Windows 2000 Server

Chapter 14 - Troubleshooting Strategies

If a problem occurs while running Microsoft® Windows® 2000, you can use the general troubleshooting methods and tools provided with the operating system to isolate and fix a wide range of problems. Information in the registry can be used to determine why services are not working correctly. General troubleshooting methods can isolate the problem, as can isolating services or drivers that are not working properly; following the specific troubleshooting examples in this chapter can help solve problems with Windows 2000. If you are unable to solve the problem yourself, find out as much information as possible before contacting Microsoft Product Support Services.

In This Chapter

Related Information in the Resource Kit

- For more information about messages generated by the Windows 2000 Executive, see "Windows 2000 Stop Messages" in this book.
- For more information about the Event Messages, see the Windows 2000 Error and Event Messages Help on the *Microsoft® Windows® 2000 Resource Kit* companion CD.
- For more information about using the registry to troubleshoot problems, see the Technical Reference to the Windows 2000 Registry (Regentry.chm) on the *Windows 2000 Resource Kit* companion CD.

Technical Support and Services

Microsoft offers technical support and services ranging from self-help tools to direct assistance with a Microsoft Product Support Services engineer. Service categories include:

- Business customer support
- Education customer support
- Software or Web developer support
- IT professional
- Personal users

These services are available in the United States and Canada only. Features of some support options differ in Canada, while services outside the United States and Canada might vary. For information on support for products obtained outside the United States and Canada, please contact the Microsoft subsidiary in your area. For a list of worldwide Microsoft subsidiaries see the Support Options link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Note Customers who are deaf or hard of hearing can reach Microsoft text telephone (TT/TDD) services at (800) 892-5234 in the United States.

Support services are subject to current prices, terms, and conditions, which are subject to change without notice. For information about specific technical support options, see the Personal Online Support link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Note To provide the highest quality of support possible, it is sometimes necessary to end support for discontinued products and apply those resources to supporting the latest developments and technologies that Microsoft has to offer.

Project Ascent

Project Ascent is at the core of Microsoft support offerings. Through Project Ascent, support processes are further tuned to meet customer requirements, and processes are integrated more tightly. In addition, Project Ascent stresses the sharing of skills, resources, and infrastructure in emerging areas and creates continual learning opportunities for people to stay current on rapidly changing products and technologies.

Other Resources

Personal Online Support makes it easy to find answers to a variety of questions. The search engine uses a natural language query, allowing you to type your question in your own words and search the vast collection of problem-solving tools and technical information, including Frequently Asked Questions.

- Submitting questions on the Internet. In the United States and Canada, you can submit your Pay-Per-Incident or Priority Annual support questions on the Internet with Web Response.
- Microsoft Certified Support Centers. Success and the ability to meet the demands of the competitive market depend on high-quality and well-defined product support in environments that integrate various combinations of hardware, software, and operating systems from multiple vendors. Central to this support is provided by Microsoft Certified Support Centers (MCSCs). MCSCs are industry leading, multi-vendor support providers who have a special relationship with Microsoft that helps ensure that they deliver high quality technical support for Microsoft products.
- MSDN Online. MSDN Online and MSDN Online Support allow you to search Microsoft developer support information, including the Knowledge Base, troubleshooters, white papers, and downloadable files. For more information about MSDN Online Support, see the MSDN link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- Microsoft TechNet. TechNet CDs are packed with valuable and accessible technical information, and monthly editions provide updated information, including Knowledge Base articles, resource kits, the Software Library, Microsoft Services Directory, educational materials, and other useful software and information. For more information about subscribing to TechNet, see the Microsoft TechNet link on the Web Resources page http://windows.microsoft.com/windows2000/reskit/webresources .
- Technical Newsgroups. Technical newsgroups offer peer support for common computer problems. You can post persistent problems on an appropriate online forum. Other users might have already discovered, reported, and found solutions and workarounds for your problem. Suggestions from others can save you time in tracking down the source of the problem and provide direction for your troubleshooting tasks.

Troubleshooting Tools for Windows 2000

The Windows 2000 Setup CD and the *Windows 2000 Resource Kit* companion CD contain many software tools to help you manage TCP/IP, networks, the registry, security, remote administration, configuration, batch files, and other areas of the operating system. Several of these tools can be used for troubleshooting. These tools can help you maintain your system in the following ways:

- Keep your system running smoothly
- Isolate problem areas
- Diagnose problems
- Fix problems
- Seek further assistance

System Information

System Information is located under **System Tools** in the Computer Management snap-in. System Information collects and displays configuration information to help support personnel diagnose and correct problems. This tool displays the required data to resolve problems, including information about hardware, system components, and the software environment. More specifically, the tool can be used to gather information about the following:

- **Hardware Resources** displays hardware resource settings such as direct memory access (DMA), interrupt requests (IRQs), input/output (I/O) addresses, and memory addresses.
- **Components** displays information about the Windows 2000 configuration and is used to determine the status of peripheral devices, ports, and universal serial bus (USB) connections.
- **Software Environment** displays a snapshot of drivers, environment variables, tasks, and services loaded into computer memory. This information can be used to see if a process is still running or to check version information.

  Note You can use the **View** menu of the Computer Management snap-in to switch between the display of Basic and Advanced information. The Advanced view shows the information in the Basic view and additional information that might be of interest to more advanced users or to Product Support Services.

System Information Categories

The information displayed by System Information is divided into five categories: System Summary, Hardware Resources, Components, Software Environment, and Internet Explorer 5. The categories and subcategories displayed in System Information can be used for troubleshooting.

Note Hardware information is not available in safe mode. While System Information can run in safe mode, it is limited to displaying system components and the software environment.

System Information allows you to save, export, and print system information.

System Summary

System Summary provides general information about your computer system. This includes information about the version of Windows that you are running, including the installation folder, the amount of physical and virtual memory, the locale and local time zone, and information about system hardware, including basic input/output system (BIOS), central procesing unit (CPU), memory, and other system resources. Use this information at the beginning of the troubleshooting process to develop a basic picture of the environment in which the problem occurs.

Hardware Resources

Hardware Resources displays hardware-specific settings, such as assigned or used IRQs, I/O addresses, and memory addresses. Table 14.1 describes the information provided in Hardware Resources.

Table 14.1 Hardware Resources

Section	Definition
Conflicts/Sharing	Identifies resource conflicts between Industry Standard Architecture (ISA) devices or Peripheral Component Interconnect (PCI) devices. Use this information to help you identify hardware conflicts or troubleshoot a nonworking device.
DMA	Reports the DMA channels in use, the devices using them, and those free for use.
Forced Hardware	Lists hardware devices that have user-specified resources as opposed to system-specified resources. This information is useful when troubleshooting Plug and Play resource conflicts.
I/O	Lists all I/O port ranges in use and the devices using each range.
IRQs	Summarizes IRQ usage, identifying the devices using the IRQs and showing free IRQs.
Memory	Lists memory address ranges in use by devices.

Components

Components displays information about your Windows 2000 system configuration, including information about the status of peripheral devices, ports, and USB connections. There is also a summary of problem devices. Table 14.2 defines some of the items that can be listed in Components.

Table 14.2 Component Item Definitions

Section	Definition
Multimedia	Lists sound card information, audio and video codecs loaded, and drive letter and model of the CD-ROM drive. With a data CD-ROM in the drive, MSInfo also performs a data transfer test.
Display	Lists video card information and current video configuration.
Infrared	Lists infrared device information.
Input	Lists keyboard and pointer device information.
Modem	Lists modem information.
Network	Lists network adapter, protocol, and Winsock information.
Ports	Lists serial and parallel port information.
Storage	Lists information on hard disk drives, floppy disk drives, removable storage, and controllers.
Printing	Lists installed printers and printer drivers.
Problem Devices	Lists devices with problems. Each device flagged in Device Manager is displayed with the corresponding status information.
USB	Lists USB controllers and drivers installed.

Software Environment

Software Environment displays a snapshot of the software installed on the computer. Table 14.3 defines some of the software components that can be listed in Software Environment.

Table 14.3 Software Environment

Section	Definition
Drivers	Lists all drivers loaded, if they are currently running, and their status.
Environment Variables	Lists all system environment variables and their values.
Jobs	Lists all open jobs, including print jobs.
Network Connections	Lists all mapped network connections.
Running Tasks	Lists all processes currently running on the system.
Loaded Modules	Lists loaded system-level dynamic-link libraries (DLLs) and programs, along with their version numbers, size, file date, and path. This is for debugging software problems, such as application faults.
Services	Lists all system services available to the system, showing current run status and start mode.
Program Groups	Lists all existing program groups for all known users of the system.
Startup Programs	Lists programs started automatically from the registry, the **Startup** menu, or Win.ini.
OLE Registration	Lists object linking and embedding (OLE) file associations that are controlled by the registry.

Internet Explorer 5

The information provided by Internet Explorer 5 includes Summary, File Versions, Connectivity, Cache, and Content.

Tools Menu

The **Tools** menu lists several key support tools that can be used for troubleshooting. The **Tools** menu is available in the Computer Management snap-in.

