is a significant improvement over previous versions of error-reporting utilities. Security and Maintenance is the successor to Problem Reports and Solutions utility introduced in Windows Vista and the Action Center that existed in Windows 7 and Windows 8.

You can use Security and Maintenance to review important notifications about security and maintenance settings that need your attention, obtain information about specific system settings, and perform recommended maintenance tasks. You can also find helpful links to troubleshooters and other tools that can help fix problems. Note, you must be connected to the Internet to check for solutions to the problems shown in this utility.

Security and Maintenance is accessed by selecting **Start**>**Control Panel**>**System and Security**>**Security and Maintenance**. Additionally, if a problem occurs on your computer that you need to address, you will see a notification in the notification area of the taskbar. When you hover over the icon in the taskbar, you will see all the recent notifications. A red circle with an *x* indicates a message about a serious problem, such as an application failure. A black clock means there is a scheduled task running in the background. A yellow exclamation point represents informational issues, which are less serious than those indicated by a red circle with an *x*. A blue *i* is used to indicate general information about the system and is not serious.

A+ Note

Be sure you familiarize yourself with all the various diagnostic tools available in the Windows operating systems. Open the Microsoft System Configuration Utility (**msconfig.exe**) and select the **Tools** tab to see a list of some of the most common diagnostic tools.

A+ 1102: 1.3

Windows Performance, Resource, and Reliability Monitors

Windows includes performance, resource, and reliability monitors, which provide detailed information about performance issues and system reliability. Performance Monitor can be configured to collect data about the computer system and specific hardware devices. Figure 17-24 shows Performance Monitor running and collecting data about a computer system.

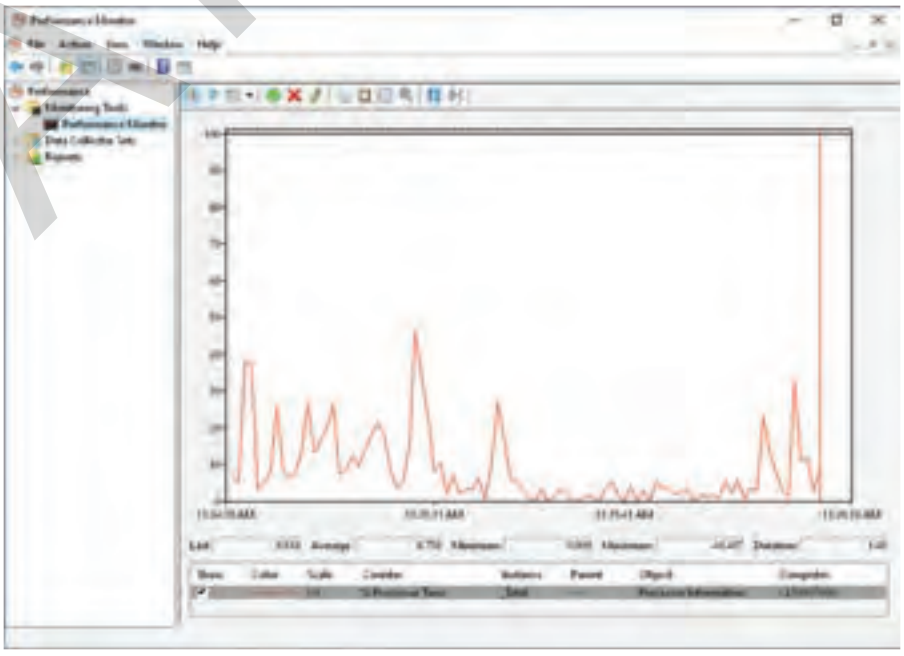


Figure 17-24 Performance Monitor examines how programs affect the computer's performance.

Goodheart-Willcox Publisher

Resource Monitor allows you to observe the effects of specific programs and services on computer hardware and resources. In Figure 17-25, Resource Monitor displays charts of system performance as it relates to the CPU, disk drive, network connection, and memory. You can select services and programs to monitor by clicking the box next to the service or program.

Both Performance Monitor and Resource Monitor can be very useful in determining the reason behind problems such as sluggish performance. Identifying the process(es) consuming the most resources can help you to find the root cause for the sluggish performance. For example, you may need to add more resources, such as RAM, to your device to run a particular process, or you may need to shut down unneeded processes to free additional resources. Either way, Performance Monitor and Resource Monitor can help you make that determination.

1101: 5.2 A+

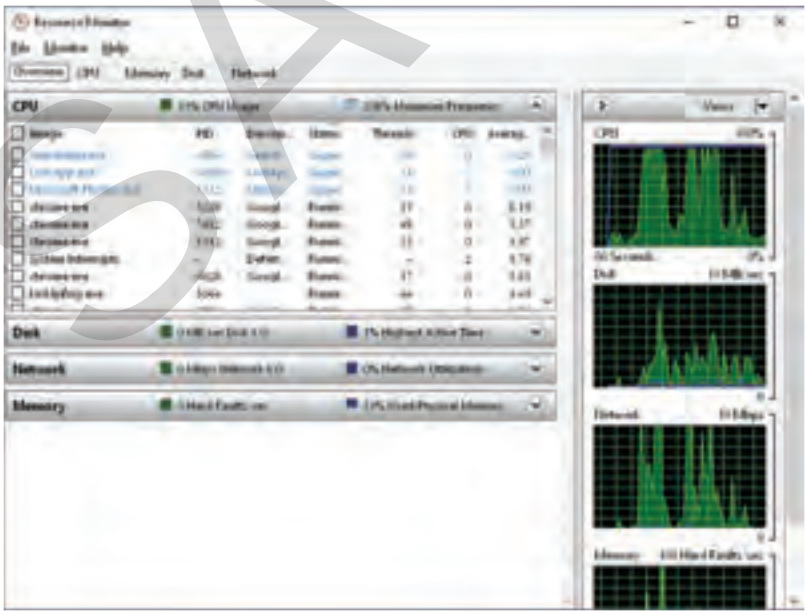
Reliability Monitor observes and records computer events that affect computer stability. It produces a historical graph appearing as a linear calendar of recorded events and indicates the seriousness of the events using icons such as a red *x* for severe events, a yellow triangle with an exclamation point for warnings, and a blue *i* for information. The effect on computer stability is displayed in graphic form on a scale from one to ten, with ten being the most severe. See Figure 17-26. This tool is similar to Event Viewer but, as you can see, much more compact and easier to interpret. Reviewing the reliability history will help locate the origin of computer problems. Reliability Monitor is another great addition to the technician's assortment of troubleshooting tools.

As of the release of Windows 7, Reliability Monitor is no longer listed as a separate tool and is instead shown as a chart listing reliability issues. The Reliability Monitor history is accessed through **Start**>**Control Panel**>**System and Security**>**Security and Maintenance**>**View reliability history**, as shown in Figure 17-27.