Disk Cleanup

Sometimes Windows 2000 uses files for a specific operation and then retains them in a folder designated for temporary files. You might also have previously installed Windows 2000 components that you are no longer using. To avoid running out of space on your hard disk drive, you can reduce the number of files on your disk, or create more free space. Disk Cleanup searches your drive and shows you files that you can safely delete. You can choose to delete some or all of those files.

Dr. Watson for Windows 2000

Dr. Watson for Windows 2000 detects errors in programs, diagnoses errors, and logs diagnostic information. The Dr. Watson for Windows 2000 log file, drwtsn32.log, can be sent to support personnel to help diagnose problems. If a program error occurs, Dr. Watson for Windows 2000 starts automatically. To start Dr. Watson manually, click Dr. Watson in the **Tools** menu. For more information about Dr. Watson for Windows 2000, see Windows 2000 Server Help.

DirectX Diagnostic

The DirectX Diagnostic Tool is a Windows-based DirectX tool that presents information about the components and drivers of the Microsoft® DirectX® application programming interface (API) installed on your system. The DirectX Diagnostic Tool helps you test the functionality of DirectX, diagnose problems, and configure your system to optimize DirectX performance. Administrators and users can test sound and graphics output, test DirectPlay service providers, and disable some hardware acceleration features. You can use the DirectX Diagnostic Tools to gather information for a support technician.

Hardware Wizard

If a device is not Plug and Play, you might have to use the Hardware wizard in the **Tools** menu to tell Windows 2000 what type of device you are installing. After the device is detected or you identify the device using the Hardware wizard, Windows 2000 might ask you to insert the Windows 2000 Setup CD or the manufacturer's disk so it can load the proper device drivers. After the device drivers are loaded onto your system, Windows 2000 configures the properties and settings for the device.

Important

Note Allow Windows 2000 to configure the device properties and settings, don't do it yourself, unless absolutely necessary. If you manually configure properties and settings, the settings become fixed, and Windows 2000 cannot modify them in the future if a problem arises or if there is a conflict with another device.

You must be logged on as an administrator or a member of the Administrators group to configure a device using the Hardware wizard.

Network Connections

Network Connections opens the Network and Dial-up Connections folder which contains network connections for your computer and a wizard to help you create a new connection. From this folder, you can open a connection, create a new connection, access the settings and components of a connection, identify your computer on the network, and add additional networking components.

Backup

Backup protects data from accidental loss in the event of hardware or storage media failure. You can use Backup to create a duplicate copy of the data on your hard disk and archive the data on another storage device such as a hard disk or a tape. If the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a hard disk malfunction, you can easily restore the data from the archived copy.

For more information about using Backup and creating a backup plan, see Windows 2000 Help and "Backup" in this book.

File Signature Verification Utility

If system files are overwritten by unsigned or incompatible versions, system instability can result. The system files provided with Windows 2000 have a digital signature which indicates that the files are original, unaltered system files or that they have been approved by Microsoft for use with Windows 2000. The file signature verification utility ensures system integrity by detecting changes to critical system files digitally signed by Microsoft. The Advanced option in the **File Signature Verification** dialog box allows you to save the file signature verification results to a log file and to search using the following criteria:

- System files that are not signed.
- Other files that are not digitally signed.

Update Wizard Uninstall

Update Wizard Uninstall is a tool that you can use to remove a patch, driver, or system file that was installed from Windows Update and to restore the previous version of the file.

You can also remove a patch, driver, or system file and restore the previous version of the file by connecting to the Windows Update Web page and following instructions to uninstall. However, if you do not have an Internet connection when you want to restore a previous version of the file, you can use Update Wizard Uninstall to accomplish the task instead.

Windows Report Tool

The Windows Report Tool collects information about your computer that can be used by support personnel to diagnose and troubleshoot problems. This tool provides a description of the problem, the expected results, and the steps required to reproduce the problem. The Windows Report Tool collects system files to help technicians make their diagnoses. You can also change system file selections.

The Windows Report Tool takes a snapshot of your computer settings and selected system and application files. This snapshot can be submitted to a computer manufacturer, software vendor, or support personnel, such as by e-mail.

Device Manager

In Windows 2000, Device Manager is located under System Tools in the Computer Management snap-in. Device Manager is a Windows-based tool for managing installed hardware. It works with both Plug and Play and devices supported by Microsoft® Windows NT® version 4.0. With Device Manager, you can check if a hardware device installed is improperly configured or is inoperable. From the **View** menu, you can sort the installed devices and system hardware resources by type or connection. You can use Device Manager to disable, uninstall, or update individual device drivers and troubleshoot problematic devices.

Important Changing resource settings improperly can disable your hardware and cause your computer to malfunction or become inoperable. It is recommended that only users who have expert knowledge of computer hardware and hardware configurations change resource settings.

You must be logged on as an administrator or a member of the Administrators group to change resource settings. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.

For Plug and Play–compliant devices, there are no true default settings. Instead, Windows 2000 identifies devices and their resource requests, and then arbitrates requests among them. If no other device requests the same resources as another device, its resource settings do not change. If another device requests its resources, the settings might change to accommodate the request. Consequently, never change resource settings for a Plug and Play–compliant device unless absolutely necessary. Doing so makes its resource settings permanently fixed, and Windows 2000 cannot grant requests from other devices to use that resource.

Fixed resource settings on Plug and Play devices can be brought back to their original state: in the **Device Properties** dialog box, on the **Resources** tab, check the **Use automatic settings** check box.

All devices supported by Windows NT 4.0 have fixed resource settings, which are defined either while upgrading from a previous configuration, or later by using the Add New Hardware Wizard in Control Panel.

Certain circumstances might require users to change resource settings after they have been configured. For example, Windows 2000 might not be able to configure one device without creating conflicts with another. In such a case, a message usually appears to explain what you can do about the problem —for example, turn off a device to make room for the new device, disable the new device, or reconfigure a device from Windows NT 4.0.

The best place for resolving conflicts that might occur is the Hardware troubleshooter in Windows 2000 online Help. If you manually change a device configuration, Device Manager helps you avoid errors that can result from editing registry entries directly. If you need or want to resolve device conflicts manually, you can use Device Manager and try the following strategies:

- Identify a free resource, and assign the device to use that resource.
- Disable a conflicting Plug and Play–compliant device to free its resources.
- Disable a legacy device to free its resources, by removing the legacy device card and not loading the device drivers.
- Rearrange resources used by other devices to free needed resources.
- Change jumpers on your hardware to match the new settings.

AVBoot

The program InoculateIT AntiVirus AVBoot V1.1is a virus scanner that scans the computer memory, master boot record (MBR), and boot sectors on all physical disks installed for memory resident and boot sector viruses. If a virus is found, AVBoot can remove the virus. To create a startup floppy disk, insert an empty floppy disk and run Makedisk.bat from the folder Valueadd\3rdparty\CA_antiv of the Windows 2000 Setup CD. To scan for viruses, insert the AVBoot startup floppy disk into drive A and restart your computer. AVBoot runs automatically. For more information about AVBoot, see the readme file in the folder Valueadd\3rdparty\CA_antiv of the Windows 2000 Setup CD.

Important It is extremely important that you regularly update your antivirus program. In most cases antivirus programs are unable to reliably detect and clean viruses of which they are unaware. False negative reports can result when using an out-of-date virus scanner. Most commercial antivirus software manufacturers offer monthly updates. Take advantage of the latest download to ensure that your system is protected with the latest virus defenses.

Whether you use a third-party antivirus program or AVBoot, regularly update the virus signature files. Once you install an antivirus program, immediately update the signature files, usually through an Internet connection. Check with the software manufacturer's documentation for specific instructions. AVBoot includes update instructions in the installation folder and on the AVBoot floppy disk.

System File Checker

System File Checker (SFC) is a command-line tool that scans all protected system files and replaces incorrect versions with correct versions. It is part of the Windows File Protection (WFP) feature of Windows 2000.

The WFP feature provides protection for system files using two mechanisms. The first mechanism runs in the background. The WFP feature is implemented when it is notified that a file in a protected folder is modified. Once this notification is received, WFP determines which file was changed. If the file is protected, WFP looks up the file signature in a catalog file to determine if the new file is the correct version. If it is not, the file is replaced from the %SystemRoot%\System32\Dllcache folder or the distribution media. By default, WFP displays the following message to an administrator:

```
A file replacement was attempted on the protected system file <file
name>. To maintain system stability, the file has been restored to the
correct Microsoft version. If problems occur with your application,
please contact the application vendor for support.
```

The second WFP mechanism is SFC, which gives an administrator the ability to scan all protected files to verify their versions. SFC also checks and repopulates the Dllcache folder. The administrator can initiate a full scan of all system files, using either the **/scanonce** or **/scanboot** switches on SFC. If the Dllcache folder becomes damaged or unusable, you can use SFC with **the /purgecache** switch to remove the contents of the Dllcache folder, and copy the files from the Windows 2000 Setup CD again. All SYS, DLL, EXE, TTF, FON, and OCX files included on the Windows 2000 Setup CD are protected. By default, all versions of Windows 2000 Server cache all system files by default to ensure server reliability. Again, all versions of Windows 2000 Professional cache only the most critical system files.

The syntax for SFC is as follows:

```
sfc [/scannow] [/scanonce] [/scanboot] [/cancel] [/enable] [/purgecache]
[/cache size=x] [/quiet]
```

The SFC switches are listed in Table 14.4.

Table 14.4 SFC Switches

Switch	Description
/scannow	Scans all protected system files immediately.
/scanonce	Scans all protected system files once at the next boot.
/scanboot	Scans all protected system files at every restart.
/cancel	Cancels all pending scans of protected system files.
/quiet	Replaces all incorrect file versions without prompting the user.
/enable	Enables WFP for normal operation.
/purgecache	Purges the file cache and scans all protected system files immediately.
/cachesize=*x*	Sets the file cache size in bytes. This change does not take effect until you restart the computer.
/?	Displays this list.

Windows Update

Windows Update is an online extension of Windows 2000. It provides a central location to find customized files and product enhancements, such as service packs, device drivers, and new features, that have been specifically selected by Windows Update to work with your computer's configuration.

When Windows 2000 is installed, an Internet shortcut to the Windows Update is created on the **Start** menu. Windows Update uses Active Setup and Microsoft® ActiveX® controls to provide product enhancements. The ActiveX controls are downloaded and installed on your system when you connect to the Windows Update Web page. Once the controls are installed, they automatically compare device drivers installed on your computer with a database of updated drivers on the server. If any drivers are found to be newer than your current set, they are offered to you to install.

Note Windows Update requires an Internet browser that supports ActiveX controls.

Device drivers, system patches, or hot fixes can be uninstalled using the Restore page on the Web site. If you are unable to connect to the Windows Update Web site, you can uninstall the latest updates by using Update Wizard Uninstall. Existing files and drivers are automatically backed up before new ones are installed.

When you select **Start**, Windows Update scans your system, generates a list of items that can be updated, and then installs the files for the items you choose to update.

For system administrators who want to closely control the types of updates that users download to their computers, Windows Update offers a number of options, including the following:

- Corporate IT Catalog. Windows Update provides a searchable catalog of updates, drivers, and more. System administrators can select which downloads are available to users, download them to a server behind a firewall, and make them available over an intranet.
- Restricting Access to Windows Update. You can use Group Policy to restrict access to Windows Update. System administrators can control access to updates to ensure that Windows 2000 configurations remain consistent across all desktops. Use the following check boxes in System Policy Editor to restrict access:
    - **Override Local Web Page** redirects the user to a specified Web page the first time that Windows Update is launched.
    - **Override Windows Update Site URL** redirects the user to a specified URL when Windows Update is launched.
    - **Disable Windows Update** disables all access to Windows Update and removes its shortcut from the **Start** menu.

NetDiag

NetDiag is a command-line, diagnostic tool included with the Support Tools on the Windows 2000 Setup CD that helps isolate networking and connectivity problems by performing a series of tests to determine the state of your network client. NetDiag diagnoses network problems by checking all aspects of a host computer's network configuration and connections. Beyond troubleshooting TCP/IP issues, it also examines a host computer's Internetwork Packet Exchange (IPX) and NetWare configurations.

IPConfig

IPConfig is a command-line tool that displays the current configuration of the installed IP stack on a networked computer. Run IPConfig whenever you need to know the status of a computer's TCP/IP configuration. Start IPConfig from the command prompt rather than from Windows Explorer to see the resulting display.

Since the results fill more than one normal command prompt screen when you use the **/all** switch, you might wish to redirect the output to a text file which can be viewed later in Notepad. To redirect IPConfig's screen output to a text file type:

ipconfig /all > ipconfig.txt

Run IPConfig whenever you need to know the status of a computer's TCP/IP configuration. When used with the **/all** switch, it displays a detailed configuration report for all interfaces, including any configured wide area networks (WAN) miniports (typically used for remote access or VPN connections). The following is a sample report:

```
Windows 2000 IP Configuration

Host Name . . . . . . . . . . . . . : TESTPC1
Primary Domain Name . . . . . . . . : reskit.com
Node Type . . . . . . . . . . . . . : Hybrid
IP Routing Enabled. . . . . . . . . : No
WINS Proxy Enabled. . . . . . . . . : No
DNS Suffix Search List. . . . . . . : ntcorpdc1.reskit.com
dns.reskit.com
reskit.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : dns.microsoft.com
Description . . . . . . . . . . . . : Acme XL 10/100Mb Ethernet NIC
Physical Address. . . . . . . . . . : 00-CC-44-79-C3-AA
DHCP Enabled. . . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . . . . . . . . . : 172.16.245.111
Subnet Mask . . . . . . . . . . . . : 255.255.248.0
Default Gateway . . . . . . . . . . : 172.16.240.1
DHCP Server . . . . . . . . . . . . : 172.16.248.8
DNS Servers . . . . . . . . . . . . : 172.16.55.85
172.16.55.134
172.16.55.54
Primary WINS Server . . . . . . . . : 172.16.248.10
Secondary WINS Server . . . . . . . : 172.16.248.9
Lease Obtained. . . . . . . . . . . : Friday, March 05, 1999 2:21:40 PM
Lease Expires . . . . . . . . . . . : Sunday, March 07, 1999 2:21:40 PM
```

A number of other useful switches for IPConfig include **/flushdns**, which deletes the DNS name cache; **/registerdns**, which refreshes all Dynamic Host Configuration Protocol (DHCP) leases and re-registers DNS names; and **/displaydns** which displays the contents of the DNS resolver cache.

The **/release** <*adapter*> and **/renew** <*adapter*> options release and renew the DHCP-allocated IP address for a specified adapter. If no adapter name is specified, the DHCP leases for all adapters bound to TCP/IP are released or renewed. Table 14.5 lists all IPConfig switches.

Table 14.5 IPConfig Switches

Switch	Effect
/all	Produces a detailed configuration report for all interfaces.
/release <*adapter*>	Releases the IP address for a specified adapter.
/renew <*adapter*>	Renew the IP address for the specified adapter.
/flushdns	Removes all entries from the DNS Resolver Cache.
/registerdns	Refreshes all DHCP leases and reregisters DNS names.
/displaydns	Displays the contents of the DNS Resolver Cache.

/showclassid *adapter*	Displays all the DHCP class IDs allowed for the adapter specified.
/setclassid *adapter*	Modifies the DHCP class ID for the adapter specified.
/?	Displays this list.

Caution Many of the advanced features of IPConfig must not be used on a client system without the assistance of a network administrator or support personnel. Using these commands incorrectly can cause problems with the client system's connection to the server.

NBTStat

NBTStat is a command-line tool that is designed to help troubleshoot NetBIOS name over TCP/IP resolution problems. It displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NetBT). When a network is functioning normally, NetBT resolves NetBIOS names to IP addresses. Start NBTStat from the command prompt rather than from Windows Explorer to see the resulting display.

PathPing

PathPing is a command-line route tracing tool that combines features of the tools Ping and TraceRt with additional information. PathPing sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. PathPing shows the degree of packet loss at any given router or link, allowing you to pinpoint which routers or links might be causing network problems. Start PathPing from a command prompt rather than from Windows Explorer to see the resulting display.

IPSecMon

The IP Security Monitor (IPSecMon) is a Windows-based tool used to confirm whether your secured communications are successful by displaying the active security associations on local or remote computers. IPSecMon can be run locally or remotely if you have a network connection to the remote computer. IPSecMon displays an entry for each active security association. Use **Options** to set the refresh rate.

Troubleshooting Options

Several troubleshooting options that are built into Windows 2000 allow you to troubleshoot and resolve problems. Some problems are accompanied by an error message or display box. Windows 2000 troubleshooting options include:

- Stop Messages
- Event Viewer
- Windows 2000 Error and Event Messages Help
- Troubleshooters
- Troubleshooting Tools for Windows 2000
- Knowledge Base
- Windows 2000 registry

Stop Messages

Windows 2000 generates Stop messages when it detects an error condition from which it cannot recover. These messages must be interpreted and appropriate action taken to resolve the problems.

Stop messages are used to identify and debug hardware and software problems that occur while loading or running Windows 2000. When a mission-critical operating system fails, it is preferable to generate an obvious error message, such as a Stop message, rather than to fail in an invisible manner and possibly corrupt data. The Stop error consists of a blue screen, the actual Stop message, the text translation, the addresses of the violating call, and the drivers loaded at the time of the Stop error. The Stop message provides information to help in locating and identifying problem areas. Stop messages indicate where the error has occurred at both the address and driver levels.

The Stop message identifies the type of exception, and the exception indicates where the problem occurred; that is, whether it involved user-mode operating system software or kernel-mode (involving operating system, third-party drivers, or hardware) operations. The third and fourth lines describe which components were immediately involved and at what addresses.

The Stop messages that appear when the system fails are documented in the Error and Event Messages Help. For information about accessing information about Stop messages, see "Troubleshooting Stop Messages" later in this chapter. For more information about troubleshooting Stop messages see "Windows 2000 Stop

Messages" in this book.