Windows Memory Diagnostics Tool

1102: 1.4 A+

Memory problems can be difficult to identify because they can occur intermittently. For example, if a computer slowly overheats after an extended period of time, RAM could stop working or cause software program errors. Often, a technician may completely reinstall the operating system only to have a random error reoccur.



Goodheart-Willcox Publisher

Figure 17-25 Resource Monitor allows you to view the performance of computer systems and resources, such as the CPU, memory, disk, and network system.

Figure 17-26 Reliability Monitor shows the history of all problems that have occurred on the computer.

Goodheart-Willcox Publisher

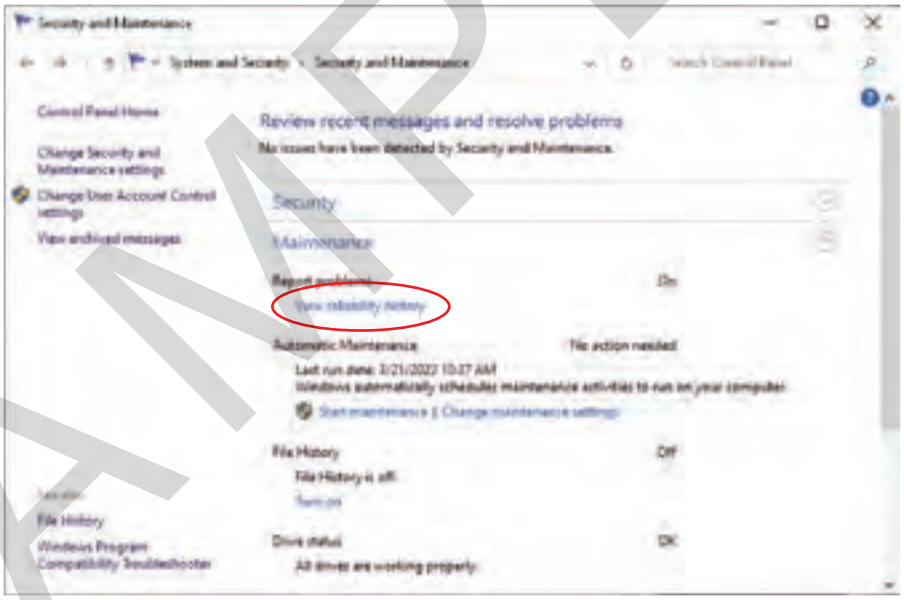


Figure 17-27 The Reliability Monitor is accessed through the Security and Maintenance window.

Goodheart-Willcox Publisher

Windows Vista first introduced the Memory Diagnostics Tool, which diagnoses memory module problems. If the Memory Diagnostics Tool detects a problem with a section of RAM, it automatically restricts the use of the RAM cell locations, which allows the computer to be used until the RAM is replaced.

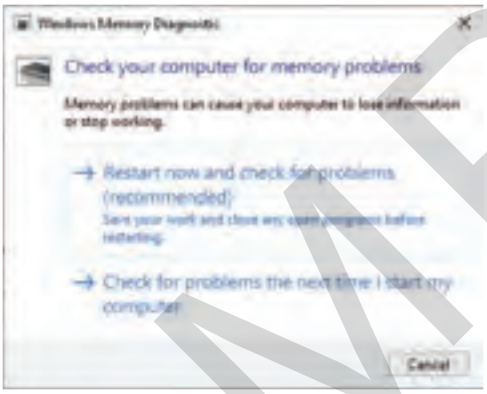
In all versions of Windows, the Memory Diagnostics Tool is accessed through **Start**>**All Apps**>**Windows Administrative Tools**>**Windows Memory Diagnostic Tool**. You can also start the Windows Memory Diagnostics Tool from the command line by entering mdsched at the command prompt, though the command prompt needs to be opened with administrative rights in order to run the Memory Diagnostics Tool from the command line.

Figure 17-28 shows the **Windows Memory Diagnostics Tool** dialog box. Notice that the test can be performed immediately or scheduled to run the next time the computer is started. The **Windows Memory Diagnostics Tool** in progress looks similar to that in Figure 17-29. Notice that the status of the memory diagnostics appears on the screen in text mode, not graphic mode. The progress of the tests is presented as a bar graph and as a numerical percentage. Any problems identified are also presented on the screen.

Component Services

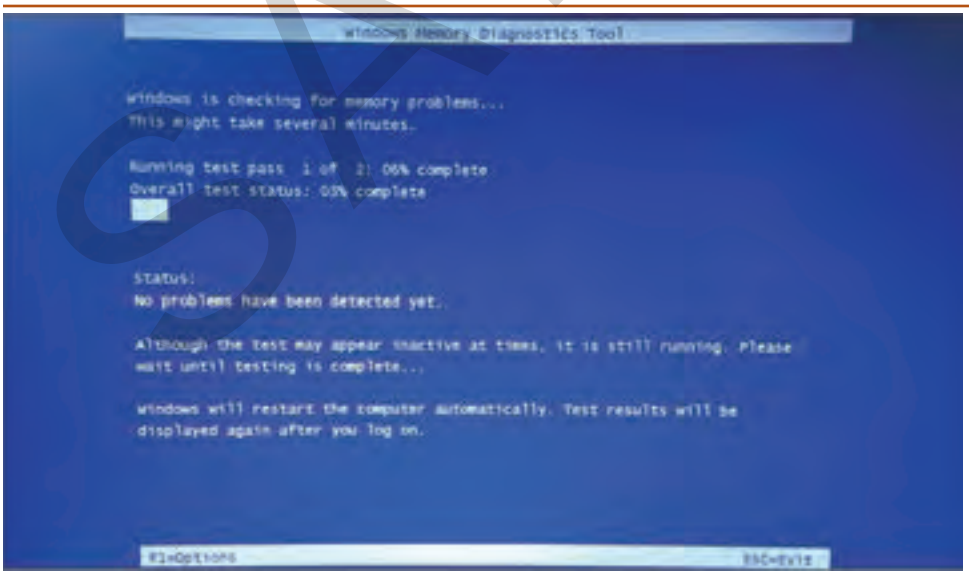
1102: 1.4 A+

The Component Services utility contains a Component Object Model (COM) that provides a suite of low-level drivers and interfaces that are needed to communicate and operate certain aspects of a personal computer. With the COM, certain software will not be able to be functional on a personal computer. Although it is suggested that a technician not make modifications to COM settings since they are installed when software installation is complete and seldom need to be configured, technicians are able to view or make modifications to COM settings, as shown in Figure 17-30.