Event Viewer

Event Viewer allows you to monitor events in your system. It maintains logs about program, security, and system events on your computer. You can use Event Viewer to view and manage the event logs, gather information about hardware and software problems, and monitor Windows 2000 security events. The Event Log service starts automatically when you start Windows 2000. All users can view application and system logs.

To access Device Manager, on the **Start** menu, click **Programs**, point to **Administrative Tools**, and then click **Event Viewer**.

Event logs consist of a header, a description of the event (based on the event type), and, optionally, additional data. Most Security log entries consist of the header and a description.

Event Viewer displays events from each log separately. Each line shows information about a single event, including date, time, source, event type, category, Event ID, user account, and computer name.

For more information about Event Viewer, see Windows 2000 Server Help.

Event Logs

You can use Event Viewer to view and manage the System, Application, and Security event logs.

System Log. The System log records events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log. The event types logged by system components are predetermined by Windows 2000.

Application Log. The Application log records events logged by programs. For example, a database program might record a file error in the Application log. Program developers decide which events to monitor.

Security Log. The Security log records security events, such as valid and invalid logon attempts, and events related to resource use, such as creating, opening, or deleting files or other objects. The Security Log helps track changes to the security system and identify any possible breaches to security. For example, attempts to log on the system might be recorded in the Security log, if logon and logoff auditing are enabled.

Note You can view the Security log only if you are an administrator for a computer.

By default, security logging is turned off, but you can use Group Policy to enable security logging. To control the types of security events that are audited, in Group Policy, go to Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy. To control the auditing of files and folders, display the properties of a file or folder. An administrator can also set auditing policies in the registry that cause the system to halt when the security log is full.

Event Descriptions

The format and contents of event descriptions vary, depending on the event type. The description indicates what happened or the significance of the event. Table 14.6 lists the five types of events recorded by the event logs.

Table 14.6 Event Types and Definitions

Event Type	**Definition**
Error	A significant problem, such as loss of data or loss of functionality.
Warning	An event that might not be significant, but might indicate a future problem.
Information	An event that describes the successful operation of an application, driver, or service.
Success Audit	An audited security access attempt that succeeds.
Failure Audit	An audited security access attempt that fails.

Viewing Events

After you select a log in Event Viewer, you can search, filter, sort, and view details about events.

Search for Events Searches can be useful when you are viewing large logs. For example, you can search for all Warning events related to a specific application, or search for all Error events from all sources. To search for events that match a specific type, source, or category, on the **View** menu, click **Find**.

Filter Events Event Viewer lists all events recorded in the selected log. However, you can filter events using specified criteria. Filtering the events that occur on your network can help you pinpoint the source of problems. All events are logged continually, whether the filter is active or not. If you archive a log from a filtered view, all records are saved, even if you select a text format or comma-delimited text format file. Filtering has no effect on the actual content of the log; it changes only the view.

Sort Events By default, Event Viewer sorts events by date and time from the newest to the oldest. When a log is archived, the default sort order is saved. You can also sort events to assess their sequence, filter events for specific characteristics, and search for events based on specific criteria.

View Details About Events The **Event Properties** dialog box shows a text description of the selected event and any available binary data. Binary data, which appears in hexadecimal format, is generated by the program that is the source of the event record. A support technician familiar with the source program can interpret its meaning. Not all events generate binary data. For more information about an event, highlight the event, and then click it.

If you archive a login log file format, you can reopen it in Event Viewer. Logs saved as event log files have an EVT file name extension and retain the binary data for each event recorded. Logs archived in text or comma-delimited format have TXT and CSV file name extensions, respectively. Such logs can be reopened in most word-processing or spreadsheet applications. Logs saved in text or comma-delimited format do not retain the binary data. When you archive a log file, the entire log is saved, regardless of filtering options.

Error and Event Messages Help

The Error and Event Messages Help is another source of troubleshooting information. Here, thousands of error messages are documented, with corresponding explanations and recommended user actions. In particular, the kernel Stop messages that appear when the system fails are documented in the Error and Event Messages Help.

The Error and Event Messages Help gives you quick access to message string definitions so that you can resolve system and network problems within a minimum amount of time. Messages are normally followed by a description of the circumstances that might generate the message and, if appropriate or needed, by a suggested user action.

Sometimes the suggested user action is to obtain help from a technical support group. If this is the case, collect the following information before contacting Product Support Services:

- The type of hardware you are using, including network hardware, if applicable.
- The exact content of the message that appears on the screen.
- A description of what happened and what you were doing when the problem occurred.

System Monitor

System Monitor is a tool that can be used to track system resources usage. System Monitor can be used to test an application's usage of system resources. Common objects that a user can log are memory, CPU, network, and disk activity.

For more information about performance monitoring see "Overview of Performance Monitoring" in this book.

Troubleshooters

The troubleshooters are self-serve utilities to help you easily pinpoint problems and identify solutions. You can use the troubleshooters to quickly solve routine glitches, or common network configuration or interoperability problems without contacting a support specialist. Troubleshooters are included in Windows 2000 Help. They ask a series of questions and provide detailed information on troubleshooting the problem.

Use the Troubleshooters to diagnose and solve technical problems with the following system components and events:

- Client Service for NetWare
- Dynamic Host Configuration Protocol (DHCP)
- Display
- Group Policy and Active Directory
- Domain Name System
- Hardware
- Internet connections
- Modem
- Microsoft® MS-DOS® programs
- Multimedia and games
- Networking (TCP/IP)

- Print
- Routing and Remote Access
- Remote Installation Services
- Sound
- Startup and Shutdown
- Stop Errors
- System setup
- Server Management
- Microsoft® Windows® 3.*x* programs
- Windows Internet Name Service (WINS)

Knowledge Base

The Knowledge Base is an excellent source of information about all aspects of using and maintaining Windows 2000. The Knowledge Base is a database of tips, hints, and solutions to known problems. It contains thousands of articles written by support professionals at Microsoft. Articles are added and updated daily.

You can search the Knowledge Base by keyword or you can specify a driver, downloadable tool, or troubleshooting tool. You can also ask a question using free-text query or you can search for specific Knowledge Base articles by referencing the unique article ID assigned to each article. An article ID is assigned in the form of the letter "Q," followed by a number. Use the keyword **kbprb** to search for problem resolutions.

To search for Knowledge Base articles, see the Knowledge Base link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Windows 2000 Registry

The Windows 2000 registry is a database repository for information about a computer's configuration. The registry contains information that Windows 2000 continually references during operations, such as:

- Profiles for each user.
- The programs installed on the computer and the types of documents that each can create.
- Property settings for folders and program icons.
- What hardware exists on the system.
- Which ports are being used.

The registry is organized hierarchically as a tree and consists of subtrees, keys, subkeys, and entries. The registry has five predefined keys through which all registry subkeys and assigned values are accessed.

Note When accessing the registry of a remote computer, only the registry keys HKEY_USERS and HKEY_LOCAL_MACHINE appear.

The five subtrees, through which all registry keys, subkeys and assigned values are accessed, are defined in Table 14.7.

Table 14.7 Registry Subtrees

Subtree	**Definition**
HKEY_CURRENT_USER	Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is referred to as a user's profile.
HKEY_USERS	Contains the root of all user profiles on the computer. HKEY_CURRENT_USER is an alias for a key in the HKEY_USERS subtree.
HKEY_LOCAL_MACHINE	Contains configuration information particular to the computer (for any user).
HKEY_CLASSES_ROOT	Contains two types of data: data that associates file types with programs, and configuration data for COM objects.
HKEY_CURRENT_CONFIG	Contains information about the hardware profile used by the local computer at system startup.

Registry Editors

A registry editor is an advanced, Windows-based tool for changing settings in your system registry, which contains information about how your computer runs. Windows 2000 stores its configuration information in a database (the registry) that is organized in a tree format. Although the registry editors Regedit and Regedt32 allow you to inspect and modify the registry, normally you do not need to do so, and making incorrect changes can break your system. An advanced user who is prepared to edit and restore the registry can safely use a registry editor for such tasks as eliminating duplicate entries or deleting entries for programs that have been uninstalled or deleted.

Folders represent subtrees, keys, and subkeys in the registry and are shown in the left pane that is displayed when you use the registry editors. In the topic pane, the entries in a key or subkey are displayed. When you double-click an entry name, it opens an editing dialog box.

Warning Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Edit your registry only if it is absolutely necessary. If there is an error in your registry and your computer ceases to function properly, you can restore the registry to its state when you last successfully started your computer. To do this, either select **Last Known Good Configuration** from the **Hardware Profile/Configuration Recovery** menu that is displayed during the startup process, or press F8 during Setup and select **Last Known Good Configuration** from the **Windows 2000 Advanced Options** menu. For more information about the **Windows 2000 Advanced Options** menu, which includes three safe mode options, see "Startup Process" in this book.

You can use a registry editor to add or delete keys and subkeys, and to add, delete, or change the values of entries. Entries that appear in the registry editors consist of three components. For example, in the following registry entry:

```
RefCount : REG_DWORD : 0x1
```

RefCount is the entry name, REG_WORD is the data type, and 0x1 is the value of the entry.