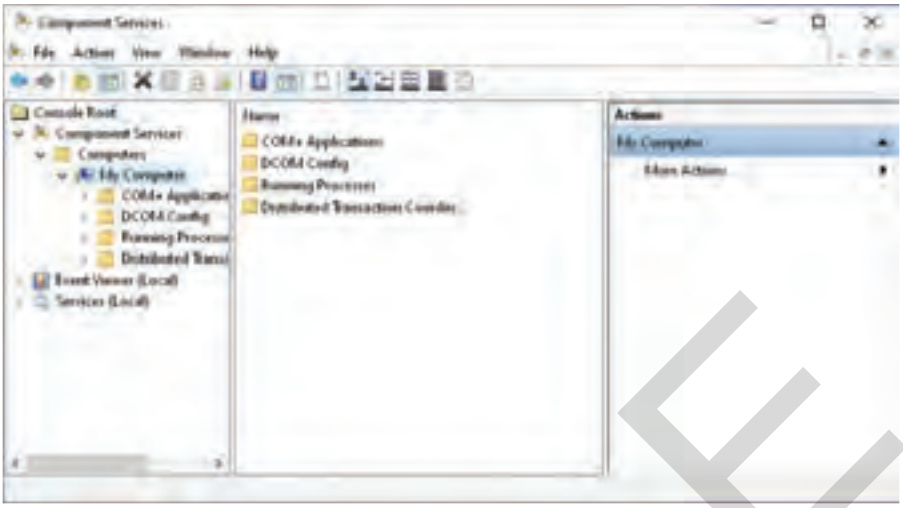
Goodheart-Willcox Publisher

Figure 17-28 The Windows Memory Diagnostics Tool was first introduced in Windows Vista.



Goodheart-Willcox Publisher

Figure 17-29 The Windows Memory Diagnostics Tool diagnoses memory module problems.



Goodheart-Willcox Publisher

Figure 17-30 Component Services provides a suite of drivers needed to communicate with certain aspects of the computer.

17.5 Boot Sequences

A good understanding of the startup process is an essential part of troubleshooting. Therefore, it is imperative that you study the boot sequence of all standard operating systems and compare the differences. One way to accomplish this is to study the programs associated with the boot disc created for each system. The boot disc contains the files necessary to boot the computer as well as some of the various enhancement files. Not all files on a boot disc are necessary for booting the system. Note, the term *boot disc* refers to any disc used to start the computer system. This is synonymous with *startup disc*, *recovery disc*, or *system repair disc*. The six phases of the Windows boot process are

- POST;
- initial startup phase;
- Windows Boot Manager phase;
- Windows Boot Loader phase;
- kernel loading phase; and
- logon phase.

Power-On Self-Test (POST)

As you now know, when a computer has power first applied to the motherboard by pressing the power switch, the BIOS or UEFI will start the boot process with a quick check of hardware components to verify that all hardware devices listed in the firmware configuration database (CMOS) are present and appear to be in working order. The firmware configuration settings are typically automatically detected or manually modified when the computer is first assembled and started the very first time. The BIOS/UEFI has a default configuration that will start most computers without a problem, but not always. Some BIOS/UEFI configurations require technician modification. The hard drive is automatically detected and configured by the BIOS/UEFI and typically does not need to be modified by the technician because all configuration data is then stored in the CMOS memory.

All systems today use either BIOS or UEFI as the first computer software routine to run on the computer, and the BIOS/UEFI is independent from the operating system. Since the POST is independent of the operating system, it is safe to assume that there is a hardware problem if the computer fails during the POST, or the POST

generates an error message or series of beeps. You can research the error message or beep codes at the BIOS or motherboard manufacturer website or conduct an online search using the contents of the error message as the key terms. The following is a partial list of the system hardware checked during the POST:

- CPU system clock
- CPU registers
- Keyboard controller
- Video controller
- RAM
- Disk controllers
- Motherboard bus
- Adapter card ROM

When POST is complete, some adapters such as video cards or hard drives may conduct their own firmware diagnostics routine, which is independent from BIOS diagnostics.

The United Extensible Firmware Interface (UEFI) is a new approach to the BIOS system. The original BIOS program was first developed in the late 1970s, and before that, each computer manufacturer had to have a matching operating system designed especially for that computer. After the BIOS was developed, you could run a variety of operating systems on the same computer. The BIOS was responsible for linking the communication between the operating system and the PC hardware.

Extensible Firmware Interface (EFI) was first introduced by Intel, but now a large group of computer hardware manufacturers is involved with creating a set of standards of design for EFI. The group organization is the United EFI (UEFI), thus EFI is now referred to as UEFI. It can be installed to work directly with the BIOS or as a replacement for the BIOS. UEFI is required on computers to use a GUID Partition Table (GPT). The transition from BIOS to UEFI has been, and will continue to be gradual, not abrupt.

There are extreme differences when comparing BIOS systems to UEFI-based systems. The BIOS is limited in size—typically less than 1 MB of ROM—and it uses 16-bit drivers. UEFI, on the other hand, is not limited in size and can load 32-bit and 64-bit drivers before the operating system is loaded. UEFI can also load and run applications during the POST without the loading of an operating system. For example, a diagnostic utility or disaster recovery tool, or even a virus scanning program, can be run before the operating system is loaded.

BIOS is not governed by any collective organization, and there is no one set of standards controlling the design of BIOS code. The United EFI (UEFI) organization has designed the EFI to be vendor-neutral, so no one operating system or BIOS manufacturer can control the firmware coding. All source code is open and shared so all software and hardware designers have full access to the EFI coding.

Initial Startup Phase

For the initial startup phase in a BIOS-based system, the POST completes and then looks for the boot device where the MBR is stored. The BIOS configuration determines the order for the computer system to locate the next boot device. The boot device could be the hard drive, optical drive, or USB flash drive. The exact order can be changed in the BIOS setup utility and stored in the CMOS memory. In general, the computer uses the hard drive as the boot device, but exceptions exist such as when a boot disc is used to start the computer or when an installation CD/DVD is used to install or recover an operating system. After identifying the location of the MBR, the BIOS loads the MBR or ntldr file into RAM or the Windows Boot Manager (bootmgr), depending on the operating system installed.