Updating Registry Information

Regedt32 and Regedit provide the following ways to update registry information:

- **Auto Refresh** (on the **Options** menu) automatically updates the registry when a change is made to registry data.
- **Refresh All** (on the **View** menu) updates all of the information in all registry editor windows.
- **Refresh Active** (on the **View** menu) updates only the information in the active registry editor window.

Note When **Auto Refresh** is in effect, a check mark appears next to the command and both **Refresh All** and **Refresh Active** on the **View** menu are unavailable.

You cannot use **Auto Refresh** while displaying the registry from a remote computer. If you click **Auto Refresh** while displaying a remote registry, the manual refresh options (**Refresh All** and **Refresh Active**) are not available. Although **Auto Refresh** appears to be working as it would if a local registry window were displayed, the contents of the remote window are not automatically refreshed.

For more information about using a registry editor to save a portions of the registry as files, and about printing, importing, and exporting registry data, see Windows 2000 Server Help and the Technical Reference to the Windows 2000 Registry (Regentry.chm) on the *Windows 2000 Resource Kit* companion CD.

Troubleshooting with the Registry

Many problems can be traced to services, device drivers, or startup control data. The Windows 2000 registry subtree HKEY_LOCAL_MACHINE contains this configuration information, so it is a good place to look for information to solve these types of problems.

Caution Do not use the registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Most of the examples in this section use the Regedt32.exe registry editor.

Table 14.8 briefly describes the registry keys for the HKEY_LOCAL MACHINE subtree.

Table 14.8 Registry Keys in the HKEY_LOCAL_MACHINE Subtree

Key	Description
HARDWARE	Describes the physical hardware in the computer, how device drivers use the hardware, and mappings and related data that link kernel-mode drivers with various user-mode code.
SAM	Contains security information for user and group accounts.
SECURITY	Contains local security policy, such as specific user rights.
SOFTWARE	Describes the software installed on each computer.
SYSTEM	Controls system startup, device driver loading, Windows 2000 services, and operating system behavior.

The SYSTEM key is the most useful for troubleshooting.

The registry information and examples in this section use the Transmission Control Protocol/Internet Protocol (TCP/IP) network protocol, which uses a DHCP server to get IP addresses. If your computer has a different configuration, or has third-party device drivers or services installed, the registry contains different information.

HKEY_LOCAL_MACHINE \SYSTEM

The HKEY_LOCAL_MACHINE \SYSTEM key contains information that controls system startup, device driver loading, Windows 2000 services, and operating system behavior. All startup-related data that must be stored (rather than computed during startup) is saved in the SYSTEM key.

Some of the most important troubleshooting information in the registry key HKEY_LOCAL_MACHINE \SYSTEM is the information in the control sets. A control set contains system configuration information, such as which device drivers and services to load and start. There are at least two control sets, and sometimes more, depending on how often you change system settings or have problems with the settings you choose:

- Clone
- ControlSet001
- ControlSet002
- CurrentControlSet

The registry subkey HKEY_LOCAL_MACHINE \SYSTEM \Select identifies how the control sets are used, and determines which control set is used at startup. This subkey contains the following entries:

- **Current**. Identifies which control set is the CurrentControlSet. When you use Control Panel options or a registry editor to change the registry, you are changing information in the CurrentControlSet.
- **Default**. Identifies which control set is used the next time you start Windows 2000, unless you either select the Last Known Good Configuration from the **Hardware Profile/Configuration Recovery** menu that is displayed during the startup process, or press F8 during Setup and select **Last Known Good Configuration** from the **Windows 2000 Advanced Options** menu.
- **Failed**. The control set that was pointed to by Default when a user last started the computer by selecting the **Last Known Good Configuration** option.
- **LastKnownGood**. The control set that is a clean copy of the last control set that actually worked. After a successful logon, the Current control set is copied to create the Clone control set, which is referenced by the LastKnownGood control set.

Note The Windows 2000 Advanced Options menu is displayed in safe mode. For more information about safe mode, see "Startup Process" in this book.

Using the LastKnownGood Configuration

You can start your computer in either of the following configurations:

- Default. The configuration that was saved when you shut down the computer.
- LastKnownGood. The configuration that was saved when you last successfully logged on to your computer. This configuration is invoked when you do the following:
  - Select **Last Known Good Configuration** from the **Hardware Profile/Configuration Recovery** menu that is displayed during startup.
  - Press F8 during Setup and select **Last Known Good Configuration** from the Windows 2000 Advanced

Options menu.

The configurations are stored as control sets in the registry key HKEY_LOCAL_MACHINE \SYSTEM. If you made changes to your configuration when you were last logged on, such as adding drivers, changing services, or changing hardware, the two control sets contain different information. As soon as you log on, however, the information in these control sets is the same. Therefore, if you are having problems with startup and think the problems might be related to changes in your configuration, do not log on. Instead, restart the computer, and start safe mode by pressing F8 when prompted. Select the **Last Known Good Configuration** option when the **Windows 2000 Advanced Options** menu is displayed. The **Last Known Good Configuration** option can help you recover from the following types of problems:

- You install a new device driver, restart Windows 2000, and the system stops responding. The LastKnownGood control set contains no reference to the new, faulty driver set and enables you to start.
- You install a new video driver and are able to restart the system. However, you cannot see anything, because the new video resolution is incompatible with your video adapter. Do not try to log on. If you have the option to shut down the computer without logging on, do so. If that option is not available, turn off the computer or use the reset button. Wait for all disk activity to stop before restarting, especially if the computer has FAT volumes.
- You accidentally disable a critical device driver. Windows 2000 is not able to start and automatically reverts to the LastKnownGood control set.

Using the LastKnownGood control set does not help in the following situations:

- Any problem that is not related to changes in control set information, such as information like user profiles and file permissions.
- Once you have logged on after making changes. The LastKnownGood control set has already been updated to include the changes made during the previous session.
- Switching between different hardware profiles. The LastKnownGood control set can only switch between configuration information in the registry. Use Hardware Profiles to correct this problem.
- Startup failures caused by hardware failures or corrupted files.
- Copying a new driver over an old one while the old one is active.

Select Subkey

The values for the entries in the Select subkey identify which control set is **Current**, **Default**, **Failed**, and **LastKnownGood**. For example, a value of 0x00000001 indicates ControlSet001 (Current).

ControlSet001 is modified when you make any changes using options in Control Panel. ControlSet001 will be used for the Default control set the next time you start the computer.

ControlSet002 is the LastKnownGood control set. If you choose this control set to start the computer, Windows 2000 uses ControlSet002.

Finding Service and Device Dependencies

This section describes using information in the Control and Services subkeys to troubleshoot problems with your computer.

When you install Windows 2000, it creates the Control and Services subkeys for each control set subkey in the HKEY_LOCAL_MACHINE \SYSTEM key. Some information, such as which services belong to which group, and the order in which to load the groups, is the same for all Windows 2000 computers. Other information, such as which devices and services to load when you start your computer, is based on the hardware and the network software installed on your computer.

Each control set has four subkeys:

- *Control*. Contains startup data for Windows 2000, including the maximum size of the registry.
- *Enum*. Contains the Plug and Play hardware tree.
- *Hardware Profiles*. Enables you to define different configurations for your computer and select the one you want to use at startup.
- *Services*. Lists all kernel device drivers, file system drivers, and Microsoft® Win32® service drivers that can be loaded by the boot loader, the I/O (Input/Output) Manager, and the Service Control Manager. It also contains subkeys describing which drivers are attached to which hardware devices, as well as the services that are installed on the system.

  Note The Control and Services subkeys can be used for troubleshooting startup and device driver problems, respectively.

Services Subkey

The registry subkey HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services contains information that controls how services are loaded. This section describes some of the entries for this subkey, with an explanation of their values.

ServiceGroupOrder Subkey

You can see the order in which device drivers must be loaded and initialized by viewing the registry subkey HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Control \ServiceGroupOrder.

Service Groups

Many device drivers are arranged in groups to make startup easier. When device drivers and services are being loaded, Windows 2000 loads the groups in the order defined by the ServiceGroupOrder subkey.

DependOnGroup Entry

When a subkey in the Services subkey has a value for the **DependOnGroup** entry, at least one service from the group must be loaded before this service is loaded.

DependOnService Entry

The **DependOnService** entry identifies specific services that must be loaded before this service is loaded.

By knowing the dependencies, you can troubleshoot problems more effectively. If a service is stopped, the services that depend on that service are also stopped. When you start a service, the Service Control Manager automatically starts services on which the selected service is dependent.

If any of the files that are part of a service are missing or corrupt, an error occurs when you try to start the service.

ErrorControl Entry

The **ErrorControl** entry controls whether an error during the startup of this driver causes the system to switch to the LastKnownGood control set. If the value of this entry is 0 (Ignore, no error is reported) or 1 (Normal, error reported), startup proceeds. If the value is 2 (Severe) or 3 (Critical), an error is reported and the LastKnownGood control set is used.

If the value of the **ErrorControl** entry is 0x1, an error is logged in the event log, but Windows 2000 completes startup.

ImagePath Entry

The **ImagePath** entry identifies the driver path and file name. You can use My Computer to verify the existence of the named file. The value of the **ImagePath** entry is %SystemRoot%\System32\Services.exe.

Start Entry

The **Start** entry determines when services are loaded during system startup. If a service is not starting, you need to determine when and how it should be starting, and then look for the services that should have been loaded prior to this service. Table 14.9 describes the values of the **Start** entry that determine when services are to be loaded.

Table 14.9 Values for the Start Entry

Value	Meaning	Description
0	Boot	Loaded by the boot loader (NTLDR or OSLOADER) during the startup sequence.
1	System	Loaded at kernel initialization during the load sequence.
2	Auto Load	Loaded or started automatically at system startup.
3	Load On Demand	Driver is manually started by the user or another process.
4	Disabled	Driver is not to be started. If a driver is accidentally disabled, reset this value by using the **Services** option in Control Panel. However, file system drivers are loaded even if they have a start value of 4.

Type Entry

The **Type** entry shows where the service fits within the Windows 2000 architecture. Table 14.10 lists a few possible values for the **Type** entry.

Table 14.10 Sample Values for the Type Entry

Value	Description

0x1	Kernel device driver.
0x2	File system driver, which is also a kernel device driver.
0x4	Set of arguments for an adapter.
0x10	A Win32 program that can be started by the Service Controller and that obeys the service control protocol. This type of Win32 service runs in a process by itself.
0x20	A Win32 service that can share a process with other Win32 services.

Many of the services that have a **Type** value of 0x20 are part of Services.exe.

Troubleshooting Suggestions

Reference materials, such as hardware and software installation records, notes about your configuration and problems experienced with it, and documentation provided with hardware and software products, can be valuable troubleshooting tools.

Keep Records

It is recommended that you record all hardware and software details in a notebook. If possible, note the order in which you set up the software, and list the software operating system and all of the software applications that are installed on the computer. When identifying your system, consider the following details:

- Number of CPUs.
- Processor class and speed of each CPU.
- Amount of RAM on each computer.
- Amount of hard disk drive space on each computer.
- Operating system, including versions and any service pack installations, hotfixes, or driver updates on each computer.
- Brand and model name of each computer.
- All software loaded on each computer.

Careful record keeping is essential to successful troubleshooting. Make sure to maintain records of your network layout, cabling, previous problems and their solutions, dates of installation of hardware and software, and so on, and keep them readily accessible.

Keep Notes

When troubleshooting a system, it is important to keep careful notes of your installation and of any troubleshooting attempts to correct the problem. You will find it valuable to read through your notes whenever a new problem occurs. The methods previously used to pinpoint other problems can also help you to handle new ones. Use a notebook to take notes as you install or set up a test scenario.

Refer to Documentation

Many problems occur when users begin a process without first familiarizing themselves with important concepts, issues, and guidelines. If you are having a problem:

- Read all the documentation.
- Check the Knowledge Base and search for information about the issue in the documentation provided in the Windows 2000 Resource Kit.
- Refer to the readme files and release notes provided with Windows 2000.

Finding Information About the Problem

Use the following checklist to find specific information about the problem:

- Check to see if the Emergency Repair Disk (ERD), backup data sets, or Disk Configuration backup is available.
- Does the computer work with another operating system?
- Try reinstalling the software to eliminate the problem.
- Determine if the system works with standard VGA.
- Is there IRQ or DMA sharing in WinMSD?
- Are any third-party services running?

- Are there terminate-and-stay-residents (TSRs) in the Task List, such as programs that are loaded with the startup group, or loaded in the registry?
- Are there any errors in Event Log? What is the exact text of the Event message?
- Search for related information in the Knowledge Base.
- Removed any nonessential cards.
- Where appropriate, contact third-party vendors for help.

Setting up the System for Further Troubleshooting

You can set up your computer to assist you in troubleshooting by configuring it to write information about errors to files that can be viewed or sent to a support engineer for analysis.

Local Stop File Creation

Setting up a system to write Stop information to a local Memory.dmp file is useful for servers that are extremely mission critical in nature and that must be backed up and running quickly. When you enable the System Recovery options to create the Memory.dmp file, the system writes the debugging information on your local hard disk drive. The Memory.dmp file on your hard disk drive can be sent to Product Support Services engineers for later analysis, and the server can be restarted. The System Recovery options in Control Panel are enabled by default on computers running Windows 2000 Server but not on computers running Windows 2000 Professional.

Sending the Dump File to Product Support Services

Compress the file, then send your file to support engineers by one of the following methods:

- Upload the file to an FTP server.
- Backup the file to tape and send the tape.
- Use Dumpflop.exe to backup the dump file onto floppy disks and send the disks.

Troubleshooting Techniques

There are several standard techniques that can be used to troubleshoot problems. Using the tools and documentation provided with your hardware and software is a good starting place. Once you have familiarized yourself with these materials, you can begin identifying the problem and testing the affected features to determine the exact cause. Problems can be caused by issues as diverse as incompatible hardware, outdated drivers, loose connections, incorrect configurations, or other issues. You can use a variety of resources to isolate the problem and determine if it is a known issue with a documented solution.

There are several basic troubleshooting tips and procedures that you can follow as a standard approach to solving problems:

- Follow the system checklist.
- Analyze symptoms and factors.
- Check to see if the problem is a common issue.
- Isolate the source of the problem.
- Define an action plan.
- Consult technical support resources.

Follow the System Checklist

Refer to the following checklist when you encounter a problem with the installation or operation of Windows 2000:

- Make sure no physical connections are loose.
- If there are any network connections, make sure they are all connected. If they are, restart the computer in case you have temporarily lost connection. Use the ping protocol to test whether client and server computers are connected.
- Even if you're not connected, restart your computers and make sure you still have the problem.
- Check Event Viewer for the system and the application events that might explain the problem. For information about using Event Viewer and the event logs, see Windows 2000 Help.
- Try a few tests of the affected feature to see if there are other problems you have not yet encountered. For more information about running test on features, see "Isolating the Source of the Problem" later in this chapter.

- Uninstall and reinstall the feature that is having a problem. Make sure the problem persists after reloading.

Analyzing Symptoms and Factors

Start troubleshooting by gathering information. Develop a clear understanding of the symptoms and collect pertinent system information to understand the environment in which they occur. Identify the exact problem to make it easier and faster for Product Support Services to solve your problem. Precisely what is not working correctly? Under what conditions does the problem occur? Which aspects of the operating system control those conditions? Is the problem specific to an application, or is it specific to a subsystem (networks, video, and so on)?

Has what you are trying to do ever worked on this computer before? If so, something might have changed that affects it. Have you changed hardware or installed new software? Has somebody else been using the computer, and could that person have made changes you do not know about?

If this program or functionality has never worked on this computer, compare the setup and configuration on this computer with the same program on another computer to identify differences.

The following questions are used by Product Support Services when troubleshooting problems. These questions can help you analyze the problem you are having.

1. Have you read the documentation?
   - If the answer is no, read the documentation to become familiar with important concepts, issues, and guidelines.
   - If the answer is yes, continue with the next step.
2. Can you install Windows 2000 on your computer using the Windows 2000 Setup program?
   - If the answer is no, contact Product Support Services.
   - If the answer is yes, continue with the next step.
3. Have you upgraded to Windows 2000 from the latest version of Windows NT? Did you apply the latest Service Pack? Are you using the latest versions of third-party drivers? Releases contain fixes to known software problems.
   - If the answer is no, install the latest version, service pack, or driver. If the problem persists, continue with the next step.
   - If the answer is yes, continue with the next step.
4. Have you installed new hardware or software recently?
   - If the answer is no, continue with the next step.
   - If the answer is yes, revert to the previous configuration. If the problem persists, continue with the next step.
   - If the error is the result of the recent change, call Product Support Services.
5. Was an error message displayed? Have you looked it up in the Error and Event Messages Help and the Knowledge Base? What is the probable cause and recommended user action?
   - If no error message was displayed, continue with the next step.
   - If you have implemented the user action recommended by the Error and Event Messages Help, and the problem still occurs, continue with the next step.
6. Check the Event Logs (System, Application, and Security, as appropriate) for any errors or warnings and search the Knowledge Base and the Error and Event Messages Help for their Event IDs.
   - If no errors or warnings were displayed, continue with the next step.
   - If you have implemented the user action recommended by the Error and Event Messages Help, and the problem still occurs, continue with the next step.
7. Did the task ever work? What happened just before it stopped working? For example, was new software installed? Did the network crash? Did the computer crash?
   - If the problem occurred after you installed new software or changed a configuration setting, reverse the activity you performed. If the problem still occurs, continue with the next step.
8. Are any files missing or have any been accidentally deleted?
9. If you are troubleshooting an installation problem, examine your notes to see if you can identify where the problem might have occurred. Did you receive any error messages during the installation process?
10. Is this a new system or an established system? If it's a new system, how is it different from earlier systems where this problem did not occur?