Keep in mind, you cannot use a nonbootable CD, DVD, or flash drive to start the computer. When nonbootable media is encountered during the boot sequence, an error message will appear on the screen. Some possible errors include the following:

- Non-system disc
- Missing Ntloader (ntldr)
- Hard disk errors

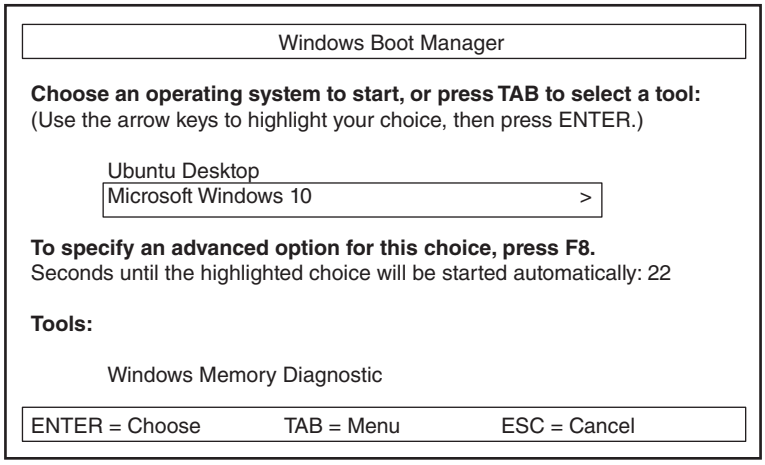
In a UEFI system, a GUID Partition Table (GPT) is used instead of an MBR to locate partitions on a physical disk. This table overcomes the partition limitations imposed by the MBR. Before GPT, Microsoft operating system partitioning was based on the limitations of the MBR. Partitions could consist of four primary partitions or three primary partitions plus one extended partition subdivided into logical partitions. This is an archaic partitioning system, which evolved from the DOS file system and had a maximum number of 128 partitions that could be supported by the Microsoft MBR. Since the GPT partitioning system does not have the same limitations of MBR-based partitions, you can have an almost unlimited number of partitions using GPT. UEFI does not require a GPT and can be used with a partition system based on MBR. Additionally, UEFI can use a disk system that contains both GPT and MBR partitions.

Windows Boot Sequence

Starting with Windows Vista, ntldr has been replaced by the Windows Boot Manager (bootmgr) and Windows Boot Loader (**winload.exe**). Ntdetect is incorporated into the kernel. Windows now also uses Boot Configuration Data (BCD) in place of the **boot.ini** file. This section begins with the Boot Manager phase.

Boot Manager Phase

The Windows Boot Manager (bootmgr) is used to select which operating system to load when more than one operating system is present on a computer. If more than one operating system is installed on a computer, a screen similar to the one in Figure 17-31 will appear. The Windows Boot Manager screen does not appear if only one operating system is installed on a computer, though it still runs even if it does not appear on the display. The default for the boot manager is 30 seconds, but the delay is reduced to approximately two seconds when only one operating system is present. It is during this two-second interval that the [F8] key can be pressed to interrupt the boot process causing the **Advanced Boot Options** menu to appear. As stated previously, the process was changed from simply pressing [F8] to pressing



Goodheart-Willcox Publisher

Figure 17-31 The Windows Boot Manager menu will appear by default if there are multiple operating systems on the computer.

[Shift][F8], but this key combination often does not work because the system simply boots too fast to interrupt the system. Instead, you can modify startup in the **Advanced startup** menu accessed through **PC settings** as presented earlier in the chapter. Once the appropriate boot device is selected, the Windows Boot Manager passes control to the Windows Boot Loader.

Boot Loader Phase

In this phase, the Windows Boot Loader first loads the kernel (**ntoskrnl.exe**) into RAM but does not yet execute it. The Windows Boot Loader file is determined by the type of firmware used: BIOS or UEFI. A BIOS-based system uses **winload.exe**, and a UEFI-based system uses **winload.efi**. Next, the hardware abstraction layer file (**hal.dll**) is loaded into RAM as well as the system registry hive. Certain key services are started to support various device drivers that are required during the boot process. Lastly, the kernel (**ntoskrnl.exe**) is executed and takes over operation of the computer system.

Kernel Loading Phase

After the kernel (**ntoskrnl.exe**) is executed, it and the hardware abstraction layer (**hal.dll**) work together to communicate with software applications, drivers, and hardware. Additionally, driver files that do not require user security clearance are typically loaded. For example, the driver and services required to minimally run the printer are loaded at this time.

The kernel and hardware abstraction layer work together to process information stored in the registry, which is required to complete the boot process. The kernel also creates a new registry key, which contains information about the drivers and devices loaded so far and through the rest of the boot operation. This information is used for the **Last Known Good Configuration** boot option when troubleshooting the system or attempting to recover from a system failure. The kernel then loads the Session Manager (**smss.exe**) and the boot process switches from text mode to graphic mode, indicated by a progress bar appearing at the bottom of the screen. The Session Manager continues to run in the background until the computer is shut down.

The Session Manager starts and runs an abbreviated version of chkdsk to determine if the system volumes and partitions are in working order. The Session Manager is also responsible for loading the page file or virtual memory. The page file supplements the amount of RAM installed on the computer.

Microsoft does not allow third-party software applications to access hardware and certain operating system files directly. However, when access is needed by third-party software applications, the Session Manager manages the activities. If the startup process fails here, you will see a blue screen error. Recall that a blue screen error is a full-screen text message describing the error on a plain, blue background. There will be a cryptic error code that can be used to conduct a search at the Microsoft website to find the most likely cause. Microsoft has a very extensive collection of troubleshooting information at its TechNet website.

Logon Phase

The logon phase is the last phase in the startup process during which the Windows logon file (**winlogon.exe**) is executed, and the Windows **Logon** dialog box appears. A user typically enters their logon name and password to proceed to the operating system desktop.

After a successful logon, the Local Security Authority (LSA) file (**lsass.exe**) loads and runs, followed by the service subsystem file, **services.exe**. The exact services loaded and started are determined by the computer's configuration and the user's credentials. Only the services the user is allowed to access will start. If there is

only one default user and the computer is not connected to a network with a server, the user can access and run all services for the computer. However, if a user has a limited account, they will only be able to run services allocated by the system administrator.

Startup programs are loaded and run at this point. Any problems such as the computer locking up or the desktop taking a long time to appear are associated with the startup files and services. If a user installs many programs over a period of time, the appearance of the desktop after completing logon will take more time.

After a successful logon, the boot process is considered a success. The registry is updated and will become the registry reference for the "Last Known Good Configuration." A failure of the system after logon is usually a sign of a failed service or a software startup application. One of the best utilities for analyzing failures after logon is the Microsoft System Configuration Utility (**msconfig.exe**). Services and software applications that might be causing the problem can be selected and isolated from startup with this utility.

17.6 Preventive Maintenance

Performing routine maintenance on the PC can help prevent future problems and improve system performance. Some of the most common but often overlooked routine maintenance items are listed in this section. To help ensure regular maintenance is performed, many of the items can be scheduled to perform automatically.

A+ 1102: 4.3

System Backups

Backups should be performed as part of routine system maintenance. You may not be able to repair a failed computer system, but you can at least restore critical data after installing a clean copy of the operating system. If the system has been configured to perform automatic backups, check to ensure the backups are being performed, as the automatic backup configuration may have been turned off or corrupted. Most backup programs keep a backup log, which is accessible through the program's main menu and can be used to verify that the backup job has run at the scheduled time and that the backup was successful. You should occasionally verify that the data could be read and restored from the backup tape.