View **System Information** in the **Computer Management** snap-in to compare the hardware, software, and configuration of the computer you were using when the problem occurred with the hardware, software, and configuration of a computer where the problem did not occur.

11. Can you reproduce this problem on a different computer that has the same hardware?
    - If the answer is yes, the problem involves software.
    - If the answer is no, check the hardware on the computer you were using when the problem first occurred.
12. What happens in safe mode? For more information about safe mode, see "Startup Process" in this book.

Checking for Common Issues

Check to see if the problem is a common issue by reviewing Windows 2000 Server Help, and other document files included on the Windows 2000 Setup CD. For example, check Read1st.txt and Readme.doc in the root folder and the files in the Setuptxt folder.

Use the Troubleshooters in Windows 2000 Server Help to diagnose and solve technical problems. For a list of troubleshooters available with Windows 2000, see "Troubleshooters" earlier in this chapter.

Isolating the Source of the Problem

Identify the variables that could affect the problem. As you troubleshoot the problem, change only one of these variables at a time. If you must escalate your issue to a support provider, your detailed notes provide valuable information to the technician who is helping you solve your problem.

For example, if your computer does not complete startup, you need to identify exactly where it fails, and write down any error messages. If you get an error such as **Missing operating system** from the system BIOS when you start your computer, the problem is very different than if startup fails after the boot loader (NTLDR) starts. You know that the NTLDR has started when you see the message:

```
Starting Windows . . .
```

followed by a bar graph. When the bar graph turns solid, the text mode switches to the graphical mode (as represented by the display of the Microsoft Windows 2000 Server Family screen).

For more information about troubleshooting startup problems, see "Startup Process" in this book.

Eliminating variables can help determine the cause of a problem. Do symptoms manifest themselves when you run the system in safe mode? If not, check the programs that run when the system is started normally. Look at the icons stored in the Startup group located in the folder Documents and Settings*username*\Start Menu\Programs\Startup. Pointers to other programs executed at system startup are located in the registry at HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows \CurrentVersion \Run.

Caution Do not use the registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Troubleshooting Ideas

The following are several troubleshooting techniques to help you isolate problems. These include, but are not limited to, hardware and driver compatibility verification, software compatibility verification, and error message analysis:

- If the problem is the result of a recent change to the system, undo that change. Device Manager lists the device drivers installed on the system. If a device fails and its driver had been recently updated, replace it with the original driver and retest.
- If an update installed from the Windows Update Web site fails to meet your expectations, restore the original files by running the **Update Wizard Uninstall** from the **Tools** menu.
- If you had no problems the last time the system was started, enter safe mode by restarting the computer and pressing F8 at the Starting Windows screen. When the **Windows 2000 Advanced Options** menu is displayed, select **Last Known Good Configuration** to restore the system configuration to the last known working version. Restoring a previous system configuration results in the loss of any changes made in the interim.
- If you find that there are additional programs executed at startup that are not listed in either of these locations, your computer might be controlled by Group Policies. For more information about policies, see Windows 2000 Server Help. If the computer is on a network, logon scripts or system management

applications might also start programs on your computer as you log on to the network.

Caution The Plug and Play specification allows an operating system to disable devices at the hardware level. For example, if you disable a COM port in Device Manager, you might be required to enter the CMOS or system setup to re-enable it.

Test each modification individually to see if it solved the problem. Make note of all modifications and their effect. This information is useful when troubleshooting problems with support personnel, and it provides an excellent reference for future troubleshooting.

Hardware and Driver Compatibility

Make sure that all hardware and drivers are compatible with Windows 2000. Many problems are related to defective or incompatible motherboards, memory, drives, and drivers. Before adding hardware or drivers to your Windows 2000 system, follow the guidelines listed here:

- For new hardware and new drivers, install Windows 2000 on a single system by running the Windows 2000 Setup CD. Test all hardware for complete functionality on this single system before preinstalling multiple computers.
- See the Hardware Compatibility List (HCL) and "Designed for Microsoft Windows" hardware logo program information. For more information, see the HCL link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- The safest, most reliable drivers to use with Windows 2000 are those that have been tested and signed by Windows Hardware Quality Lab (WHQL). For information about driver signing, see the Windows Hardware Quality Lab link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- See the hardware-related readme files provided on the Windows 2000 Setup CD.

Software Compatibility

Make sure that all preinstalled software is compatible with Windows 2000. Certain problems can be related to software that doesn't work well with Windows 2000 or that has an installation routine that is not easily adapted to the preinstallation process.

Install Windows 2000 on a single system by running Windows 2000 Setup from the product CD. Install and test all software for complete functionality on this single system before preinstalling on multiple computers.

Viruses and Error Messages

Check for viruses and see error message documentation. Many problems are related to unexpected errors or system failures. For example, the computer stalls, general protection faults occur, and so on.

- If protection faults are occurring or the system is failing with Stop messages, check the Knowledge Base for documentation about error messages.
- Run virus-checking software on the reference system, network reference system, and target computers. It is recommended that regular virus checks be scheduled for all systems as a preventative measure. For more information about virus protection, see "AVBoot" earlier in this chapter.

Test the Affected Feature

Sometimes a single component is behaving incorrectly, such as giving error messages whose origin is cryptic or failing under conditions that cannot be duplicated. If you cannot pinpoint the problem, you might want to try a few tests on the component to gather additional information. Following are examples of tests that can help pinpoint a problem with a component:

- Make sure the component gives correct responses for valid inputs.
- Make sure the component gives incorrect responses for invalid inputs.
- Follow the data. As the data moves from one component to another, examine the inputs and outputs to see if you can determine where the error happens.
- Use a different set of inputs to see if the problem still occurs. Put together a file that produces a simple known output, and try the test again.
- If there is more than one computer involved, use independent means to test whether the computers are connected.
- If you can, check the installation to make sure communication is established between processes.

Developing an Action Plan

It is a good idea to outline your troubleshooting plan on paper. Decide what steps you want to take, and what you expect to do based on the results of each step. Then do the steps in order, and follow your plan.

If you see a result for which you have no plan:

- Return to the isolation phase.
- Determine what happens in similar situations.
- Define another plan.

Contacting Technical Support Services

Do as much as you can to troubleshoot your system, and carefully document your attempts. If you have followed the guidelines discussed in this chapter and the problem persists, contact Product Support Services.

Gather the following information before contacting Product Support Services:

- The version of operating system that you are running.
- The service packs and hotfixes that you have applied.
- The top four lines of any Stop message displayed.
- The frequency nature and the trap.
- Information about any third party drivers or services that are installed.
- A detailed hardware list, including configuration information:
  - Computer make and model
  - Hard disk type and size
  - Disk controllers installed
  - Amount of memory installed
  - Tape drive model
  - CD-ROM drive model
  - Network adapter
  - Serial ports
  - Other adapters

Troubleshooting Hardware Problems

Certain problems can arise when incompatible hardware is used with software, when hardware is configured incorrectly, when cables and other connections are not working properly, or from other hardware-related issues.

Hardware Compatibility List

The Hardware Compatibility List (HCL) is a compilation of computers and system hardware that have been extensively tested with Windows 2000 for stability and compatibility. It is the guide used by Product Support Services to determine if a computer is supported for use with the Windows 2000 operating system.

The most common cause of hardware problems is the use of hardware that is not listed on the HCL. To avoid problems, make sure that you are using a device make and model that is listed on the HCL.

It is especially important to refer to the HCL if you plan to use modems, tape backup units, or SCSI adapters. If your system component is not included on the list, contact Microsoft for an updated Windows 2000 HCL.

Even if several models from a manufacturer are included in the HCL, only those models that are included in the list are supported: a slightly different model might cause problems. Where special criteria are required for a model to be supported (for example, if a particular version of a driver is required), this information is described as a footnote in the HCL. As additional hardware is tested, including device drivers and other system components, the HCL is updated. The updated list and software are available through the electronic services listed at the end of the HCL.

If the system is not on the HCL or if components not on the HCL, such as hard disk drive controllers, net cards or video, appear to be involved in the problem, Product Support Services might not be able to fully support and diagnose the problem.

For the latest HCL, see the Hardware Compatibility List link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Tip Use System Information to determine the hardware configuration of the computer that you are troubleshooting. Print the hardware information and save it to a file, keeping the report and file with the other configuration information for your computer. You can use the report when planning to change the configuration.

Other Approaches to Troubleshooting Hardware Problems

If your hardware components are listed on the HCL, and you are still having problems, check that the physical connections are secure.

If you are using a SCSI device, check its termination. Even if you are sure the termination is correct, and you are having problems that could be due to incorrect termination, open the computer case and check again. Whenever possible use active rather than passive terminators.

Note Terminators are used to provide the correct impedance at the end of a cable. If the impedance is too high or too low, internal signal reflections can take place. These echoes represent noise on the cable and can corrupt subsequent signals, which can result in degraded performance or data loss.

Passive terminators are resistors with the appropriate resistance value for the characteristic impedance of the cable. Active terminators are slightly more sophisticated electronics that are able to better maintain the correct impedance necessary to eliminate signal reflection.