If you have installed a patch, however, you should verify that you could still restore data. Microsoft has many problems with their DLL files, which are used in the restoration process and could develop a problem after a system patch is installed. Remember, a system backup is the best data protection against viruses, malware, or other disasters. Antimalware software does not protect files or restore them; only a system backup can do that.

Aside from a full backup, which backs up all data regardless of whether it was updated, there are two commonly accepted methods of backing up files: *incremental* and *differential*. The difference between the two is determined by the **archive bit**, which is a single bit within a file that indicates whether that file has been backed up. This issue is important on large data systems where backups are performed daily to ensure against data loss.

A+ 1102: 4.3

A *synthetic backup*, often called a *synthetic full backup*, begins with the previous full and incremental backups created over a period of time and combines them into a synthesized full backup. This has the effect of creating a full backup, without the time-consuming process normally associated with a full backup.

An **incremental backup** is an operation that only backs up files that have changed since the last backup. An incremental backup requires a disc or tape for each daily backup, and in this instance the archive bit is reset. To reconstruct an

entire collection of data, a copy of the last full data backup plus each incremental backup in sequence must be used, as shown in Figure 17-32. When performing a **differential backup**, *all* data changes since the last full backup are copied. Only one disc or tape is needed to perform the differential backup because it copies all changes in data since the last full backup was performed. To restore the data, you need only the last full backup and the last differential backup. With a differential backup, the archive bit is *not* reset.

The reason for selecting an incremental or differential backup is based on the amount of time and disc or tape space required for each type of backup. Since the incremental backup only copies changes from the last incremental backup, there is less to copy. This results in a shorter time period required to perform the backup. A differential backup copies all data changes since the last full backup. This can require a significant amount of storage space and time if there is a great number of days between full backups. These differences may seem insignificant at first, but when you are talking about the large volumes of data that some corporations generate, you can be talking about significant periods of time and backup storage space.

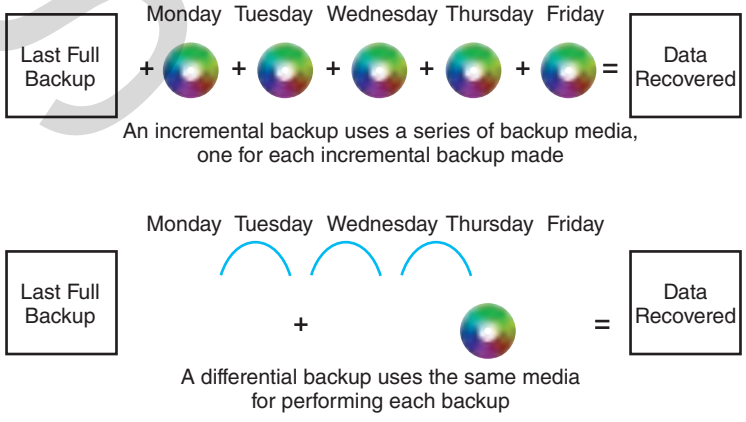
System Image

Windows includes a utility for creating a **system image**, which is an exact replica of a hard drive partition, including all personal and operating system files. The system image can be used to repair a computer system to an exact copy the day the system image was created. The main difference between making a system backup and creating a system image is the selection of files and folders. A system backup allows you to choose which files and folders to back up, but a system image does not allow you to choose which files and folders to copy.

Figure 17-33 shows the options available to create a system image, create a system repair disc, and automatically back up the computer. A system repair disc contains a collection of system recovery files and produces a system recovery menu. The exact look and collection of files is determined by the operating system for which it is created.

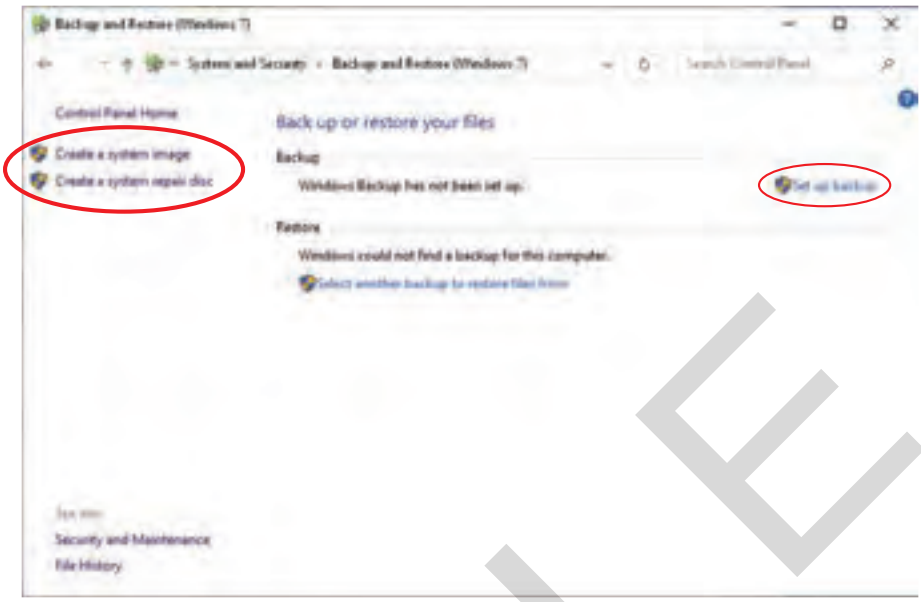
You should make a system image immediately after the initial configuration of a new computer system. You should also periodically create a new system image after making major changes to a computer system such as the installation of a new software application. A system image is vital to computer system recovery after a major system failure.

System backups can be performed on a routine basis such as once a week at a particular time. The backup should be located at another location such as a network drive.



Goodheart-Willcox Publisher

Figure 17-32 The incremental method requires the complete set of discs or tapes plus the last full backup to restore the system data. The differential method requires only the last differential backup made plus the last full backup to restore the system.



Goodheart-Willcox Publisher

Figure 17-33 A system image and a system backup are two of the best options for protection from malware that damage or destroy system files and folders. A system repair disc can be created and used to start a computer that fails to complete the boot sequence.

A+ 1102: 1.3

Disk Cleanup Utility

The Disk Cleanup utility can be used to regain hard drive space consumed by such items as temporary files, files sitting in the Recycle Bin, unused Windows components, unneeded installed programs, and old restore points created by System Restore. Some of the temporary files that Disk Cleanup allows you to remove are downloaded program files, temporary Internet files, and offline files. The Disk Cleanup utility performs the functions of other Windows programs, such as Recycle Bin and Add or Remove Programs. From this one utility, the Recycle Bin can be emptied, saving you the extra steps of accessing Recycle Bin and clicking **Empty Recycle Bin**. Windows components and installed programs can be uninstalled, rather than accessing Add or Remove Programs.

The Disk Cleanup utility can be used to remove all but the most recent restore points created by System Restore, which automatically backs up system information. This information can be used to restore a computer to a previously operational state. Depending on factors such as how much hard drive space is available, how much hard drive space is allocated to System Restore, and the amount of activity on the hard drive, System Restore can save one to three weeks of system information in restore points.

Disk Defragmenter Utility

As you recall from Chapter 10, files can become fragmented over time by opening, closing, and deleting them as well as by changing their contents. These activities can cause a file to become segmented and stored in various clusters across the hard drive. The Disk Defragmenter utility rearranges all files on your hard drive into a continuous series of clusters, resulting in better disk performance. Previously, it was recommended that the Disk Defragmenter utility be run at least once per month depending on the amount of file activity on the system, but since Windows 10 provides built-in defragmentation services, this is no longer the case. Should you desire to do so, be aware that running Disk Defragmenter on a large disk can take a very long time, so schedule the Disk Defragmenter to run when you do not need to use the computer for an extended period of time.

Chkdsk

1102: 1.2 A+

Windows systems use chkdsk to inspect the hard drive and correct errors in the file structure, such as bad sectors, lost clusters, cross-linked files, and directory errors. Some computer problems can be solved, and performance improved, by making sure that the hard drive has no errors.

Figure 17-34 shows the **chkdsk** command and its results. Two common switches used with the chkdsk command are the **/F** switch and the **/R** switch.

- The **/F** switch is used to fix errors automatically as they are located during the disk inspection.
- The **/R** switch is used to locate bad sectors on the disk and recover readable information.

Chkdsk can also be accessed through the hard drive **Properties** dialog box as shown in Figure 17-35. Notice the option for error-checking and the **Check** button. To access the **Properties** dialog box for a hard drive, right-click the drive that you

A+ Note

ScanDisk is an earlier version of a disk-checking program similar to chkdsk. You may see ScanDisk as a distraction answer on the A+ Certification Exam.

Goodheart-Willcox Publisher

Figure 17-34 The **chkdsk** command is used to check the hard drive for disk errors.

Goodheart-Willcox Publisher

Figure 17-35 The hard drive **Properties** dialog box has an option for checking the disk for errors and correcting them, if necessary.

want to check, click **Properties**, and then click the **Tools** tab. Under **Error-checking**, click **Check now**. If you select to repair disk errors automatically and the disk is in use, you will be prompted to reschedule the disk check for the next time you restart the computer.

Install Patches

Check for the latest software patches for your operating system. Patches should be installed on a regular basis, especially as a matter of security. Many operating system security problems are discovered after the release of an operating system. Checking for and installing patches on a regular basis will keep the security level high on the computer system. Some patches can have adverse effects on your computer system, so be sure to back up your system files before installing a patch.

Virus Protection Updates

Virus protection software requires updates on a regular basis, and your virus protection can fail to protect your system if it does not contain the latest virus definitions. Check the company website of your virus protection software for the latest virus information and updates.

Clean the Physical System

Routinely check and clean the cooling system on the computer, including the power supply fan(s) and the fans located on critical components such as the CPU, chipset, memory modules, and video cards. Also, remove dust accumulation from passive heat sinks located in the same areas using a static-free vacuum cleaner.

Also, be sure to remove dust and debris from the keyboard, mouse, and monitor screen. Do not use chemicals when cleaning the plastic parts of a computer system or the screen area. First, attempt to clean the plastic parts with a dry, soft, lint-free cloth, and if that does not clean the area, try a damp cloth. As a last resort, you may use a mild cleaning solution, but keep water away from electronic components inside the computer and computer vents, and avoid the use of any harsh chemicals for cleaning the computer and computer components.

Two Microsoft websites provide extensive information that will be valuable when troubleshooting computers. The first site, Microsoft Support, is designed for the average computer user, and the second website, Microsoft TechNet, is designed for advanced technicians or IT professionals. Save both links in your Internet browser because you will most likely be using them often to assist you in troubleshooting computer problems.

A+ 1101: 5.1

17.7 CompTIA A+ Troubleshooting Objectives

The CompTIA A+ Certification Exam Objectives list a sequence of actions related to troubleshooting. These objectives are a common source for at least one troubleshooting question on the A+ Certification Exam. The objectives are ambiguous and need some explanation. Also, be aware that exact sequence and objective phrasing may change when the exam is updated. The following troubleshooting steps are taken from the 220-1101 CompTIA A+ Certification Exam Objectives in Domain 5:

1. Identify the problem.
2. Establish a theory of probable cause (question the obvious).

3. Test the theory to determine cause.
4. Establish a plan of action to resolve the problem and implement the solution.
5. Verify full system functionality and, if applicable, implement preventive measures.
6. Document findings, actions, and outcomes.

To better prepare you for any questions that may appear on the exam related to these objectives, each step has been expanded and a more detailed explanation given.

Identify the Problem

1101: 5.1 A+

The first step to the troubleshooting process is to identify the problem correctly. You must gather information from the user. The following are typical questions that you should ask as a technician:

- What is the computer doing or not doing?
- When did the problem first occur?
- Did you recently install a software application?
- Can you demonstrate the problem for me?

Do not be surprised if a user is not totally truthful with you. A user will most likely not tell you they attempted to do something against company policy or something they knew was wrong. For example, if the last thing a user did before the problem began was attempt to install a game or a software application, the user may fear losing their job and lie to hide that fact from you.

While not listed as a separate step, you should perform a backup (if possible) before you begin attempting to correct the problem or making any changes to the computer system. After backing up the system, look in Event Viewer, which may prove to be a better source of information than the user regarding what changes have occurred. For example, if the user attempted to install a software package, it will be listed in one of the event logs or the reliability history as an informational event. If the customer has caused the problem, do not make the customer feel uncomfortable about it. Simply tell them, "This type of problem happens all the time," and then go on to repair the system.

Also, always get a customer's permission before performing major corrections to the computer system such as replacing a motherboard or reinstalling the operating system, which could wipe out all previous software packages that the customer installed. Furthermore, this maintains transparency in your work while allowing you to converse with the user more in-depth about the issue.

As mentioned previously, a user may feel embarrassed or frightened to admit to the technician that they may have caused an issue to their device. However, it is vital that information regarding the environmental and infrastructural changes that may have occurred is obtained. In other words, something environmental may have caused the machine to become faulty, or perhaps the user allowed another coworker to use their machine to complete some of their work. While it may sound mundane, this information and criteria will help a technician derive and establish a theory of probable cause.