Verify that the SCSI cables are not longer than they need to be. If a two-foot cable is long enough to connect the device to the controller, do not use a three-foot cable. The acceptable lengths vary depending on such factors as whether you are using basic SCSI, SCSI-2, wide SCSI, ultra-wide SCSI, or differential SCSI; the quality of the termination; and the quality of the devices being used. Consult your hardware documentation for this information.

Check your hardware configuration. I/O and interrupt conflicts that went unnoticed with another operating system must be resolved when you switch to Windows 2000. Likewise, you must pay close attention to CMOS and Extended Industry Standard Architecture (EISA) configuration parameters when using Windows 2000.

The Knowledge Base is a good source of information for hardware problems. There are several articles about memory problems, memory parity errors, SCSI problems, and other hardware information in the Knowledge Base.

If your computer crashes randomly and inconsistently, you might have memory problems. You can use the **/maxmem** switch in the Boot.ini file to troubleshoot memory problems. For more information about the **/maxmem** switch, see "Startup Process" in this book.

Troubleshooting Specific Problems

Certain problems are common and have known solutions. If you can isolate the cause of a problem, or determine what actions seem to cause the problem, you can refer to documentation and troubleshooting articles to help you find a solution.

Troubleshooting Setup

During the GUI portion of Setup, Windows 2000 installs drivers, creates accounts, configures the network settings, and builds the system tree. If there are hardware problems or conflicting hardware settings, Windows 2000 probably will not succeed in installing or upgrading.

Problems after the final reboot of Windows 2000 Setup are normally due to incorrect information either in the Boot.ini file or in the hardware configuration. For more information about troubleshooting startup problems, see "Startup Process" in this book.

Many problems can be avoided with routine virus checks. Be sure to check for viruses before installing or upgrading to Windows 2000 on a computer that is already in use.

Troubleshooting Stop Messages

Information about troubleshooting Stop messages is provided in Windows 2000 Help and there is a Stop Errors troubleshooter. For detailed information about gathering information about and troubleshooting Stop messages see "Windows 2000 Stop Messages" in this book.

Troubleshooting the Startup Process

The following are the phases of a successful startup process:

- Initial phase
- Boot loader phase
- Kernel phase
- Logon phase

Any one of these startup phases can prevent the computer from starting successfully and might require troubleshooting. Troubleshooting might require examining the Boot.ini file, verifying drivers, or replacing damaged or missing files. You might also need to refer to the following steps:

- Identify the phases of a successful Windows 2000 startup.
- Identify the events of the initial phase of the startup process.
- Identify the events of the boot loader phase of the startup process.
- Identify the events of the kernel phase of the startup process.
- Identify the events of the logon phase of the startup process.
- Identify the contents and switches of Boot.ini.
- Verify which drivers were successfully loaded.
- Replace missing or damaged files.

Windows 2000 provides a variety of options that you can use when a computer does not start, including safe mode, the Windows 2000 setup floppy disks, the Recovery Console and the Emergency Repair Disk (ERD).

For more information about using the Windows 2000 startup floppy disks to start your computer, see "Planning a Reliable Configuration" in this book. For more information about troubleshooting startup problems and using safe mode, see "Startup Process" in this book. For more information on using the Recovery Console and the emergency repair process see "Repair, Recovery, and Restore" in this book.

Troubleshooting Networking Problems

Isolating the problem allows your problem report to be as informative as possible and greatly speeds up the investigation process. Refer to the following troubleshooting steps when you suspect that you have a network problem:

- Check your hardware (hub, cables, and so on).
- Check your network adapters and drivers.
- Use the ipconfig.exe tool. At the command line type:

  ipconfig /all

Scan through the output from ipconfig.exe, and try to answer the following questions:

- Do you have an IP address?
- Do you have a default gateway?
- Do you have a DHCP server?

Try to ping the default gateway and DHCP server. Attach the output to your mail, and then type:

ipconfig /all > c:\mail_attachment1.txt

Use the Netdiag.exe tool. At the command line type:

netdiag.exe

Scan through the output looking for words like "FATAL."

Make sure the domain controller is working properly by pinging the domain controller.

DHCP might be the problem. Try releasing your IP address, restarting DHCP and getting an IP address again.

If you can't get an address, do a network sniff of *all* traffic to and from your computer and to and from the DHCP server from which you usually get addresses. If you can't connect (even though you have a valid address), a network sniff of the connection attempt could be useful.

Note Use Nbtstat and Nslookup for name resolution and to report problems.

For more information about troubleshooting network problems, see the *Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide*.

Troubleshooting Video Problems

If your screen stays black or is skewed after a restart, either the video device is not resetting correctly during the restart or the video is sharing an IRQ.

Turn the power off and restart. If the video works, you probably need to turn the power off each time you restart Windows 2000. This problem is related to the video and system-BIOS.

If the video is still not working properly after shutting the power down and restarting, check for IRQ and memory conflicts with other cards on your system.

If you have installed a new video driver, or used the **Display** option in Control Panel to change the display type, you might have created an incompatibility between the driver and the video device. If you get a black screen instead of the logon message when you restart Windows 2000 this is likely the case.

Turn off your computer or use the reset button to restart your computer. In safe mode, select the **Last Known Good Configuration** option from the **Windows 2000 Advanced Options** menu. For more information about troubleshooting problems using safe mode, see "Startup Process" in this book.

Another option is to start your computer in safe mode and select **Enable VGA mode** from the **Windows 2000 Advanced Options** menu. Windows 2000 uses the standard VGA driver to start up. You can then use the **Display** option to reconfigure your video device.

Note Windows 2000 requires new video and printer drivers. Microsoft® Windows NT® version 3.51 and Microsoft® Windows NT® version 4.0 drivers for these devices do not work correctly when you are running Windows 2000.

Troubleshooting Services and Drivers

Some services are configured to start automatically on Windows 2000. The specific services depend on your computer configuration and which network services and protocols you are using.

To view which services should start automatically (and which did start), click **Start**, click **Administrative Tools**, click **Computer Management**, and then select **Services and Applications**.

Sometimes, if a file that is needed to load or run Windows 2000 becomes corrupt or is deleted, the system displays a message about a problem with the file. You might also get information logged in the event log. Either of these clues can help you find the problem.

Not all executable files (EXEs) or dynamic-link libraries (DLLs) report missing or corrupt files, and the symptoms of a missing file can be unpredictable. However, it is recommended that all Windows 2000 EXEs and DLLs be protected by System File Protection (SFP).

What do you do if there is no indication of an error, but you think that a component did not start correctly? To check the files, at the command prompt type:

SFC /Scannow

SFC scans all your protected System files immediately. You can check to see if all the Windows 2000 system files exist and appear to be uncorrupted. Symptoms of corruption include a file that is an unusual size (for example, zero bytes or larger than its original size), or having a date or time that does not match the Windows 2000 installation date or dates on service packs that you have installed. You can use Windiff.exe, which is included with the Support Tools on the Windows 2000 Setup CD to compare files in your %SystemRoot%\System32 folder and subfolders with files in these folders on another computer that is running Windows 2000.

Note SFP protects DLL, EXE, OCX, and SYS operating system files, as well as several TrueType and System Font files.

If you can log on to your computer, you can use the Drivers utility on the *Windows 2000 Resource Kit* companion CD to display information about the device drivers that were loaded. If you have previously printed the output from the Drivers utility (by redirecting the output to a printer or a file), you can compare the previous output with one produced when you think that drivers are not loading. Another method of determining if there are drivers missing from the list is to run the Drivers utility on a similar computer and compare the results.

Table 14.11 describes the output from the Drivers utility. The most important field is **ModuleName**, which is the name of the component.

Table 14.11 Drivers Utility Output

Column	Definition
ModuleName	The driver's file name.
Code	The nonpaged code in the image.
Data	The initialized static data in the image.
Bss	The uninitialized static data in the image. This is data that is initialized to 0.
Paged	The size of the data that is paged.
Init	Data not needed after initialization.
LinkDate	The date that the driver was linked.

Troubleshooting Problems with Portable Computers

Hardware profiles are especially useful for troubleshooting problems with portable computers. You can have one hardware profile for running your portable computer when it is in the docking station, and another one for the undocked situation. When you have more than one hardware profile defined, select the one that you want to use during startup from the **Hardware Profile/Configuration Recovery** menu.

To set up the hardware profiles, install Windows 2000 Professional when your portable computer is docked. Windows 2000 Setup installs the network software that you need to use your docking station and creates a hardware profile called Original Configuration (Current). You can copy this hardware profile and customize the new hardware profile.

You can also use the undocked hardware profile to set a different video resolution for your portable computer. For example, the Original Configuration can have the video resolution set to 1024x768 to run on your monitor, and you can change your undocked configuration to use a resolution of 640x480 or 800x600 as appropriate.

Additional Resources

- For more information about troubleshooting tasks, see Windows 2000 Server Help.
- For more information about the Microsoft AnswerPoint Information Services, see the *Windows 2000 Server Start Here* book.
- For more information about troubleshooting techniques, see the Knowledge Base link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Send feedback to Microsoft