Establish a Theory of Probable Cause

1101: 5.1 A+

Once you have gathered sufficient information from the user about the problem and backed up the system files, you can form your theory about the probable cause. Recall the information presented earlier in the chapter about the three stages of system operation—hardware failure, software failure, and user-generated problems—to determine when the problem occurs. If necessary, conduct external or additional internal research based on the symptoms presented to help you establish a theory of probable cause. Nevertheless, also be sure to consider your organization's policies before implementing any changes regarding your theory.

If your theory and probable cause can be implemented according to your organization's polices, you may then determine if the cause was internal or external. If the cause was internal, you may need permissions from other administrators to investigate your theory further. An example of this would be files that are transmitted via the Human Resources office. In order to test this theory, you may need to have someone from the Human Resources office present with you, since there will be confidential information about members of the organization.

A+ 1101: 5.1

Test the Theory to Determine Cause

Test your theory with corrective actions related to what you believe is the cause of the problem. If your theory proves irrelevant to the issue with which you are confronted, you will need to determine if another theory needs to be generated or if the issue needs to be escalated to another means of action or technician with more experience. Once you establish another theory of probable cause, take corrective actions again. Repeat the sequence of establishing a theory and performing corrective action until the problem is solved. If you encounter a problem that you feel too inexperienced to fix, do not hesitate to escalate the issue to a technician with more experience than you have. It is better to ask for help than to make the problem worse.

A+ 1101: 5.1

Establish a Plan of Action

Establishing a plan of action to resolve the problem and implementing the solution relates to more than just repairing the computer; you need to ensure that the problem will not occur again. The plan of action may be as simple as replacing the power supply. In the last step, you tested the possibility that the power supply was defective and changed out the original power supply for one that is in known working order. The change fixed the problem, so you can now notify the customer that a new power supply is needed and provide a price quote for repair. If the customer gives permission, you can go order the replacement and repair the computer. Since components can differ significantly from one manufacturer to another, *always* refer to a vendor's instructions for guidance. This can save time if you get confused or become unsure of how to proceed. It can also help identify any unique actions that must be taken for a given component.

To prevent a reoccurrence of the problem, you can ask if the customer has surge protection or a UPS unit. The installation of a surge protector or UPS can help prevent losing a power supply in the future due to power surges. You also need to establish the fact that a power supply can still fail due to wear and tear or old age.

A+ 1101: 5.1

Verify Full System Functionality and Implement Preventive Measures

To verify full system functionality, you should not only check the system yourself, but also have the customer test the computer system. You need to establish that the computer is truly fixed to the customer's satisfaction.

A+ 1102: 3.1

In the example from the previous section with the damaged power supply, implementing preventive measures can be any number of procedures ranging from installing a UPS unit for surge protection to customer education. The education for the customer should be as simple as possible and not condescending in nature. You should *never* make customers feel uneducated about something they did if they are the cause of the problem. For example, if a computer failed because of a recent driver update, show the client how to "roll back" the driver, which will go a long way in winning a customer's confidence in you. It is not all about making money

from customer repairs. The customer who brought a computer in for repair will most likely not attempt a repair, even if it is as simple as rolling back the driver. The customer will respect the fact that you are willing to show how to make the repair, and it will also make the customer confident that you are not out to inflate the repair bill. A good customer relationship is the most valuable asset that a computer repair business can have.

Document Findings, Actions, and Outcomes

1101: 5.1 A+

Documentation of the findings, actions, and outcomes is standard practice in the computer-repair industry, largely so another technician can see what has been done to the system. For example, if the original technician does not come in because of illness and another technician takes over the repair or provides a status report to the customer, the documentation will prove vital. Clients are not going to be happy when they call about the computer repair and the response is, "I do not know. The person working on it is not here." Documentation also proves valuable when computers return for the same problem, which happens frequently. The existing documentation should have details about the problem, how it was fixed, and next steps should the problem reoccur.

Troubleshooting becomes much easier with experience. There will be times when you can immediately identify the source of a problem, though it will not be as easy other times. This is especially true with an intermittent problem. Do not hesitate to ask for help from other technicians or from sources such as the manufacturer website and the Internet in general, but always consider the source of information. There is a lot of bad information about computer repair on the Internet, especially in chat rooms or discussion groups, and many times, the solutions you find from questionable sources will cause more problems rather than fix the system. With time, dedication, and study, you will become an excellent technician.

Chapter Summary

17.1 Common-Sense Practices

- When troubleshooting, determine the major area at fault, determine what action occurred just prior to failure or problem, write down settings before you change them, go slowly, and think the problem through.

17.2 Troubleshooting by Boot Stage

- When troubleshooting computer problems, the first thing you must do is isolate the problem. The best way to go about this is to decide when the problem is occurring. In other words, at what stage of computer operation is the problem occurring?
- The three stages of computer operation are the POST, the loading and initialization of the required operating system files, and after the logon when services and application software are loaded and running.
- If the problem occurs during POST, it is most likely a hardware failure. A beep code is used to indicate failures before the video system is initialized, when there is no display on which to print screen messages.
- If the problem occurs during the second stage—operating system loading and initialization—the problem is most likely related to a corrupt operating system file or a driver.
- During the third stage, startup programs, services, and applications are loaded. The most common problems that can occur during the third stage are usually due to corrupt or incompatible drivers and files.

17.3 Commonly Encountered Problems

- A startup problem causes the computer to lock up during the boot process. These problems occur too early in the PC operation to be solved by system diagnostic tools.
- Common startup problems involve the power supply, CPU, hard drive (boot device), RAM, BIOS, CMOS, system configuration, loading of drivers, and the loading of the operating system.
- Hard drives have a high failure rate because mechanical systems have a higher failure rate than electronic systems.
- Hard drives can also fail because of corrupted files and data.
- If the read-write head becomes damaged or impaired, users and technicians may not be able to retrieve data from the hard drive.
- The S.M.A.R.T. Error Detection Tool can be used to discover when a drive produced an error, was not functioning properly, or if a drive needs to be replaced. Furthermore, the S.M.A.R.T. Error Detection Tool may provide fixes for technicians such as the hard drive needing to be reformatted or if the disk needs to have miscellaneous data removed to utilize the necessary hard drive space needed for present and future files and data.
- Besides hard drive failure, most other computer mechanical problems arise from two areas: improper hardware upgrades and accumulation of dust in the system.
- Many possible system failures can occur after a hardware upgrade. The first thing to check when a system fails to boot is the power and cable connections.
- Large amounts of dust can cause heating problems by blocking air filters and by collecting on processor heat sink fans and fan components, preventing the proper dissipation of heat.
- Other symptoms may cause a personal computer to lock up, overheat, cause loud disruptive noises, and other intermittent device failures. When a technician understands that these issues may arise, it also augments their troubleshooting abilities.

- System lockups are primarily discovered when an operating system cannot be modified and users perceive that the screen has frozen, since they do not see their mouse moving or their applications functioning.
- Although each model of a personal computer may be vastly different, it should have a serial number or service tag located on the console portion of the machine for a technician to obtain parts information along with the machine's warranty information.
- Should a technician not be able to find the cause of the faulty hardware, he or she will then need to either access the system's BIOS or boot into Windows Safe Mode to obtain the proper error logs and codes to determine which piece(s) of hardware are faulty.

17.4 Windows Diagnostic Utilities

- Some of the diagnostic utilities included in Windows are the DirectX Diagnostic Tool, System File Checker, Registry Editor, Event Viewer, Problem Steps Recorder, Widows Security and Maintenance, Performance Monitor, Resource Monitor, Reliability Monitory, Windows Memory Diagnostics Tool, and Component Services.
- DirectX is a software development tool used for multimedia applications that allows programmers to access many Windows built-in features, but a poorly written program using DirectX can cause severe system hangs or crashes.
- The System File Checker (**sfc.exe**) can be run to check for corrupt, changed, or missing files from Windows-based applications and restore system files.
- Registry Editor is a Microsoft software tool used to view and modify the system registry files. You should never attempt to repair the registry files directly. An error made in the registry files can render the computer system inoperable, resulting in your having to reinstall the system onto a clean hard drive.
- Event Viewer is a centralized depository of various logs relating to system setup and configuration, applications, security, and more. Logs are categorized by event type, including Error, Warning, Information, and Audit success.
- Problem Steps Recorder is a screen capture tool to record a problem as it is occurring.
- Remote Assistance allows a user to invite another user to access their computer and assist in repair.
- Windows Security and Maintenance identifies problems as they occur on the system and can be used to find solutions automatically.
- Performance Monitor can be configured to collect data about the computer system and specific hardware devices. Resource Monitor allows you to observe the effects of specific programs and services on computer hardware and resources. Reliability Monitor observes and records computer events that affect computer stability.
- Windows Memory Diagnostics Tool diagnoses memory module problems, and when problems are detected, it automatically restricts the use of the RAM cell locations, allowing the computer to be used until the RAM is replaced.
- The Component Services utility contains a Component Object Model (COM) that provides a suite of low-level drivers and interfaces that are needed to communicate and operate certain aspects of a personal computer.

17.5 Boot Sequences

- The major boot sequence phases for Windows are POST, initial startup, Windows Boot Manager, Windows Boot Loader, kernel loading, and logon.

17.6 Preventive Maintenance

- Performing regularly scheduled maintenance can prevent future problems and improve system performance.
- System backups should be performed regularly as part of routine maintenance.

- A system image is an exact replica of a hard drive partition, including all personal and operating system files. The system image can be used to repair a computer system to an exact copy the day the system image was created.
- The Disk Cleanup utility can be used to regain hard drive space such as that consumed by temporary files, files sitting in the Recycle Bin, unused Windows components, unneeded installed programs, and restore points created by System Restore.
- The Disk Defragmenter utility rearranges all files on your hard drive into a continuous series of clusters, resulting in better performance.
- Chkdsk is used to inspect the hard drive and correct errors in the file structure, such as bad sectors, lost clusters, cross-linked files, and directory errors.
- Staying up to date on patches, virus updates, and regular cleaning of the device can also help prevent issues.

17.7 CompTIA A+ Troubleshooting Objectives

- The A+ Certification Exam troubleshooting steps are identify the problem; establish a theory of probable cause; test the theory to determine cause; establish a plan of action to resolve the problem; verify full system functionality; and document findings, actions, and outcomes.

Review Questions

1. Identify five common-sense practices you should follow when troubleshooting a computer.
2. List four major fault areas to consider when troubleshooting a computer.
3. What are the three major stages of computer operation?
4. List the most likely causes of boot failure at each boot stage.
5. What are the most common causes for blue screen errors?
6. What is the most likely cause when you have a computer with no power lights and an inoperable fan?
7. Diagnose a computer that attempts to boot to the wrong device.
8. What actions should be taken if a user's profile is slow to load?
9. List three screen messages that may appear due to a bad hard drive or corrupt MBR.
10. What command can be used in Windows to recover an MBR?
11. What two areas of mechanical problems can arise other than hard drive failure?
12. What are potential causes of system lockups or intermittent device failures?
13. List and describe four Windows diagnostic utilities.
14. Which four hardware resources are monitored by the Resource Monitor?
15. Recall the Windows boot sequence.
16. How has the current Windows boot process changed since the release of Windows Vista?
17. Describe eight preventive maintenance tasks.
18. What is the difference between an incremental backup and a differential backup?
19. List the CompTIA A+ troubleshooting steps.
20. At what point should a technician escalate the problem?

Sample A+ Exam Questions

1. Which of the following is *not* checked during the POST?
   A. CPU system clock
   B. RAM
   C. Drivers
   D. Video controller

2. Which of the following typically causes a failure during the POST?
   A. Corrupt operating system boot files
   B. A printer driver
   C. A critical hardware device
   D. A software application
3. Which two files are required to load the Windows operating system for versions after Vista? Select two.
   A. **ntldr**
   B. **bootmgr**
   C. **autoexec.bat**
   D. **ntoskrnl.exe**
4. What is the name of the kernel in Windows versions after Vista?
   A. **ntldr**
   B. **ntoskrnl.exe**
   C. **ntdetect.com**
   D. **service.exe**
5. Which command is used to detect and automatically fix errors on a Windows 10 hard drive?
   A. **chkdsk/f**
   B. **fmbr**
   C. **scandisk**
   D. **msconfig32**
6. Which utility scans for corrupt, changed, or missing files from Windows-based applications?
   A. **regedit.exe**
   B. **msconfig.exe**
   C. **bootrec.exe**
   D. **sfc.exe**
7. How do you access the Backup and Restore feature in Windows?
   A. **Start**>**All Programs**>**System Restore**
   B. **Start**>**Control Panel**>**System and Security**>**Backup and Restore**
   C. Right-click **Computer**, select **Properties** from the shortcut menu, and then select the **System Restore** tab
   D. **Start**>**All Programs**>**Accessibility**>**System Restore**
8. Which command can be run to view and manually edit the system registry in Windows?
   A. **msconfig**
   B. **sysconfig**
   C. **regediting**
   D. **regedt32**
9. Which command can be issued to open the Microsoft System Configuration Utility?
   A. **sfc**
   B. **sysconfig**
   C. **msconfig**
   D. **regedit**
10. What would be used to diagnose a problem that occurs during the POST phase of the system boot operation?
    A. A POST card
    B. A multimeter
    C. System Configuration Utility
    D. A DOS disk